Status of Policing in India Report 2023

Surveillance and the Question of Privacy

COMMON CAUSE
A ROMANCE WITH PUBLIC CAUSES SINCE 1980

लोकनीति
Programme for Comparative Democracy

LAL FAMILY FOUNDATION

CSDS
centre for the study of developing societies

For limited circulation, not for sale

Lokniti, 29, Rajpur Road, Civil Lines, Delhi 110 054
Phone: +91-11-23942199 Fax: +91-11-23943450
Email: csdsmain@csds.in; lokniti@csds.in
Website: www.csds.in; www.lokniti.org

Common Cause, Common Cause House, 5, Institutional Area,
Nelson Mandela Road, Vasant Kunj, New Delhi 110 070
Phone: +91-11-26131313
E-mail: commoncauseindia@gmail.com; contact@commoncause.in
Website: www.commoncauseindia.in

Published by

Common Cause & Lokniti – Centre for the Study Developing Societies (CSDS)

Disclaimer

The material in this publication is copyrighted. No part of this report can be reproduced either on paper or electronic media without permission in writing from CSDS. Request for permission to reproduce any part of the report may be sent to CSDS.

Usage of information

Forwarding/copy/using in publications without approval from Common Cause and CSDS will be considered as infringement of intellectual property rights.

Cover images credit: AI-generated images using Midjourney

Designed & Printed by

FACET Design
D-9, Defence Colony, New Delhi - 110024
+91-11-24616720, 24624336

Status of Policing in India Report 2023

Surveillance and the Question of Privacy

COMMON CAUSE
A ROMANCE WITH PUBLIC CAUSES SINCE 1980

लोकनीति
Programme for Comparative Democracy

LAL FAMILY FOUNDATION

CSDS
centre for the
study of developing
societies

Team members

Advisory Committee
Sanjay Kumar
Vipul Mudgal
Suhas Palshikar
Sandeep Shastri

Lead Researchers
Radhika Jha
Jyoti Mishra

Authors
Mohd Aasif
Anshi Beohar
Devesh Kumar
Aaliyia Malik
Umar Mohiddin
Aaryan Pandey
Vanshika Sharma

Research Support
Himanshu Bhattacharya
Himanshu Kapoor
Dhananjay Kumar Singh
Divyanshoo Singh

State Coordinators
Andhra Pradesh: E. Venkatesu
Assam: Dhruba Pratim Sharma
Gujarat: Mahashweta Jani
Haryana: Harish Kumar
Karnataka: Veena Devi
Kerala: Sajad Ibrahim
Maharashtra: Nitin Birmal
NCT of Delhi: Biswajit Mohanty
Punjab: Jagroop Kaur and Varun Goel
Tamil Nadu: Gladston Xavier
Uttar Pradesh: Shashikant Pandey
West Bengal: Suprio Basu & Jyoti Chatterjee

State Supervisors
Andhra Pradesh: Kiran Kumar Gowd
Assam: Nurul Hasan
Gujarat: Chandansinh Rathod
Haryana: Ravikant
Karnataka: Nagesh KL
Kerala: PS Abhishek
Maharashtra: Shivaji Motegaonkar
NCT of Delhi: Himanshu Kapoor
Punjab: Jatinder Singh
Tamil Nadu: Paul Nathan
Uttar Pradesh: Ranjana Upadhayay
West Bengal: Rima Gosh

Interns
Mahima Charan
Abhishek Maity
Faeza Wasi

Acknowledgment

The Status of Policing in India Report (SPIR) 2023 - Surveillance and the Question of Privacy owes its existence to the invaluable guidance and support from a team of experts and practitioners who work on issues related to surveillance and policing in India. We extend a special thanks to the serving IPS Officers, Mr. Subhash Chandra, Mr. Prashant Kumar, and Mr. Brijesh Singh, for sharing their expertise with us. Additionally, we would like to acknowledge the valuable insights shared by Ms. Anushka Jain (Policy Counsel, Internet Freedom Foundation), Mr. Apar Gupta (Executive Director, Internet Freedom Foundation), Mr. Arvind Verma (Former IPS officer and Professor, Criminal Justice, Indiana University), Ms. Beatrice Jauregui (Associate Professor, Centre for Criminology & Sociolegal Studies, University of Toronto) and Mr. Gagan Sethi (Vice-Chairperson, Centre for Social Justice) during the Focused Group Discussion (FGD).

We would also like to extend our gratitude to Mr. Manoj Mitta (Senior Journalist), Ms. Meeran Borwankar (Former IPS officer), Mr. Nandkumar Sarvade (Former IPS officer), Mr. Osama Manzar (Founder and Director, Digital Empowerment Foundation), Mr. Paranjoy Guha Thakurta (Senior Journalist), Mr. Prabir Purkayastha (Editor, NewsClick, and Advisory Board Member, Software Freedom Law Centre), Mr. Sanjay Sahai (Former IPS officer and Director, TechConPro Pvt Ltd), and Mr. Vibodh Parthasarathi (Faculty, Media Studies, Jamia Millia Islamia) for participating in the FGD.

We are deeply grateful for the insightful and constructive suggestions provided by domain experts on the research questionnaire and design. We extend our special thanks to Ms. Anita Gurumurthy, Mr. Aakar Patel, Mr. Ashwin Verghese, Mr. Andrew Ferguson, Ms. Anushka Jain, Mr. Apar Gupta, Mr. Arvind Verma, Ms. Beatrice Jauregui, and Ms. Devyani Srivastava for their valuable recommendations. We also appreciate our partner organisation, the Indian Police Foundation (IPF), particularly its President Mr. N Ramachandran, IPS, and former DGP for their continued support.

This study would not have been possible without the meticulous teamwork of state coordinators, state supervisors, field investigators, the data screening and data entry teams, researchers, and data analysts at Common Cause, Lokniti-CSDS, and their collaborators at numerous universities and institutions across India, who conducted training workshops, helped in sampling, and supervised pilot trials. We must also recognise the assistance provided by interns, Abhishek Rana, Purnajyoti Guha Thakurta, Rounak Mahajan, and Varnika Bhardwaj to the SPIR team.

We extend our deepest gratitude to our philanthropic partners, the Lal Family Foundation. We are indebted to them for believing in the project's philosophy of creating baseline literature on policing in India to help policymakers make fact-based decisions.

The Status of Policing in India Report (SPIR) 2023 builds on the foundation laid by Common Cause leadership since the 1990s. We express our special gratitude to the organisation's founder Director, Mr. H.D. Shourie, and all members of its Governing Council, past and present, particularly Mr. Vikram Lal, Mr. Kamal Kant Jaswal, Mr. Prakash Singh, and Dr. B.P. Mathur, who provided valuable guidance for the police reforms program from time to time.

We extend our special acknowledgement to the thousands of people who participated in the survey across the country. Their contribution is deeply appreciated.

Contents

List of Tables

List of Figures

Introduction

Surveillance and privacy: The context

Surveillance, as a concept, is ancient. Early humans needed it to survive their harsh environments. And when they settled in tribes and kingdoms, they required it to defend their communities. The evolving avatars of the modern state have consistently acquired sophistication in surveillance for reasons ranging from national security to witch-hunts.

Today, when the revolution in IT and communications has made surveillance all-pervasive, the spotlight is on privacy as a fundamental right. A big concern is that a variety of state and non-state players track every move we make. They profile our daily lives, our needs, habits, opinions, even aspirations, leaving us no choice to even opt out of their relentless shadowing. Some even manipulate our emotions and belief systems in order to polarise minds for electoral gains. The mundaneness of it all raises a plethora of legal and philosophical questions which we are trying to fathom through this study.

The present volume is the fifth Status of Policing in India Report (SPIR) by Common Cause and the Lokniti programme of CSDS. It systematically studies surveillance and a variety of surveillance technologies deployed by state agencies or the metaphorical big brother, and a range of private companies. It uses three parallel methods of investigation, i.e., official data on the installation and use of surveillance apparatus; a focused group discussion with domain experts; and an extensive survey of common people across India. The Report also studies legal and operational aspects of digital policing and surveillance. It assesses the awareness and perceptions of the police and the public around surveillance technologies and the state of training and preparedness of those operating them.

We believe that matters of surveillance and privacy profoundly impact the state of democracy, human rights, and the conduct of free and fair elections. As far back as in 2010, Cambridge Analytica harvested data of over 70 million Facebook users including their friends and contacts, for micro-targeting voters in the US elections. Since then, technology has undergone a tectonic shift. The Pegasus spyware, developed by the Israeli company NSO, which claimed to have sold it to 'vetted' governments, remotely installed a trojan horse virus on the smartphones of individuals to access every conceivable type of data. It was mostly used for the surveillance of dissenters, opposition leaders and journalists. Even though surveillance is often done by individuals and private companies, a bigger cause for concern is targeted surveillance by state agencies.

Surveillance and privacy

As targeted surveillance gets more sophisticated, citizens' personal data becomes more and more vulnerable. There is also a legislative void around the breach of data through surveillance, globally, and India is no exception. Our own surveillance projects such as the National Intelligence Grid (NATGRID), Centralized Monitoring Systems (CMS), and Network Traffic Analysis (NETRA), among others, allow the enforcement agencies to intercept, monitor and scrutinise any telephonic or internet communication. Several local authorities and state governments also use a variety of surveillance methods such as drones, CCTV cameras, phone tapping, and Facial Recognition Technology (FRT). Many of these impinge on the citizens' right to privacy emanating from Article 21 and the fundamental freedoms guaranteed under the Constitution of India.

At a time when technology is reshaping the world and corporate and state agencies are innovating fast, the constitutional guarantee of fundamental rights is the only protection available to the citizen against illegal surveillance. But such protection can only be effective if the law catches up sensibly with emerging technologies. The citizens also need to understand the value of their personal data which is being collected, stored, and shared often without their consent or knowledge. This involves some serious questions: Do we need a legal basis for surveillance or interception of the citizens' data? Should the agencies conducting surveillance have judicial or parliamentary oversight? How can the lawful authorisation of surveillance be made transparent? What is the legal remedy available to a citizen who is subjected to illegal or malicious surveillance?

It is pertinent here that the theoretical foundation of surveillance is built on the Foucauldian panopticon, or the round prison where all cells are visible from a central point, and where the exercise of power is linked with supervision by authorities (Foucault 1977). The notions of punishment and control were central to Foucault's political context of such surveillance, where authorities could watch every prisoner without being seen. It was meant to be a disciplinary institution where the suspicion of being under observation will have a chilling effect on future dissent. Panopticon was characterised by an "unequal gaze" between the rulers and the ruled.

Modern democracies try to correct this age-old imbalance by empowering the citizen with the right to information (RTI) and by protecting the whistle-blower who may expose corrupt or undemocratic practices. This allows the citizen to reverse the unequal gaze: by monitoring, scrutinising, and sometimes exposing, the state's actions for better accountability. However, many proposed changes, such as those envisaged under the Digital Personal Data Protection Bill, 2022 seek to dilute that power of the citizen. The draft Bill expands the scope of information which can be denied on the grounds of privacy. This may leave the information seeker to the whims and fancies of the authorities already endowed with disproportionate power over citizens. The RTI is becoming more like an aberration because the ecology of surveillance affects not just privacy but also civil liberties, internet freedom, and the existence of independent media.

Internet unfreedoms

The citizens' privacy is further restricted by the revenue models of the global internet giants like Google, Facebook, Twitter, WhatsApp, YouTube, etc. who track and profile us for profits. We were excited when some incredible products – such as Google search and Gmail – came to us for 'free.' But we, the users, turned out to be the real products in this business. By checking some boxes, we 'willingly' share our data with AI-based algorithms which go on to profile us neatly. But their snooping does not stop at marketing products. In many countries, the global internet platforms were caught bending their own standards of good governance in order to oblige the ruling dispensations, particularly in their missions to control dissent or to polarise opinions.

The internet also empowers the citizen to some extent but the state has the upper hand; it can switch off networks. According to a recent global report, the most frequent internet shutdowns, 84 times, were reported in India in 2022— the highest number for any country for the fifth consecutive year 2023. The authorities in India seem to have unlimited powers when it comes to surveillance followed by search and seizure. Phones and laptops are often taken away without mentioning the hash value – a unique numerical code which marks the integrity of the device or data seized. There are instances of malware being planted in some devices, allegedly by the police. The police and prison authorities in India have also been empowered to collect biological samples and behavioural attributes of under trials, convicts, or anyone arrested for an offense, under the Criminal Procedure (Identification) Act of 2022, which was passed without much discussion in Parliament.

The issue of surveillance is intrinsically linked with that of internet freedom which is on a consistent decline as per the Freedom House Report 2022. The report warns that "in at least 53 countries, users faced legal repercussions for expressing themselves online, often leading to draconian prison terms" (Shahbaz et.al 2022). This, obviously, would not have been possible without mass surveillance by private and state-sponsored agencies. A cause for concern globally is the fact that the production, dissemination, and impact of politically vital information is possessed and processed by the global internet platforms. And that is why ending big techs' monopoly over political communication is vital to save democracy from the perils of fast-changing technology, argues Fukuyama, Richman, and Goel in Foreign Affairs (Fukuyama et. al, 2020).

A silver lining?

It is heartening that the onslaught on citizen's privacy is being pushed back by many individuals, academics, institutions, and advocacy organisations across the world. Some global alliances are raising their voice against illegal, unchecked, and unaccountable surveillance. Coalitions of investigative journalists, citizen labs, whistle-blowers, and civil rights activists have exposed things like the Pegasus phone tapping scandal in which many governments, including India, were allegedly snooping on dissenters and adversaries. In another positive step, a nine-judge Constitutional Bench of the Supreme Court has held privacy as an intrinsic part of the Right to Life and Personal liberty under Articles 14, 19, and 21 of the Constitution. In another case, a Supreme Court-appointed committee, headed by Justice R V Raveendran, has recommended legal reforms to regulate electronic surveillance by intelligence agencies (Swami, 2022).

It may appear counterintuitive but the common people often support surveillance, perhaps, on the assumption that it is in the interest of national security and public safety. But they tend to take their right to privacy more seriously when it involves their financial data and bank transactions. We hope that improved awareness will make them mindful that protecting democratic freedoms, or the integrity of elections, is as crucial for our collective well-being as protecting our financial data. Our attempt in this study is to make sense of the ecosystem of surveillance from the citizens' perspective. We hope that it is also a step in the direction of improving awareness about privacy as a fundamental right and creating democratic resilience against illegitimate surveillance.

As always, we will be keen to know your feedback to the findings of this report.

Vipul Mudgal
Director, Common Cause

References

#KeepItOn. (2023). Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022. Retrieved from: https://www.accessnow.org/cms/assets/uploads/2023/03/2022-KIO-Report-final.pdf.

Foucault, M. (1977). *Discipline and Punish: The Birth of Prisons.* Pp 195-209, Vintage.

Fukuyama, F., Richman, B. Goel, A. (November 24, 2020). How to Save Democracy from Technology. *Foreign Affairs,* January/February 2021. Retrieved from: https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology.

Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. (2022). *Freedom on the Net 2022,* Freedom House, 2022, freedomonthenet.org

Swami, P. (2022, August 28). Surveillance State Isn’t a Secure One, Indian Govts Need to Get This. *The Print.* Retrieved from: https://theprint.in/opinion/security-code/surveillance-state-isnt-a-secure-one-indian-govts-need-to-get-this/1104180/.

Chapter 1:

Digital Surveillance: Conceptualisation and Theoretical Debates

CHAPTER 1

Digital Surveillance: Conceptualisation and Theoretical Debates

Modern life is nearly inconceivable without the use of artificial intelligence. It impacts and contributes to almost all aspects of our lives, including health, education, nutrition, livelihoods, community, emotional well-being, and relationships. According to World Bank data from 2020, 43 percent of Indians use the internet, and a more recent Global Digital Report shows that the internet penetration rate stood at 47 percent of the total population at the start of 2022 (Kemp, 2022).

Although technological terms such as artificial intelligence, machine learning, speech recognition, and language processing might appear at first glance to be convoluted and futuristic, they are deeply integrated into the everyday life of a common person in India. Even mundane activities such as using Google, emailing, using an online map app, scrolling through social media platforms, and shopping online involve the use of these technologies.

The use of such technology has also seeped into governance, including areas such as criminal justice and policing. However, the very complexity of technology enables it to conveniently shield from its users some of the serious threats it poses to people's right to privacy. The murkiness of the entire network of technology-enabled surveillance leaves ample scope for loopholes in the law, accountability, and traceability, making it difficult to distinguish between the private and the public, the legal and the illegal, ease of access and surveillance, and even the surveyor and the surveyed. This brings into sharp focus the issue of consent and the connotations that the term might carry in the digital world.

1.1. The surveillance landscape: Who, how and why?

Answering some of the most fundamental questions on surveillance is also perhaps the most complex issue due to the nebulous ways in which surveillance plays out in the real world. While both the state and private sector regularly engage in surveillance activities, the boundaries often overlap, as do the stated objectives behind these practices. One example is the Facebook-Cambridge Analytica scandal of 2013, which brought to light the practice of private companies misusing Facebook users' data for shaping electoral choices.

Broadly speaking, state and private surveillance follow two separate logics, even though they intersect at many points. For the private sector, surveillance aims to capture people's personal information for profiling their consumeristic behaviour. People's data becomes a commodity harvested by data mining agencies to be sold to companies for curating their marketing strategies per the users' preferences. This ever-increasing surveillance by the private sector has led to what philosopher Shoshana Zuboff terms as "surveillance capitalism" – surveillance meant to monitor data and modify and direct people's behaviour. This system has shifted the focus from individuals to entire societies, profiling them at one level, and nudging them towards specific consumeristic behaviours at the other. Zuboff further argues that surveillance capitalism uses 'instrumentarian power' to monitor and shape our actions remotely, unimpeded by law. Instead of relying on the ideas of violence and fear, these digital networks work in impersonal and ubiquitous ways, systematically eliminating people's right to resist (Zuboff, 2018).

The state, on the other hand, proclaims to employ these technologies for reasons of maintaining order in society, ensuring compliance with the law, and better administration and management of the public. However, the unchecked use of surveillance by the state can take much more nefarious forms, being used for controlling any kind of dissent, controlling electoral behaviour, constricting people's freedoms and rights, ensuring conformity to a specific notion of the ideal citizenry, and targeting groups or communities that may be seen as unfit and incongruous.

Philosopher Jeremy Bentham came up with the concept of the panopticon for prisons, an infrastructure designed in such a way that prisoners can always be watched centrally by a guard, but the prisoners themselves would not be able to tell whether or not they are being watched. This surveillance design attempts to create the illusion or fear of being continually monitored. The panopticon is a circular structure in which prisoners are housed in cells arranged around a central guard tower (McMullan, 2015). This design allows a single guard to observe all of the prisoners at once, without the prisoners knowing whether they are being watched at any given time. This creates a sense of constant surveillance and control, even when no actual monitoring is taking place.

French philosopher Michel Foucault later used the panopticon as a metaphor for society's broader system of social control and discipline. He argued that the mere threat of surveillance and coercion can lead to individuals internalising self-regulation, even in contexts outside of the prison. This means that individuals may modify their behaviour based on the possibility of being observed, even if they are not being monitored.

Foucault's theory highlights the power dynamic between those who are observing and those who are being observed. He suggests that surveillance can be a tool for those in positions of power to maintain control over others, by creating a sense of constant monitoring and the fear of potential consequences for non-conformity (Mason, 2023).

The core argument against state surveillance and its potential for inducing internalised behavioural modification is a central concern for the right to privacy. In India, although such technologies are not yet commonplace, the use of CCTV cameras by private companies and individuals is becoming increasingly widespread. However, research worldwide suggests that the presence of CCTV cameras has little to no impact on crimes. Despite this, there is a popular narrative that supports the installation of more cameras to improve law-and-order, among both the public and politicians. The Delhi Chief Minister, Arvind Kejriwal, boasted about the city's record of having the most CCTV cameras per square mile worldwide and promised to install another 1.4 lakh cameras (Vincent, 2021). Moreover, the sharing of private user data with police has already begun in several cities. For example, the Bhopal police launched a mobile application called 'Bhopal Eye,' which allows the police to access live feeds from private users' CCTV cameras (Chandran, 2023).

1.2. Surveillance trends in India: The broad contours

Governments worldwide, including India, are increasingly using big data technology to expand their surveillance powers. In India, the datafication of individuals for governance and business purposes has become a pervasive issue due to the absence of strict data protection laws. Both state and private actors are collecting and storing as much data as possible in the hope of utilising it at a later point, despite a Supreme Court ruling declaring privacy a fundamental right.

Commonly used surveillance technologies

1. **CCTV cameras**: These are widely used in public spaces, commercial buildings, and residential areas for surveillance and monitoring.
2. **Facial recognition technology:** This technology is used to identify individuals from images or videos captured by cameras. It is commonly used by law enforcement agencies and border security forces in India.
3. **Drones:** Also known as unmanned aerial vehicles (UAVs), drones are flying machines that can be operated remotely without a human pilot on board. They are typically equipped with cameras, sensors, and other technology that allows them to perform various tasks such as capturing aerial photos and videos, conducting surveys, and even delivering packages.
4. **Mobile tracking systems:** These are used to track the location of mobile phones and are commonly used by law enforcement agencies to track suspects or investigate crimes.
5. **Big data analytics:** Big data analytics surveillance is the practice of collecting and analysing large amounts of data from various sources to monitor and track individuals, groups, or populations. This type of surveillance relies on sophisticated algorithms and software tools that can process vast amounts of data quickly and accurately. The data that is collected can come from a variety of sources, such as social media, mobile phones, sensors, cameras, and other digital devices.
6. **Social media monitoring tools:** These tools are used by government agencies and law enforcement agencies to monitor social media activity and track the online behaviour of individuals.
7. **Automated number plate recognition (ANPR):** This technology is used to capture and read vehicle number plates, which can help in identifying and tracking vehicles involved in criminal activities.
8. **Biometric identification systems:** These are used to identify individuals based on their unique biological characteristics such as fingerprints, iris scans, and facial recognition.
9. **Stingray devices:** These are portable devices that mimic cell phone towers and intercept cellular signals, allowing authorities to track the location and communications of suspects.
10. **Internet surveillance systems:** These are used to monitor internet traffic and communications, enabling government agencies to intercept and analyse emails, instant messages, and other forms of online communication.
11. **Voice recognition:** This technology uses algorithms and machine learning to identify and authenticate an individual based on their unique voice pattern or vocal characteristics. This technology analyses various aspects of a person's voice, such as pitch, tone, accent, and pronunciation, to create a voiceprint that can be used to identify them.
12. **Spyware:** Spyware is a type of malicious software that is designed to secretly collect information from a computer or mobile device without the user's knowledge or consent. It can be installed on a device through a variety of methods, such as through phishing emails, infected downloads, or by exploiting vulnerabilities in software or operating systems. Once installed, spyware can monitor a user's online activity, capture keystrokes, record conversations, and even take screenshots of the device's display. This information is then sent back to the attacker, who can use it for various purposes, such as identity theft, financial fraud, or espionage.

Surveillance has recently gained much traction due to the increasing number of news reports regarding various instances of surveillance and cybercrimes (Steinmetz, 2020). Police in several Indian states has routinely used facial recognition technology (FRT) to stop and screen people on suspicion. FRT software systems are being hooked up to a spreading network of closed-circuit television (CCTV) by multiple state-owned agencies to identify people on a real-time basis (Mukul & Sasi, 2021). Since 2019, several states and central agencies have extensively used FRT and drones on civilians, notably during the Covid-19 lockdown and protests against the Citizenship Amendment Act and farm laws (PTI, 2019).

Along with camera-based technology like drone cameras, CCTV, and facial recognition technology, the Indian government has proposed several surveillance-based intelligence-gathering projects such as NATGRID, CCTNS, NETRA, CMS, and AASMA. There is also a concern amongst a section of society about India's flagship identification project UID (also known as Aadhaar), which collects biometric details and other demographic details of citizens and provides a unique identification number to each individual. Serious privacy concerns have been raised about Aadhaar, especially since the government has started pushing people to link their Aadhaar ID with phone numbers, bank accounts, pensions, etc.

Cybersecurity experts have pointed out that Aadhaar numbers, along with other sensitive data, were available on the internet for sale (Khaira, 2018). Digital surveillance has expanded the powers of states to surveil and brought on board private actors with even greater capacities to grab mass data. Thus, citizen-centric data protection regulations are inevitable.

The absence of stringent legal regulations about citizens' privacy rights has provided cushioning to the actions of governments and private actors globally. Getting official information about surveillance is a significant challenge privacy rights activists face, primarily due to the secrecy inherent to surveillance. A major chunk of public discourse on surveillance and privacy in India is still based on unofficial reports. Rapidly evolving technology is constantly challenging the existing norms of the privacy policy and legislation and, as many experts have pointed out, India's surveillance framework needs a real improvement on the transparency, oversight, and accountability front.

Some surveillance projects in India

1. **Central Monitoring System (CMS):** The CMS is a government-run project that enables law enforcement agencies to monitor all telecommunications and internet traffic in India. The system can intercept and analyse voice and data communications, as well as track the location of mobile phones.
2. **Crime and Criminal Tracking Network and Systems (CCTNS):** The CCTNS is a digital surveillance project launched by the Indian government to improve law enforcement in the country. The system allows police to track and share information on criminal cases and suspects, and provides a centralised database of criminal records and information.
3. **Aadhaar:** Aadhaar is a biometric identification system that assigns a unique identification number to each Indian citizen. The system collects biometric data such as fingerprints and iris scans, which can be used for identity verification and authentication.
4. **National Intelligence Grid (NATGRID):** NATGRID is a project aimed at creating a centralised database of intelligence and law enforcement data from various agencies across India. The system allows agencies to share information and track individuals and groups of interest.

5. **Railway Protection Force (RPF) Surveillance System:** The RPF surveillance system is used to monitor railway stations and trains for criminal activity and other security threats. The system includes cameras, sensors, and other technologies to detect and prevent crime.
6. **Smart Cities Mission:** The Smart Cities Mission is a government initiative aimed at developing sustainable and technologically advanced urban infrastructure in cities across India. The initiative includes projects related to smart transportation, waste management, public safety, and other areas, many of which involve digital surveillance technologies.
7. **Social Media Monitoring:** In 2020, the Indian government reportedly launched a project to monitor social media platforms like Facebook, Twitter, and Instagram for "inflammatory" content. The government stated that the project was intended to prevent communal violence and other threats to public order.
8. **National Cyber Coordination Centre (NCCC):** The NCCC is a project aimed at improving India's cybersecurity infrastructure. The system monitors internet traffic and provides real-time alerts about cyber threats and attacks to government agencies and other organisations.
9. **Advanced Application for Social Media Analytics (AASMA):** It is designed to collect live data of users from multiple social networks, do sentiment analysis on the content they post, track their location, and alert authorities accordingly.

1.3. Surveillance by the police in India

1.3.1. Mass surveillance and predictive policing

Surveillance is a tool employed worldwide under the philosophy of preventive policing. However, as discussed earlier, it has been found that popular surveillance mechanisms have little to no effect on crime rates. In India, the most commonly used surveillance tool by the police so far is CCTV cameras. However, because of the lack of data and transparency, the frequency of usage of other tools is largely unknown. Nonetheless, police forces across the states are progressively heading towards more regularised usage of other tools, including facial recognition video analytics, which can be done using the CCTV camera feed.

Different state police forces are at different levels of usage of such tools, functioning within a legal vacuum that can provide safeguards. States such as Delhi (in 2015) and Himachal Pradesh (in 2020) launched predictive policing strategies, which include crime mapping and analytics using artificial intelligence (AI) algorithms for future predictions of crimes and mapping out 'hotspots' for certain types of crimes. However, the same critiques of the use of these technologies that have been levelled against police forces in western countries, such as the United States, would be applicable, debatably more so, in India.

One major component that predictive policing relies on is the use of historical crime data. This data, in India, is tainted with caste, religious and class-based prejudices, with Muslims, Dalits and Adivasis being frequently targeted by the criminal justice system unfairly and resulting in these groups being disproportionately over-incarcerated. Another factor that would hinder the objectivity of the predictive policing matrix using past crime data is the factor of burking, or non-registration of crimes by the police. It has been pointed out in several studies that burking occurs more frequently in crimes committed against vulnerable groups, such as crimes against women, children, etc. Thus, the sheer unreliability of the crime data itself would make its usage for predictive policing suspect.

Unlike western nations from whom the concepts have been borrowed, Indian police forces are not very forthcoming with information regarding the use of these AI tools and strategies that they have launched. In 2015, Delhi launched the Crime Mapping, Analytics and Predictive Systems (CMAPS) for live spatial hotspot mapping of crimes, criminal behaviour patterns and suspect analysis. However, efforts to collect information regarding both its usage and efficiency have been unfruitful because of the large exceptions for law enforcement under the RTI Act. An ethnographic study of the Delhi Police's CMAPS project (Marda & Narayan, 2020) found that the data suffer from three kinds of biases:

1. Historical bias: The fact that there has historically been greater surveillance of disadvantaged groups along the axis of caste, religion, gender and class, which causes a training data bias in the algorithms, with the bias being actively embedded within the system.
2. Representation bias: The input data for CMAPS consists of calls to the Dial 100 call centre and a national database used to track crimes and criminals. Since most of these calls come from the socio-economically underprivileged parts of the city, there is an over-representation of these localities in the CMAPS sample while the higher-income and upscale areas are often under-represented.
3. Measurement bias: In the temporary settlements of Delhi, there is lesser accuracy of spatial distribution, while in the privileged neighbourhoods, more nuanced data is available, thus making them less likely candidates for future scrutiny. The authors of the study note that this bias is a result not only of the system's blind spots but also due to the vulnerable individuals' inability to engage with the system as well as others. For instance, some callers from poor localities, particularly women, did not know their address or locality, thus being asked by the call takers to find out and call again.

The use of technology by state police forces in India for surveillance purposes raises serious concerns regarding privacy violations and potential misuse of power. The CMAPS data system, as noted in the study, is not only discriminatory but also lacks transparency and accountability. The study further notes that there is indirect discrimination in the CMAPS data because of higher granularity in the crime data occurring in socio-economically well-off neighbourhoods, while the crimes occurring in poorer areas are often clumped together and plotted at the same spot due to a lack of accurate information, thereby making the latter more likely to be "crime hotspots". It points to direct discrimination as well, by adding layers of design which filter immigrant colonies and minority settlement areas, stemming from the system's belief that these areas are de facto more likely to be more prone to criminal activities. To add to this, the arbitrariness in how certain crimes and the related information is categorised by individual officers, in the absence of standardised formats or prescribed forms, is further likely to work against marginalised groups.

The use of drones and mobile surveillance vehicles during the pandemic by several states further highlights the need for safeguarding citizen privacy and the protection of data. To monitor the usage of drones, the Centre passed the Unmanned Aircraft System (UAS) Rules in March 2021. These rules failed to provide any safeguards for citizen privacy and the protection of data (Somayajula, 2021). In the recent push for 'smart policing', state police forces have been acquiring and started using technology such as drones and mobile surveillance vehicles. In the 56th Conference of DGs and IGs held in Lucknow in late 2021, Prime Minister Narendra Modi backed setting up a 'High Power Police Technology Mission' under the Union Home Minster (Economic Times, 2021).

The absolute lack of concern for citizens' privacy is implicit in the manner in which these technologies are being used by the police, irrespective of the occurrence of crime in an area. This was apparent in the practice of the Hyderabad police which eventually led to the filing of a PIL in the court by the aggrieved person. An activist, SQ Masood was stopped by the Hyderabad Police in May 2021 while on his way home and asked to remove his mask at the peak of the second wave of the pandemic so the police could take his photo. This was done without any instigation by Masood or the occurrence of any crime, and he was not informed of how his information would be used, where it would be stored or to whom it would be available. Masood went on to file a PIL in the Telangana High Court, which is ongoing. Such actions can have a chilling effect on people's freedom of expression and right to protest.

Even as there is a lack of legal framework regulating such forms of predictive policing, several states have experimented with predictive policing models, notwithstanding the fact that such models have been found to carry inherent biases along the lines of race, ethnicity, etc. in several other countries. Because of these reasons, the German Constitutional Court struck down predictive algorithms for policing in February 2023 (Killeen, 2023), as have US cities such as Santa Cruz (Asher-Schapiro, 2020).

Here are a few examples of predictive policing being used in India:

1. Mumbai Police: In 2018, the Mumbai Police announced that it was planning to implement a predictive policing system to improve law and order in the city. The system was expected to use data analytics to identify crime hotspots and predict criminal activities. The police department had partnered with a private company to develop the system.
2. Telangana Police: In 2019, the Telangana Police launched a new initiative called "Cop Connect," which uses predictive analytics to identify potential crime hotspots and take preventive measures. The system uses data from various sources, including crime records, social media, and CCTV footage, to predict crime patterns.
3. Delhi Police: In 2020, the Delhi Police launched a new initiative called "Prahari" to improve the safety and security of women in the city. The system uses predictive analytics to identify potential crime hotspots and deploy police personnel accordingly. The police department has also developed a mobile app called "Himmat Plus," which allows women to send SOS alerts to the police in case of emergency.

The use of Automated Facial Recognition System (AFRS) software to screen crowds at anti-government rallies is another instance of potential misuse of technology by the police. The deployment of such technology without appropriate safeguards raises the risk of discriminatory targeting of certain groups, particularly minority communities and marginalised groups. Even as the Automated Facial Recognition System (AFRS) software was installed by the police to identify missing children, there have been reports of the software being used to screen crowds at the anti-Citizenship Amendment Act rallies (Al Jazeera, 2019) or those protesting against the farm laws introduced by the government (Parkin, 2021)

1.3.2. Targeted surveillance and discrimination

While mass surveillance has become common in most modern democracies, targeted surveillance of specific individuals or groups by the state and its agencies, such as the police, is rapidly emerging. The recent Pegasus spyware attack by elected governments in India and other countries demonstrated one of many ways targeted surveillance is used to control dissent and access sensitive information. This study aims to understand the forms, impact, and perceptions regarding both mass and targeted surveillance by the police.

Targeted surveillance can also be directed against certain groups or communities, such as De-Notified Tribes (DNTs) in India. Historically considered "criminal" tribes, DNTs were de-criminalised in 1952, but police practices continue to unfairly target members of this community. The Habitual Offenders Act and Prevention of Anti-Social Activities laws provide legal powers to the police to restrict civil liberties, frequently used against DNTs and other vulnerable groups. Reports indicate that persons belonging to the DNT community are treated like criminals, without proper cause, with movement restricted both inside and outside the village, leading to suicide in some cases (Gothoskar, 2017).

Police surveillance may also be more frequently directed against socio-economically vulnerable groups such as Dalits, Adivasis, and religious minorities due to the larger structure of discrimination and criminalisation of these communities within the police system. Reports such as the Status of Policing in India Report series document discriminatory attitudes and perceptions among police personnel, with Muslims, Dalits, and Adivasis more likely to be incarcerated and investigated slower for crimes committed against them. One such example is the Bhima Koregaon case of 2018, where group of activists and intellectuals were arrested on an alleged conspiracy to incite violence at a Dalit commemoration event in Maharashtra. The activists and intellectuals were charged with sedition and other serious offences. The arrests were widely criticised as an attempt to stifle dissent and opposition to the government. It was alleged that the arrests were made based on evidence collected through targeted surveillance of the accused.

Surveillance technologies reinforce pre-existing biases within the technological codes, making it more likely to target racial minorities. In India, a 2021 study by Vidhi Centre for Legal Policy suggests that the Delhi Police's use of facial recognition technology could make Muslims likelier targets (Vipra, 2021).

Surveillance technology is also not always as reliable as it is made out to be. In June 2020 in Detroit, USA, a Black man, Robert Williams, was wrongly convicted of a crime he did not commit due to the inaccuracy of biometric facial recognition technology. Soon after, another Black man, Michael Oliver, was arrested under similar circumstances as Williams (Johnson, 2022). These cases indicated both the racial bias fed into the algorithm because of the lack of diversity in the database (the accuracy was higher amongst white men) as well as the unreliability of the technology itself. Aside from the system reinforcing racial biases, the scientific basis behind some of the tools that are used as evidence in court, such as voice recognition, has also been questioned for its lack of accuracy.

Despite the limitations of technology, such as the inaccuracy of biometric facial recognition technology and the lack of diversity in the database leading to racial bias, Delhi Police considers 80 percent as the threshold for the accuracy of FRT to positively identify suspects (Internet Freedom Foundation, 2022). However, this figure is too low for an official investigation by the police. To illustrate its unreliability, a comparison can be made with FRT technologies being used by tech companies such as Amazon and Microsoft in the USA which, in a 2018 study by the American Civil Liberties Union, was found to have 80 percent accuracy. This technology, the study noted, falsely matched as many as 28 members of the US Congress, and was found to be more unreliable for Blacks and other people of colour (Outlook India, 2022). At least 23 US cities have banned the police use of FRT and passed laws to that effect (Ban Facial Recognition, n.d.).

Targeted surveillance has also been used as a tool to stifle dissent in India. A 2018 report published by the Software Freedom Law Centre (SFLC), India revealed that Indian government has been outsourcing internet monitoring to third parties, including foreign companies, according to RTI information accessed by them. It also revealed that on an average, more than one lakh telephone interception orders are issued by the Central government every year (SFLC, 2018).

1.3.3. Surveillance of the accused

While it is easier to argue in favour of the right to privacy of common people, the issue becomes much more complex when it comes to the right to privacy of individuals who have been convicted of certain crimes. In 2018, the Indian government launched the National Registry of Sexual Offenders, which contains names, addresses, photographs, fingerprints, DNA samples, PAN, and Aadhaar numbers of convicted sex offenders. This list can only be accessed by law enforcement officers with requisite clearance. However, similar practices in other countries have led to dangerous trends. In the year 2000, a newspaper gained access to data from the sex registry of London and published the names and whereabouts of the offenders under its "Name and Shame Campaign." This was followed by a series of mob attacks and lynching of persons named in the registry as well as those mistakenly identified as those named by the campaign (The Guardian, 2000).

In India's current political climate, where mob lynching and vigilante policing are on the rise, such information could potentially create a vigilante state with little regard for due process of law. Furthermore, the registry will store information on the offenders for a period of 15 years. Both the European Court of Human Rights and the European Court of Justice have ruled that storing sensitive personal data for long periods or permanently for "future prevention of crime" is illegal. The argument is that the information is used to vilify offenders even after they have served their sentences (Bhandari, 2018).

These trends in the Indian police, with the backing of the government and perhaps even the common public, to get unhindered access to people's information and sensitive data in the name of public safety and security, remain unchecked and unregulated by the legal apparatus.

In early April 2022, the Parliament passed the controversial Criminal Procedure (Identification) Act, 2022. The Act authorises executive authorities, including the police and prisons departments, to collect, analyse and store biometric and personal data on any person who has been arrested, whether undertrials or convicts. This Act raises concerns of privacy violation of not just the convicted persons, but also the undertrials, who in the Indian legal system are presumed innocent until proven guilty. Concerns have also been raised about the fact that it may even be used to collect the personal information of those apprehended under the various preventive detention laws, thus widening the surveillance net to unprecedented levels, putting potentially everyone at risk of violation of right to privacy. Particularly in the absence of any kind of data protection mechanisms, this Act has potential for wide misuse. The constitutionality of this Act has been challenged in a Public Interest Litigation in the Delhi High Court (Batra, 2022).

1.4. Legal framework and oversight mechanisms for privacy protection in India

Article 12 of the Universal Declaration of Human Rights states that "Everyone has the right to the protection of the law against arbitrary interference with his privacy, family, home or correspondence." In December 2013, the United Nations adopted a resolution titled "The right to privacy in the digital age," which recognised the potential for surveillance and data collection to infringe on privacy and other human rights. The resolution emphasised the need for national legislation, oversight mechanisms, and transparency to protect privacy both online and offline.

In India, the legal mechanism around surveillance has been underdeveloped for some time. While a draft Bill on Right to Privacy was introduced by the Ministry of Personnel, Public Grievances, and Pensions in 2011, it wasn't until 2017 that the Supreme Court declared privacy to be a fundamental right under Article 21 of the Constitution. The court also acknowledged the right to privacy as part of the freedoms guaranteed by Part III of the Constitution.

In 2018, an expert committee chaired by Justice Srikrishna submitted a report on the right to privacy, which included a draft Personal Data Protection Bill. However, when the Bill was introduced to Parliament in 2019, it contained significant changes that led to criticism from Justice Srikrishna. The revised Bill was referred to a Joint Parliamentary Committee, which submitted a report in December 2021 containing 97 amendments, 93 recommendations, and seven dissenting notes (Gupta & Panjiar, 2022). Based on the Committee's report, the Union Government withdrew the Bill in August 2022 (Barik, 2022). In February 2023, the government, in an affidavit submitted to the Supreme Court, stated that it will present the revised Digital Personal Data Protection Bill in Parliament's Budget Session of March 2023 (Bhan, 2023).

Currently, legal recourse against illegal surveillance by individuals or private companies exists, including the ability to file an FIR or approach the Magistrate court. However, legal protections against state surveillance are limited, and there is a lack of adequate national legislation and oversight. The UN Office of the High Commissioner has noted that weak procedural safeguards and ineffective oversight contribute to reduced accountability and that mass surveillance by governments is becoming a dangerous habit. The need for national legislation, oversight mechanisms, and transparency to protect privacy both online and offline is crucial in India.

There are legal remedies available to victims of illegal surveillance by individuals or private companies. The Cyber Cells of state police forces can be approached to report such incidents, and victims of cybercrime can file an FIR under Section 154 of the Criminal Procedure Code, 1973. If the police officer or cell refuses to investigate the complaint, a private complaint can be filed under Section 156 (3) read with Section 190 of the Criminal Procedure Code, 1973, seeking a direction to the police station concerned to investigate the matter.

In cases where illegal surveillance is suspected in contravention of the Indian Telegraph Act, 1955 and Rule 419A of the Indian Telegraph Rules, 1951, or under Section 69 or 69B of the Information Technology Act, 2000, the most effective remedy is to approach the High Court against the government to quash the unlawful order. However, legal remedies for state surveillance are largely absent, making the classification between legal and illegal surveillance difficult.

According to the UN Office of the High Commissioner Report on the Right to Privacy in the Digital Age, a lack of adequate national legislation, weak procedural safeguards, and ineffective oversight reduce accountability, and government mass surveillance is becoming a dangerous habit. An RTI application revealed that the Indian government issues around 7500-9000 telephone interception orders each month on average, and citizens are routinely subjected to government surveillance (Times of India, 2018).

Indian law allows the government to intercept and monitor communication networks under various grounds, but there is no provision for perpetual mass surveillance. Several state-sponsored surveillance systems are in place in India, such as CMS, NATGRID, NETRA, and CCTNS. However, there is a concerning legal vacuum that requires immediate reconsideration.

The right to privacy applies not only to the contents of communications but also to personal development and the ability to communicate parts of ourselves to the outside world. Biometric surveillance technologies are often deployed with a questionable legal basis and breach data protection laws or infringe upon fundamental human rights such as privacy. It is essential to regulate electronic evidence gathering techniques by law enforcement through a warrant-based system subject to relevant laws and oversight.

Legal provisions regulating surveillance in India

India has a complex web of laws, regulations, and procedures that govern surveillance activities, including electronic surveillance, physical surveillance, and interception of communications. Here are some of the key legal provisions regulating surveillance in India:

1. **Indian Telegraph Act, 1885:** This Act authorises the government to intercept or detain any message transmitted by telegraph, to disclose the contents of such messages to authorised persons, and to direct any telegraph officer to perform such duties as may be necessary for these purposes. Section 5(2) of the Act empowers the government to conduct surveillance for the "security of the state" or to prevent "public emergency".

2. **Rules governing surveillance:** The government has also issued various rules and guidelines to regulate surveillance activities, including the Indian Telegraph Rules, 1951, which provide for the interception and monitoring of telegraph messages, and the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which provide for the interception and monitoring of electronic communications under the IT Act.

   Rule 419A of the Indian Telegraph Rules, 1951 lays down the procedure for telephone tapping. It was introduced by way of an amendment in 2007 after the Supreme Court observed the lack of procedure governing telephone tapping in the case People's Union for Civil Liberties v. Union of India (AIR 1997 SC 568).

3. **Information Technology (IT) Act, 2000:** This Act contains provisions for the interception and monitoring of electronic communications, including emails, telephone conversations, and other forms of online communication. Section 69 of the IT Act allows the government to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient to do so in the interest of the sovereignty, integrity, defence, security or economic interests of India.

   Whereas Section 69 deals with surveillance of internet data, Section 69B deals with the surveillance of Internet metadata. Metadata is any data that gives information about other data.

4. **Code of Criminal Procedure (CrPC), 1973:** The CrPC authorises law enforcement agencies to conduct surveillance in the course of investigating criminal offences. Section 91 of the CrPC allows the police to issue a summons or a search warrant for the production of any document, electronic record or other thing necessary for the purposes of any investigation, inquiry or trial.

In addition to these laws, license agreements such as the Unified Access Service License (UASL), Internet Service License (ISL), and the Unified License (UL) between the Department of Telecommunications and telecommunications service providers also enable the government to receive assistance from telecommunication service providers in conducting surveillance. Licensees must also provide, in the interests of security, "suitable monitoring equipment as per the requirement of the DOT or law enforcement agencies".

Conclusion

Surveillance is a complex issue that involves both the state and private sectors, with the boundaries often overlapping. Private surveillance aims to capture personal information for profiling consumeristic behaviour, while state surveillance proclaims to employ these technologies for reasons of maintaining order in society. However, the unchecked use of surveillance by the state can take nefarious forms, being used for controlling any kind of dissent, constricting people's freedoms and rights, and targeting specific groups or communities. The power dynamic between those observing and those being observed highlights the potential for inducing internalised behavioural modification, creating a sense of constant monitoring and the fear of potential consequences for non-conformity. Therefore, the right to privacy is a central concern when it comes to state surveillance. While the use of CCTV cameras by private companies and individuals is becoming increasingly widespread in India, research worldwide suggests that their presence has little to no impact on crimes. Despite this, a popular narrative supports the installation of more cameras to improve law-and-order, among both the public and politicians.

While there are concerns about the use of facial recognition technology, closed-circuit television, and other surveillance-based intelligence-gathering projects, there is also apprehension about the Aadhaar identification project, which collects biometric details and demographic information. With the growing threat of cybercrimes and the availability of sensitive data online, citizen-centric data protection regulations are necessary. There is a need for more transparency, oversight, and accountability in India's surveillance framework to protect citizens' privacy rights.

Another cause for concern is the lack of transparency, data reliability and privacy violations. The deployment of predictive policing strategies and the usage of historical crime data to inform such strategies are problematic, given the inherent biases in the data collection process. The lack of safeguards for citizen privacy and data protection, as exemplified by the recent rules for unmanned aircraft systems, highlights the need for regulation and accountability in the use of surveillance technology by state police forces. There is a pressing need for greater transparency and accountability to be built into the design and implementation of such technologies in India.

References

Al Jazeera. (2022, January 25). Privacy Fears as India Police Use Facial Recognition at Rally. Accessed January 25, 2022, from https://www.aljazeera.com/news/2019/12/30/privacy-fears-as-india-police-use-facial-recognition-at-rally.

Asher-Schapiro, A. (2020, June 25). California City Bans Predictive Policing in US First. *Thomson Reuters.* Retrieved from: https://www.reuters.com/article/us-usa-police-tech-trfn-idUSKBN23V2XC.

Ban Facial Recognition. (n.d.). *Fight for the Future.* Retrieved February 17, 2023, from https://www.banfacialrecognition.com/

Barik, S. (2022, August 4). Government Withdraws Data Protection Bill to Bring Revamped, Refreshed Regulation. New Delhi, *The Indian Express.* Retrieved from: https://indianexpress.com/article/india/government-withdraws-data-protection-bill-8068257/.

Batra, S. (2022, April 20). PIL in Delhi HC Challenges Criminal Procedure (Identification) Act, 2022. *The Print.* Retrieved from: https://theprint.in/india/pil-in-delhi-hc-challenges-criminal-procedure-identification-act-2022/923771/.

Bhan, I. (2023, February 1). Budget 2023: Digital Personal Data Bill to be Introduced in Second Half, Says Govt to SC. *The Economic Times.* Retrieved from: https://brandequity.economictimes.indiatimes.com/news/digital/digital-personal-data-bill-to-be-introduced-in-second-half-of-budget-session-govt-to-sc/97515750.

Bhandari, V. (2018, September 25). Why India's Registry of Sex Offenders May do More Harm Than Good. ***Scroll.*** Retrieved from https://scroll.in/article/895346/why-indias-registry-of-sex-offenders-may-do-more-harm-than-good.

Chandran, R. (2023, January 14). Police in India Are Expanding Their Surveillance Reach by Tapping into Private Security Systems. *Scroll.* Retrieved from: https://scroll.in/article/1041633/police-in-india-are-expanding-their-surveillance-reach-by-tapping-into-private-security-systems.

Economic Times. (2021, November 22). PM Modi Backs Tech-Driven High-Power Police Technology Mission. Accessed on 25th January 2022 Retrieved from https://government.economictimes.indiatimes.com/news/technology/pm-modi-backs-tech-driven-high-power-police-technology-mission/87841341.

Gothoskar, S. (2017, December 13). Police's Continued Victimisation of 'Denotified' Tribal Communities Can No Longer Go Unchallenged. The Wire. Retrieved from: https://thewire.in/politics/polices-continued-victimisation-denotified-tribal-communities-can-no-longer-go-unchallenged.

Gupta, A. and Panjiar, T. (2022, August 5). Withdrawal of Personal Data Protection Bill: Who Benefits from The Delay? *The Indian Express.* Retrieved from: https://indianexpress.com/article/opinion/columns/withdrawal-of-personal-data-protection-bill-who-benefits-from-delay-8071067/.

Internet Freedom Foundation (2022, August 17). Delhi Police's Claim That FRT is Accurate With A 80% Match Are 100% Scary. Retrieved from: https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/.

Johnson, K. (2022, March 7). The Hidden Role of Facial Recognition Tech In Many Arrests. *Wired.* Retrieved from: https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/.

Kemp, Simon (2022, February 15). Digital 2022: India. *Kepios.* Retrieved from: https://datareportal.com/reports/digital-2022-india.

Khaira, R. (2018, January 3). Rs 500, 10 Minutes, And You Have Access to Billion Aadhaar Details. Jalandhar, *Tribune India.* Retrieved from: https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

Killeen, M. (2023, February 16). German Constitutional Court Strikes Down Predictive Algorithms for Policing. *Euractiv.* Retrieved from: https://www.euractiv.com/section/artificial-intelligence/news/german-constitutional-court-strikes-down-predictive-algorithms-for-policing/.

Marda, V. and Narayan, S. (2020). Data in new Delhi's Predictive Policing System. In *FAT* '20: Proceedings of ACM Conference on Fairness, Accountability, and Transparency, January 27–30, 2020, Barcelona, Spain.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3351095.3372865.

Mason, M.K. (2023). Foucault and His Panopticon. Retrieved from: https://www.moyak.com/papers/michel-foucault-power.html.

McMullan, T. (2015, July 23). What Does the Panopticon Mean in the Age of Digital Surveillance? *The Guardian.* Retrieved from: https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham.

Mukul, P. & Sasi, A. (2021, August 28). Facial Recognition Spreads, Concern Over Absence of Data Protection Law. New Delhi, *The Indian Express.* Retrieved from: https://indianexpress.com/article/india/facial-recognition-technology-airports-railway-station-national-crime-records-bureau-7474624/.

Outlook India. (2022, August 18). Explained: Why Delhi Police's Facial Recognition Mechanism to Nab Accused Raises Concerns. Retrieved from: https://www.outlookindia.com/national/delhi-police-s-80-per-cent-match-of-facial-recognition-to-nab-accused-raises-concern-finds-rti-news-217182.

Parkin, B. (2021, January 28). Indian police Use facial Recognition in Search for Farmer Protestors. *Financial Times*. Retrieved from https://www.ft.com/content/044add20-7129-44a8-bc9d-92919a73d049.

Press Trust of India (2019, December 19). Anti-CAA Stir, Delhi Police Use Drone to Keep Track of Protestors. New Delhi, *India Today*. Retrieved from: https://www.indiatoday.in/amp/india/story/anti-caa-stir-delhi-police-use-drone-to-keep-track-of-protesters-1629729-2019-12-19.

Software Freedom Law Centre and World Wide Web Foundation (2018). Communications Surveillance in India. Retrieved from: https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.

Somayajula, D. (2021, August 4). Drone Policing During Covid Exposes India's Need for Data Protection Law. *The Print*. Retrieved from: https://theprint.in/opinion/drone-policing-during-covid-exposes-indias-need-for-data-protection-law/708714/.

Steinmetz, J. (2020, March 6). Increased Surveillance in Public Spaces is Changing Not Just How We Act, But Also How We Think. *Scroll.in*. Retrieved from: https://scroll.in/article/954946/increased-surveillance-in-public-spaces-is-changing-not-just-how-we-act-but-also-how-we-think.

The Guardian. (2000, August 4). News of the World Suspends Name-and-Shame Campaign. Accessed January 25, 2022 from https://www.theguardian.com/society/2000/aug/04/childprotection.

The Times of India (2018, December 22). RTI Reveals 9.000 Phones, 500 Emails Intercepted Each Month Under UPA. Retrieved from: https://timesofindia.indiatimes.com/india/upa-govt-intercepted-7500-9000-phones-every-month-rti/articleshow/67207969.cms.

The World Bank Data (2020). 'Individuals using the Internet (% of Population)- India'. Retrieved from: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IN.

Vincent, P.L. (2021, December 21). Delhi to Get 1.4 Lakh More CCTV Cameras, Says Arvind Kejriwal. New Delhi, *The Telegraph Online*. Retrieved from: https://www.telegraphindia.com/india/delhi-to-get-1-4-lakh-more-cctv-cameras-says-arvind-kejriwal/cid/1841803.

Vipra, J. (2021). The Use of Facial Recognition Technology for Policing in Delhi: An Empirical Study of Potential Discrimination. Working Paper, Vidhi Centre for Legal Policy. Retrieved from: https://vidhilegalpolicy.in/wp-content/uploads/2021/08/The-Use-of-Facial-Recognition-Technology-for-Policing-in-Delhi-compressed.pdf.

Zuboff, S. (2018). 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power'. *Public Affairs*.

Chapter 2:

Surveillance Trends in India: Official Data Analysis

Key findings

- The number of CCTV cameras available with the police, including those from private establishments, institutions and societies, is significantly lower than the overall number of CCTV cameras within the cities.
- There is no statistically significant relationship between the CCTVs available with police stations and the rates of total cognisable crimes, murder, and auto/motor theft from 2016 to 2020.
- Even amongst states that have a high registration of cybercrimes, the infrastructural capacity of the state to handle such cases does not match up to the high volumes of registration of cybercrimes.
- The chargesheeting and conviction rates for cybercrime offences across the country is lower than the chargesheeting and conviction rates for total cognisable IPC and SLL crimes. In Assam, for instance, despite 6096 persons being arrested for cybercrimes in 2021, the chargesheeting rate was about 16 percent and the conviction rate was 2.2 percent.
- Overall, in 13 states and UTs, the coverage of CCTV in police stations as reported in the RTI data is lower than as reported in the BPRD data.

CHAPTER 2

Surveillance Trends in India: Official Data Analysis

Official data on police surveillance in India is limited and difficult to obtain, resulting in little transparency and accountability in its implementation. The Indian Telegraph Act and the Information Technology Act provide legal provisions for surveillance by law enforcement agencies, but their scope and impact on civil liberties are unclear due to the lack of transparency. Civil society organisations and researchers have attempted to gather and analyse data on surveillance practices, which have revealed widespread use of surveillance technologies, such as facial recognition systems and electronic communications interception. However, much remains unknown about the extent and impact of police surveillance in India.

The limited availability of information makes it challenging to conduct a scientific analysis of surveillance data. For instance, to study the effect of CCTVs on crime rates, one requires micro-level data on the coverage of CCTVs by the police or state departments, comparable micro-level data on the number of crime incidents in that location within a given time period, and information on the level of police or state access to private CCTV cameras. However, in India, this information is only available at a district or state level without comparable time periods, making it difficult to draw any correlation between the two. Additionally, unreported crimes further complicate the analysis. Aside from this, difficulties also arise when we consider that several cases of crimes go unreported (Tiwari & Rao, 2016). Due to such limitations, it was not possible to conduct correlational analysis of the official data. Nevertheless, this chapter presents the larger data trends that have emerged from official reports.

This chapter presents an analysis of trends in surveillance practices in India, drawing from multiple data sources including the official data published by the Bureau of Police Research and Development (BPRD) and National Crime Records Bureau (NCRB). In addition to this, the chapter also uses data compiled through Right to Information (RTI) applications filed by the research team at both the state and central levels. To provide further insight into the extent of surveillance practices, the chapter also references the RTI data compiled by the Internet Freedom Foundation (IFF) on the use of Facial Recognition Technology (FRT) by various government departments. By combining data from multiple sources, this chapter sheds light on the various forms and extent of surveillance in India.

This chapter has been divided into the following sections:

- **Section 1** includes an analysis of the crime data vis-à-vis the available data on CCTV coverage in states to test for a possible correlation between the two
- **Section 2** looks at the capacity of the states to deal with cybercrimes and conduct social media monitoring

- **Section 3** looks at the cybercrime laws and the IT Act provisions as a tool to curb dissent in the country
- **Section 4** analyses and presents data on the CCTV coverage of police stations in India from both the BPRD reports as well as information gathered through RTI applications
- **Section 5** presents data from private sources on the extent of installation and use of FRT by government departments at the state and central levels.

2.1. CCTVs and crime data

Despite the aforementioned limitations, a preliminary analysis of the correlation between CCTV coverage and crime rates at the state level was conducted to identify any emerging trends that could be examined in further detail through a micro-level study.

The available information on CCTV coverage comes from two sources: city-level data collected from news reports and CCTV data available to the police, as published by the Bureau of Police Research and Development (BPRD) at the state level. While the former provides a more comprehensive dataset, the latter is more pertinent for this analysis as it indicates the number of CCTV systems installed in private establishments, institutions, and government buildings that are accessible to the police.

Table 2.1: City-wise CCTV camera coverage in India (Private sources)

Name of city	Number of CCTV cameras	Cameras per square mile
Delhi	436,600	1446.03
Chennai	282,126	614.56
Hyderabad	440,299	157.14
Mumbai	63,598	145.13
Indore	200,600	133.29
Lucknow	13,440	99.74
Kolkata	22,316	56.28
Bangalore	14,927	17.61
Kanpur	1,405	9.01
Pune	17,724	6.07
Kochi	982	5.78
Jaipur	1,000	5.55
Surat	4,655	2.65
Ahmedabad	6,461	2.06
Thrissur	269	0.23
Kozhikode	186	0.21

Source: *Comparitech Data, July 11, 2022*

Table 2.2: State-wise number of CCTV cameras available with the police, including those from private establishments (Government sources)

Name of the state	Number of CCTVs available with the police as on 01.01.2022*	Cameras per square mile available with the police*
Andhra Pradesh	14,770	0.2
Arunachal Pradesh	99	0.0**
Assam	558	0.0**
Bihar	127	0.0**
Chhattisgarh	3,140	0.1
Goa	524	0.4
Gujarat	14,354	0.2
Haryana	2,758	0.2
Himachal Pradesh	2,517	0.1
Jharkhand	749	0.0**
Karnataka	1,611	0.0**
Kerala	2,092	0.1
Madhya Pradesh	32,031	0.3
Maharashtra	35,292	0.3
Manipur	222	0.0**
Meghalaya	188	0.0**
Mizoram	730	0.1
Nagaland	32	0.0**
Odisha	780	0.0**
Punjab	8,058	0.4
Rajasthan	6,529	0.0**
Sikkim		0.0**
Tamil Nadu	22,912	0.5
Telangana	282,558	6.5
Tripura	316	0.1
Uttar Pradesh	3,066	0.0**
Uttarakhand	965	0.0**
West Bengal	7,772	0.2
A&N Islands	597	0.2
Chandigarh	329	7.5
D&N Haveli and Daman and Diu	204	0.9
Delhi	10,218	17.8

Jammu and Kashmir and Ladakh	606	0.0**
Lakshadweep	308	0.0**
Puducherry	103	0.5
All India	**456,807**	**0.4**

**The CCTV data of private establishments, institutions and societies including government establishments and were also shown in the data.*

***Note: Zero denotes extremely low values because of small number of CCTVs available with the police compared to the geographical size of the states.*

Source: *CCTV availability- Data on Police Organisations, 2022, BPRD. Area of states: Statistics Times Website*

Tables 2.1 and 2.2 above clearly indicate that the number of CCTV cameras available with the police, including those from private establishments, institutions and societies, is significantly lower than the actual overall number of CCTV cameras within the cities, as reported by an international study conducted in 2022. For example, as of 2022, Chennai reportedly has around 2.8 lakh cameras, whereas in the entire state of Tamil Nadu, the police had access to just about 22,912 cameras in 2021. This includes the cameras used by the police for traffic management, investigation, and security purposes.

While an exact comparison between the two datasets is not viable due to differences in the years to which the data pertains, the extent of the difference suggests that there is a high probability of the police not having access to a large number of CCTV cameras owned by private individuals or companies. If the contrary were true, then in the case of Delhi, for instance, the number of CCTV cameras was around 10,000 in 2021 according to BPRD, while private sources suggest that the number of cameras in 2022 is more than four lakhs, an exponential increase of more than 40 times. Thus, there is a high likelihood that the police have access to only a fraction of the actual overall number of CCTV cameras at a state or even a city level.

Despite the limitations of a macro-level analysis, we attempted to identify any discernible patterns in crime vis-à-vis the availability of CCTV cameras with the police. In order to understand the trends, it was important to look at time-series data; therefore, we compared the data for a period of five years, from 2016 to 2020.

Table 2.3: State-wise data on actual number of CCTV cameras available with the police and number of CCTVs per police station over a five-year period

	2020		2019		2018		2017		2016	
	Number of CCTV cameras available in police stations	CCTVs per police station	Number of CCTV cameras available in police stations	CCTVs per police station	Number of CCTV cameras available in police stations	CCTVs per police station	Number of CCTV cameras available in police stations	CCTVs per police station	Number of CCTV cameras available in police stations	CCTVs per police station
Andhra Pradesh	20968	20.5	19918	19.5	14770	14.4	1102	1.1	3553	3.5
Arunachal Pradesh	50	0.5	33	0.4	0	0.0	71	0.8	71	0.7
Assam	558	1.6	551	1.6	673	2.0	673	2.0	430	1.2
Bihar	127	0.1	127	0.1	125	0.1	125	0.1	125	0.1

Chhattisgarh	2296	5.0	1035	2.3	693	1.6	509	1.2	71	0.2
Goa	70	1.6	74	1.7	151	3.5	151	3.5	151	5.8
Gujarat	13451	18.4	13045	18.3	7361	10.4	7361	10.4	1168	1.8
Haryana	1934	5.0	1200	3.1	925	2.6	1235	3.8	425	1.4
Himachal Pradesh	1211	8.2	1096	7.4	749	5.8	315	2.5	292	2.5
Jharkhand	1103	2.0	587	1.1	587	1.1	587	1.1		0.0
Karnataka	1586	1.5	1536	1.5	2997	2.9	2773	2.6	1066	1.1
Kerala	965	1.7	915	1.7	592	1.1	526	1.0	908	1.7
Madhya Pradesh	31199	27.9	24733	22.1	21206	19.0	8263	7.5	3031	2.8
Maharashtra	24076	20.7	39587	34.0	39587	34.0	11777	10.1	5224	4.5
Manipur	64	0.8	15	0.2	51	0.6	51	0.6	155	1.6
Meghalaya	187	2.5	201	2.7	158	2.2	129	2.1	126	3.2
Mizoram	384	8.7	224	5.3	224	5.9	186	4.9	189	5.0
Nagaland	88	1.0	88	1.0	0	0.0	32	0.4	32	0.4
Odisha	780	1.2	865	1.4	865	1.4	790	1.2	702	1.1
Punjab	7601	17.7	2399	5.6	1801	4.3	4576	10.7	33467	83.9
Rajasthan	5432	6.1	4838	5.4	4838	5.4	2287	2.6	2153	2.5
Sikkim		0.0	8	0.3	7	0.2	7	0.2	7	0.2
Tamil Nadu	150254	66.1	47375	23.8	40112	19.9	4924	2.5	844	0.5
Telangana	282558	336.0	282558	337.2	275528	338.1	214952	272.8	841	1.2
Tripura	316	3.9	355	4.3	313	3.9	72	0.9	52	0.6
Uttar Pradesh	4965	3.0	2135	1.3	2134	1.4	2134	1.4	1048	0.7
Uttarakhand	965	6.1	965	6.1	933	5.9	562	3.6	368	2.4
West Bengal	7663	12.1	6005	9.5	3825	6.4	4109	7.0	3899	6.7
A&N Islands	126	5.3	36	1.5	36	1.5	36	1.5	28	1.2
Chandigarh	350	19.4	389	22.9	701	41.2	326	19.2	358	21.1
D&N Haveli and Daman and Diu	152	19.0	126	21.0	126	18.0	109	18.2	63	9.0
Delhi	7194	34.4	6897	33.0	5332	25.5	4390	22.6	4017	20.9
Jammu and Kashmir and Ladakh	240	1.0	201	0.8	26	0.1	180	0.8	180	0.8
Lakshadweep		0.0		0.0	0	0.0	45	2.8	43	2.7
Puducherry	103	1.9	103	1.9	103	1.9	103	1.9	103	1.9
All India	**569016**	**33.0**	**460220**	**27.3**	**427529**	**25.8**	**275468**	**16.8**	**65190**	**4.2**

Source: *Data on Police Organisations, (2017-2021) BPRD*

The following crime data for the years 2016-2020 has been statistically correlated with the data on CCTVs available with the police in this analysis:

1. Total cognisable crime rate (IPC and SLL): This indicator was used to examine if there is any correlation between the presence of CCTV cameras and the overall reported crime rates over the years.
2. Murder rate: As per criminologists, the rate of murder is one of the few types of violent and serious crime that has a high reporting rate. Thus, this indicator was used to examine if CCTV cameras have any impact on violent crimes.
3. Auto/motor vehicles theft rate: This indicator was selected as it has a high likelihood of near-accurate reporting amongst non-violent crimes. Additionally, international micro-level studies on the impact of CCTVs on crime have suggested that CCTVs act as a limited deterrent against auto theft (Piza, 2018). This hypothesis was tested in the Indian context with the available data.

Table 2.4: State-wise number of CCTVs per police station vis-à-vis rate of total cognisable crimes (IPC and SLL) (2016-20 average)

State	CCTVs per police station (2016-2020 average)	Rate of total cognisable crimes (IPC and SLL) (2016-2020 average)
Andhra Pradesh	11.8	308.7
Arunachal Pradesh	0.5	191.0
Assam	1.7	350.4
Bihar	0.1	212.6
Chhattisgarh	2.0	340.2
Goa	3.2	231.1
Gujarat	11.9	688.5
Haryana	3.2	646.1
Himachal Pradesh	5.3	262.5
Jharkhand	1.0	155.6
Karnataka	1.9	260.4
Kerala	1.4	1623.6
Madhya Pradesh	15.9	486.5
Maharashtra	20.7	403.4
Manipur	0.8	131.0
Meghalaya	2.5	122.7
Mizoram	6.0	229.0
Nagaland	0.6	74.8
Odisha	1.3	261.0
Punjab	24.4	238.5
Rajasthan	4.4	344.8
Sikkim	0.2	132.4
Tamil Nadu	22.6	869.1

Telangana	257.0	354.5
Tripura	2.7	126.7
Uttar Pradesh	1.6	264.6
Uttarakhand	4.8	298.2
West Bengal	8.3	199.9
A&N Islands	2.2	713.9
Chandigarh	24.8	337.8
D&N Haveli and Daman and Diu	17.0	69.5
Delhi	27.3	1270.9
Jammu and Kashmir and Ladakh	0.7	204.6
Lakshadweep	1.1	160.0
Puducherry	1.9	331.3
All India	**21.4**	**323.9**

Source: *Data on Police Organisations, (2017-2021) BPRD; Crime in India (2016-2020), NCRB*

Table 2.5: State-wise number of CCTVs per police station vis-à-vis rate of murder (2016-20 average)

State	CCTVs per police station (2016-2020 average)	Rate of murder (2016-2020 average)
Andhra Pradesh	11.8	1.9
Arunachal Pradesh	0.5	4.1
Assam	1.7	3.5
Bihar	0.1	2.6
Chhattisgarh	2.0	3.4
Goa	3.2	1.8
Gujarat	11.9	1.6
Haryana	3.2	3.8
Himachal Pradesh	5.3	1.3
Jharkhand	1.0	4.4
Karnataka	1.9	2.1
Kerala	1.4	0.9
Madhya Pradesh	15.9	2.4
Maharashtra	20.7	1.8
Manipur	0.8	2.1
Meghalaya	2.5	2.9
Mizoram	6.0	2.2
Nagaland	0.6	1.4

Odisha	1.3	3.1
Punjab	24.4	2.4
Rajasthan	4.4	2.1
Sikkim	0.2	2.1
Tamil Nadu	22.6	2.2
Telangana	257.0	2.3
Tripura	2.7	3.4
Uttar Pradesh	1.6	1.9
Uttarakhand	4.8	1.7
West Bengal	8.3	2.1
A&N Islands	2.2	2.3
Chandigarh	24.8	1.7
D&N Haveli and Daman and Diu	17.0	1.2
Delhi	27.3	2.4
Jammu and Kashmir and Ladakh	0.7	1.1
Lakshadweep	1.1	0.3
Puducherry	1.9	2.0
All India	**21.4**	**2.2**

Source: *Data on Police Organisations, (2017-2021) BPRD; Crime in India (2016-2020), NCRB*

Table 2.6: State-wise number of CCTVs per police station vis-à-vis rate of auto/motor thefts (2016-20 average)

State	CCTVs per police station (2016-2020 average)	Rate of auto/motor thefts (2016-2020 average)
Andhra Pradesh	11.8	8.0
Arunachal Pradesh	0.5	15.1
Assam	1.7	13.6
Bihar	0.1	15.2
Chhattisgarh	2.0	10.4
Goa	3.2	12.0
Gujarat	11.9	11.5
Haryana	3.2	58.0
Himachal Pradesh	5.3	3.6
Jharkhand	1.0	11.9
Karnataka	1.9	14.8
Kerala	1.4	3.4
Madhya Pradesh	15.9	19.2
Maharashtra	20.7	18.7

Manipur	0.8	22.0
Meghalaya	2.5	5.8
Mizoram	6.0	12.2
Nagaland	0.6	11.3
Odisha	1.3	7.5
Punjab	24.4	9.7
Rajasthan	4.4	26.1
Sikkim	0.2	1.7
Tamil Nadu	22.6	7.6
Telangana	257.0	9.8
Tripura	2.7	3.9
Uttar Pradesh	1.6	13.2
Uttarakhand	4.8	8.1
West Bengal	8.3	3.4
A&N Islands	2.2	1.7
Chandigarh	24.8	46.3
D&N Haveli and Daman and Diu	17.0	3.0
Delhi	27.3	201.3
Jammu and Kashmir and Ladakh	0.7	7.1
Lakshadweep	1.1	4.1
Puducherry	1.9	18.3
All India	**21.4**	**16.8**

Source: *Data on Police Organisations, (2017-2021) BPRD; Crime in India (2016-2020), NCRB*

For this analysis, we calculated the correlation coefficient between the number of CCTV cameras per police station (considered as the independent variable) and the rates of crimes (considered as dependent variables) for each of the above indicators. This was done to determine if there is a statistical impact of CCTV coverage on the rates of crimes.

The hypothesis being tested is that in states where the police have a higher number of CCTV cameras per police station, the rates of crime would be lower, and the rates of crimes should decrease over the years with an increase in the availability of CCTV cameras with the police. Conversely, the null hypothesis is that there is no relationship between the number of CCTVs per police station and the rate of total cognisable crime, murder, or auto/motor theft.

We also calculated the p-values, or the asymptotic significance value (2-sided), to assess the statistical significance of the results. P-value is statistical tool used to test whether the difference or correlation between variables is significant or simply by chance. If the p-value is small (less than 0.05) it means that the data is unlikely to have occurred by chance alone and the correlation can be considered to be statistically significant. A p-value higher than 0.05, on the other hand, means that there is greater likelihood of the correlation occurring by chance, and that the correlation is not statistically significant.

The results of the analysis are presented below:

Table 2.7: Correlation coefficients and p values of CCTVs per police station vis-à-vis rate of total cognisable crimes (IPC and SLL)

Year	Correlation coefficient	P value
2020	0.13	0.43
2019	0.06	0.74
2018	0.04	0.82
2017	0.03	0.88
2016	-0.02	0.92
2016-2020 average	**0.05**	**0.76**

Independent variable: CCTVs per police station; Dependent variable: Rate of total cognisable crimes (IPC and SLL)
All data is state-wise.

Table 2.8: Correlation coefficients and p values of CCTVs per police station vis-à-vis rate of murder

Year	Correlation coefficient	P value
2020	-0.004	.983
2019	-0.01	.953
2018	-0.08	0.67
2017	-0.03	0.86
2016	-0.05	0.79
2016-2020 average	**-0.02**	**0.91**

Independent variable: CCTVs per police station; Dependent variable: Rate of murder All data is state-wise.

Table 2.9: Correlation coefficients and p values of CCTVs per police station vis-à-vis rate of auto/motor thefts

Year	Correlation coefficient	P value
2020	0.05	0.80
2019	0.03	0.84
2018	0.02	0.89
2017	0.02	0.89
2016	0.18	0.31
2016-2020 average	**0.05**	**0.79**

Independent variable: CCTVs per police station; Dependent variable: Rate of murder All data is state-wise.

As indicated by the p values greater than 0.05 for all variables, there is no statistically significant relationship between the CCTVs available with police stations and the rates of total cognisable crimes, murder, and auto/motor theft from 2016 to 2020. In other words, the number of CCTV cameras available with the police does not appear to have an impact on the rate of the above-mentioned crimes.

Several studies conducted in India have examined the correlation between CCTV cameras and crime rates, but their findings have been mixed. For instance, a study conducted in Delhi found that CCTV cameras installed in high-crime areas had a significant impact on reducing crime rates, with crime rates decreasing by up to 44 percent in areas with cameras. The presence of cameras acted as a deterrent to potential offenders (Mishra & Gupta, 2011). However, another study conducted in Mumbai found no significant correlation between CCTV cameras and crime rates. While CCTV cameras may help in the detection of crimes, they did not appear to have a significant impact on reducing crime rates (Singh & Bhandari, 2011). Similarly, a study conducted in Chennai also found no significant correlation between CCTV cameras and crime rates. While CCTV cameras may assist in detecting crimes, they did not appear to have a significant impact on reducing crime rates (Jaishankar & Kumar, 2010).

2.2. Cybercrime and social media monitoring capacity of states

Most states in India have established dedicated units or police stations for investigating cybercrimes. They have also set up social media monitoring cells under existing frameworks like the Crime and Criminal Tracking Network and Systems (CCTNS). The primary goal of these cells is to monitor and prevent the spread of fake posts, inflammatory comments, and inappropriate photos and videos on social media platforms such as Facebook, Twitter, Instagram, and WhatsApp (Selvaraj, 2022).

Table 2.10: State-wise number of cybercrime cells, police stations and social media monitoring cells as of 2021

State	Number of cybercrime police stations	Number of cybercrime cells	No. of social media monitoring cells
Andhra Pradesh	3	3	1
Arunachal Pradesh	1	0	1
Assam	0	3	1
Bihar	1	48	48
Chhattisgarh	1	29	0
Goa	1	1	1
Gujarat	24	5	0
Haryana	8	40	27
Himachal Pradesh	1	1	1
Jharkhand	7	15	6
Karnataka	8	1	31
Kerala	19	19	1
Madhya Pradesh	1	11	1
Maharashtra	46	49	41
Manipur	1	10	9
Meghalaya	1	11	1
Mizoram	1	0	1
Nagaland	1	12	1
Odisha	15	34	0
Punjab	2	28	24
Rajasthan	2	15	3

Sikkim	0	1	0
Tamil Nadu	46	47	1
Telangana	3	24	18
Tripura	0	1	1
Uttar Pradesh	18	79	1
Uttarakhand	2	13	13
West Bengal	31	39	2
A&N islands	0	1	1
Chandigarh	0	1	1
D&N Haveli and Daman & Diu	0	3	0
Delhi	15	0	1
Jammu and Kashmir	2	0	1
Ladakh	0	2	1
Lakshadweep	0	1	1
Puducherry	1	1	0
All India	**262**	**548**	**241**

Source: *Data on Police Organisations, 2022, BPRD*

Based on the data presented, Maharashtra, UP, and Tamil Nadu have the highest number of specialised cells or police stations dedicated to cybercrime investigation, while Bihar, Maharashtra, and Karnataka have the highest number of social media monitoring cells. However, state-wise comparisons of reported rates of cybercrime are difficult due to variations in reporting and registration of crimes across states (Table 2.10).

Table 2.11: Caseload of cybercrimes on specialised police stations and units as of 2021

State	Rate of total cybercrimes	No. of total cybercrimes	Number of cybercrimes per cybercrime police station/ unit
Andhra Pradesh	3.5	1875	312.5
Arunachal Pradesh	3.1	47	47.0
Assam	13.8	4846	1615.3
Bihar	1.1	1413	28.8
Chhattisgarh	1.2	352	11.7
Goa	2.3	36	18.0
Gujarat	2.2	1536	53.0
Haryana	2.1	622	13.0
Himachal Pradesh	0.9	70	35.0
Jharkhand	2.5	953	43.3
Karnataka	12.1	8136	904.0
Kerala	1.8	626	16.5
Madhya Pradesh	0.7	589	49.1

Maharashtra	4.5	5562	58.5
Manipur	2.1	67	6.1
Meghalaya	3.2	107	8.9
Mizoram	2.5	30	30.0
Nagaland	0.4	8	0.6
Odisha	4.4	2037	41.6
Punjab	1.8	551	18.4
Rajasthan	1.9	1504	88.5
Sikkim	0.0	0	0.0
Tamil Nadu	1.4	1076	11.6
Telangana	27.3	10303	381.6
Tripura	0.6	24	24.0
Uttar Pradesh	3.8	8829	91.0
Uttarakhand	6.3	718	47.9
West Bengal	0.5	513	7.3
A&N islands	2.0	8	8.0
Chandigarh	1.2	15	15.0
D&N Haveli and Daman & Diu	0.5	5	1.7
Delhi	1.7	356	23.7
Jammu & Kashmir	1.1	154	77.0
Ladakh	1.7	5	2.5
Lakshadweep	1.5	1	1.0
Puducherry	0.0	0	0.0
All India	**3.9**	**52,974**	**65.4**

Source: *Data on Police Organisations, 2022, BPRD; Crime in India, 2021, NCRB*

An indicative analysis of case load on specialised cybercrime police stations/units suggests that, on average, each unit handles over 65 cases of cybercrime at the national level. Interestingly, the states with the highest reported rates of cybercrime also have the highest caseloads per unit, including Assam (over 1,600 cases per unit), Karnataka (over 900 cases per unit), and Telangana (about 380 cases per unit) (Table 2.11). However, as with data on most other cases of crimes, a state-wise comparison is not feasible because of the huge variation in the rate of registration of these crimes across states. Thus, a higher rate of cybercrime could simply be an indication of better reporting and registration of the crime in a particular state, while a lower rate could indicate poorer registration in another.

The data suggests that even amongst states that have a high registration of cybercrimes, the infrastructural capacity of the state to handle such cases does not match up to the high volumes of registration of cybercrimes. For instance, Assam, which has the second-highest cybercrime rate in the country, next only to Telangana, has only three cybercrime cells and no cybercrime police stations.

On the other hand, troublingly, some states have an unusually high number of social media monitoring cells. In a context where the state limitations of surveillance are not properly legally defined and in the absence of data protection laws, such cells presumably function without any kind of constitutional or judicial oversight, thus providing them wide discretion to conduct digital surveillance of citizens. Noteworthy states in this regard are Bihar, Maharashtra, Karnataka, Haryana and Punjab.

Further, whether with respect to the cybercrime cells/police stations or the social media monitoring cell, it is important to note that these numbers only refer to reported cases and physical infrastructure, and do not necessarily reflect the actual number of cybercrime cases or the availability and capacity of trained personnel for investigation. Additionally, the quality and quantity of human resources for cybercrime investigation, including personnel training, is a critical aspect not reflected in this data.

2.3. Cybercrime laws and IT Act laws as a tool for controlling dissent

Given the increasing threat of cybercrime, there is a growing need to build specialised physical and human infrastructure to tackle it. However, we must also ensure that this infrastructure is not used as a surveillance mechanism by the police and the state, infringing upon the right to privacy and freedom of speech of individuals. There have been frequent reports of activists and journalists being arrested over social media posts that are critical of the party in power, a political leader, or a particular government policy. For example, Mohammed Zubair, the co-founder of a fact-checking website AltNews, was arrested in June 2022 for a Twitter post that he made four years ago in 2018. Numerous other cases of arrests over critical social media posts have been reported from the states of Assam, erstwhile state of Jammu and Kashmir, Manipur, and Uttar Pradesh, to name a few.

The Crime in India Report 2021 by the National Crime Records Bureau reports the number of cases investigated under the Information Technology Act, 2000 and other IPC cases of cybercrimes, disaggregated by motive. Some of this data has been presented below.

Table 2.12: State-wise number of cybercrime cases registered under the IT Act, IPC and SLL in 2021

States	IT Act		IPC cases		SLL cases	
	Total Offences under the IT Act	Percentage of overall cybercrime cases	Total cybercrime cases under IPC	Percentage of overall cybercrime cases	Total cybercrime cases under SLL	Percentage of overall cybercrime cases
Andhra Pradesh	171	9.1	1694	90.3	10	0.5
Arunachal Pradesh	43	91.5	4	8.5	0	0.0
Assam	3840	79.2	1006	20.8	0	0.0
Bihar	11	0.8	1402	99.2	0	0.0
Chhattisgarh	205	58.2	146	41.5	1	0.3
Goa	10	27.8	26	72.2	0	0.0
Gujarat	444	28.9	1082	70.4	10	0.7
Haryana	414	66.6	191	30.7	17	2.7
Himachal Pradesh	54	77.1	16	22.9	0	0.0
Jharkhand	832	87.3	120	12.6	1	0.1
Karnataka	8125	99.9	11	0.1	0	0.0
Kerala	460	73.5	161	25.7	5	0.8
Madhya Pradesh	297	50.4	278	47.2	14	2.4

Maharashtra	537	9.7	5015	90.2	10	0.2
Manipur	8	11.9	58	86.6	1	1.5
Meghalaya	105	98.1	2	1.9	0	0.0
Mizoram	12	40.0	18	60.0	0	0.0
Nagaland	8	100.0	0	0.0	0	0.0
Odisha	730	35.8	1269	62.3	38	1.9
Punjab	250	45.4	292	53.0	9	1.6
Rajasthan	596	39.6	894	59.4	14	0.9
Sikkim	0	0.0	0	0.0	0	0.0
Tamil Nadu	831	77.2	240	22.3	5	0.5
Telangana	655	6.4	9644	93.6	4	0.0
Tripura	24	100.0	0	0.0	0	0.0
Uttar Pradesh	7586	85.9	1229	13.9	14	0.2
Uttarakhand	701	97.6	17	2.4	0	0.0
West Bengal	62	12.1	450	87.7	1	0.2
A&N Islands	2	25.0	6	75.0	0	0.0
Chandigarh	4	26.7	11	73.3	0	0.0
D&N Haveli and Daman & Diu	5	100.0	0	0.0	0	0.0
Delhi	284	79.8	71	19.9	1	0.3
Jammu & Kashmir	120	77.9	26	16.9	8	5.2
Ladakh	0	0.0	5	100.0	0	0.0
Lakshadweep	1	100.0	0	0.0	0	0.0
Puducherry	0	0.0	0	0.0	0	0.0
All India	**27427**	**51.8**	**25384**	**47.9**	**163**	**0.3**

Source: *Crime in India, 2021, NCRB*

Note: According to the 'Principal Offence Rule', when multiple criminal offenses are committed during a single incident, only the most serious offense is recorded as the primary or principal offense. The other offenses committed during the same incident are recorded as subsidiary or supplementary offenses.

According to the Crime in India Report 2021, the majority of reported cybercrimes are registered under the Information Technology (IT) Act, 2000, in many states. At the national level, nearly 52 percent of the overall cases registered as a cybercrime have been registered under the IT Act (Table 2.12).

Within the IT Act, at the all-India level, a large share of cases, 42 percent, were registered under Section 66D- cheating by personation by using computer resource. Another 24 percent of the cases were registered under Section 67 of the IT Act (Publication/ transmission of obscene/ sexually explicit act in electronic form), while other sections of the Act combined formed the remaining 34 percent of the cases. In some states, however, the majority of the cybercrimes are registered under the Indian Penal Code (IPC).

This categorisation of cybercrime cases under the IT Act or the IPC respectively is particularly politically significant when we take into consideration the fact that several of the cases of journalists, activists and human rights defenders being charged with cybercrimes fall under these very provisions, particularly under the IT Act. Further, Section 66A of the IT Act, which made sending offensive messages through communication services a punishable offence, was struck down by the Supreme Court in the landmark case of *Shreya Singhal vs Union of India*, 2015, in which Common Cause was a co-petitioner. However, several media outlets highlighted the fact that people continued to be prosecuted under the Section even after it was nullified by the Supreme Court. In October 2022, the Supreme Court reiterated the *Shreya Singhal* judgement and ordered the police to stop prosecuting free speech on social media (The Hindu, 2022).

States that have registered more than 80 percent of the cyber offenses under IPC are Andhra, Bihar, Maharashtra, Manipur, West Bengal, Telangana, and Ladakh. Within the total cybercrime cases registered under IPC, a majority, 55 percent, pertained to cases of fraud (Sec 420 r/w Sec 465, 468-471 IPC).

Although these numbers appear small compared to other kinds of crime cases, they are concerning because often, these very provisions are also employed by the state to charge those expressing their dissent or critique of the government or any government policy online, thus inhibiting their freedom of expression. For example, a journalist, late Vinod Dua was charged with sedition and spreading fake news under the IPC and IT Act provisions for his comments on the Citizenship Amendment Act and handling of the Covid-19 pandemic by the government in 2020 (The Wire, 2021). In 2019, climate activist Disha Ravi was arrested under the IT Act and charged with sedition for her alleged involvement in the creation and dissemination of a toolkit on social media in support of the farmers' protest (Trivedi, 2021). In another instance, in 2018, journalist Kishorechandra Wangkhem was arrested and charged under the National Security Act and the IT Act for uploading videos on Facebook critical of the state government in Manipur (Choudhury, 2021).

However, it is important to note that the provisions under the IT Act or cybercrime offenses under the IPC as reported by the NCRB may not reveal the entire extent of the cases filed under these provisions, particularly when they are clubbed together with serious offenses such as sedition, as was the case in all three examples mentioned above. This is because the crime reporting in NCRB Crime in India follows the 'Principle Offence Rule', wherein in each case where multiple legal provisions are attracted, only the most serious offense is reported at the 'primary offense' in the crime data. Thus, for example, all of the above cases are likely to have been recorded only as 'sedition' cases in the crime records.

The data presented above only reflects the total number of cases registered under specific provisions of cybercrimes, without indicating whether any of these cases involved social media content that was critical of the government or a particular political party. To gain insight into this, the motives recorded by the police behind certain cybercrimes can provide useful information on the number of cases that may be politically motivated.

Table 2.13: Selected cybercrime motives as reported by NCRB in 2021

State/UT	Political motives	Terrorist activities	Inciting hate against country	Disrupt ing public service
Andhra Pradesh	36	0	0	3
Arunachal Pradesh	0	0	0	0
Assam	112	3	12	5
Bihar	0	0	0	0
Chhattisgarh	0	0	0	0
Goa	1	0	0	0

Gujarat	6	1	0	1
Haryana	2	0	4	2
Himachal Pradesh	2	1	0	0
Jharkhand	0	0	0	0
Karnataka	3	0	0	1
Kerala	2	0	0	2
Madhya Pradesh	3	1	0	1
Maharashtra	5	0	0	2
Manipur	0	0	2	0
Meghalaya	0	0	0	0
Mizoram	0	0	0	0
Nagaland	0	0	0	0
Odisha	0	0	0	0
Punjab	3	1	1	0
Rajasthan	5	0	2	1
Sikkim	0	0	0	0
Tamil Nadu	44	0	0	9
Telangana	17	2	0	0
Tripura	0	0	0	0
Uttar Pradesh	64	0	10	9
Uttarakhand	0	0	0	0
West Bengal	4	0	0	0
A&N Islands	0	0	0	0
Chandigarh	0	0	0	0
D&N Haveli and Daman & Diu	0	0	0	0
Delhi	0	0	0	1
Jammu & Kashmir	2	2	0	3
Ladakh	0	0	0	0
Lakshadweep	0	0	0	0
Puducherry	0	0	0	0
All India	**311**	**11**	**31**	**40**

Source: *Crime in India, 2021, NCRB*

Notably, Uttar Pradesh, Tamil Nadu, Andhra Pradesh, and Assam stand out (Table 2.13). In Assam, 112 registered cases of cybercrimes were allegedly politically motivated, three included terrorist activities, 12 were committed with the motive of inciting hate against the country, and five were for disruption of public services. Reportedly, 64 cases of cybercrimes in UP had political motives, 10 were committed with the motive of inciting hate against the country, and another 9 were categorised under the disruption of public service. Similarly, in Tamil Nadu and Andhra Pradesh, 44 and 36 cases, respectively, of cybercrimes with political motives were filed by the police.

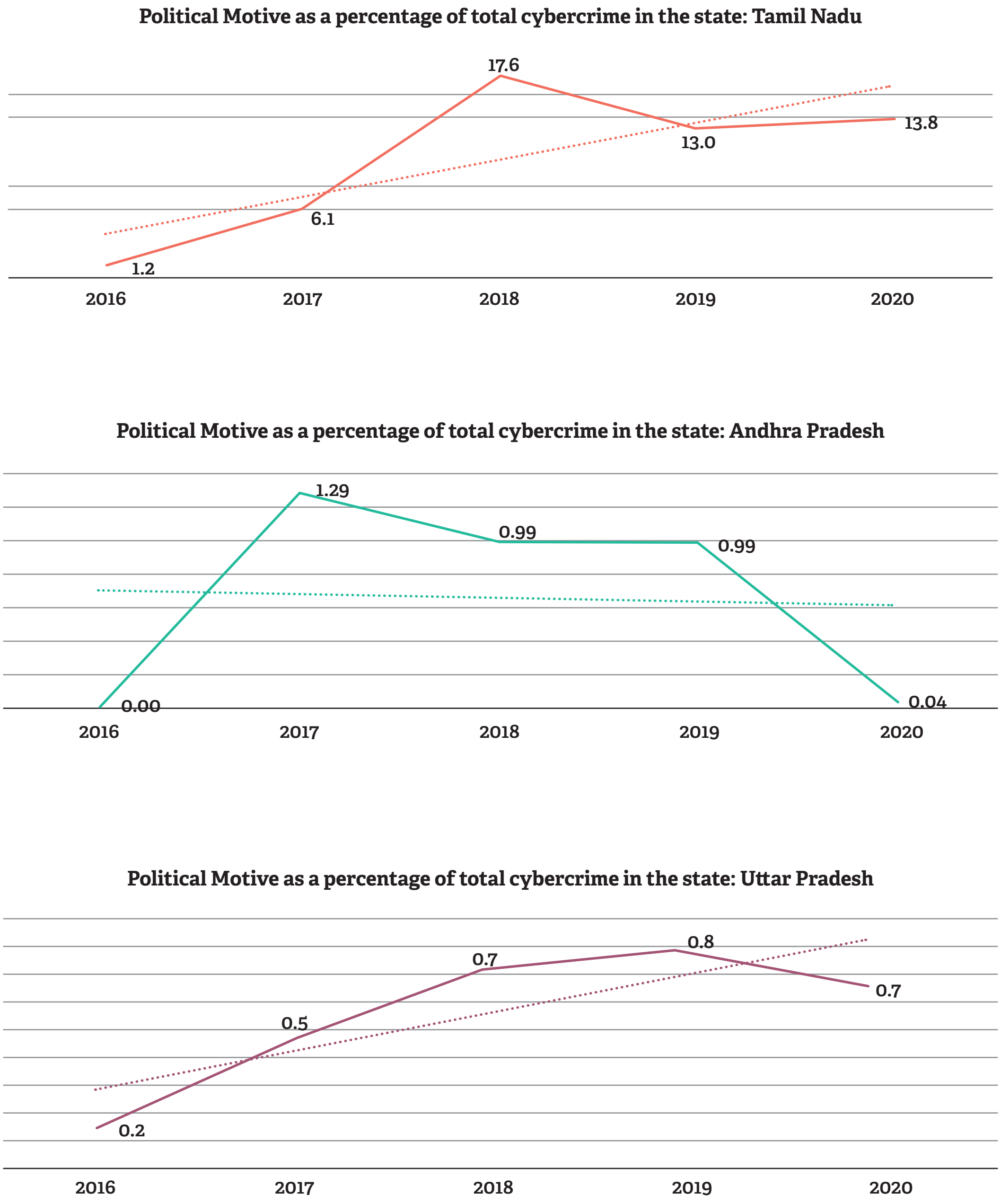
Table 2.14: State-wise number of cybercrime offences with a reportedly political motive from 2016-2020

State	2016	2017	2018	2019	2020
Andhra Pradesh	0	12	12	88	67
Arunachal Pradesh	1	0	0	0	0
Assam	10	10	9	16	24
Bihar	3	0	0	0	7
Chhattisgarh	1	3	4	5	0
Goa	0	0	0	0	0
Gujarat	0	4	0	1	3
Haryana	0	0	0	1	1
Himachal Pradesh	0	3	4	1	3
Jharkhand	0	16	1	0	0
Karnataka	6	20	22	9	18
Kerala	6	9	18	16	10
Madhya Pradesh	0	0	1	2	3
Maharashtra	2	3	20	12	9
Manipur	0	0	0	0	10
Meghalaya	1	1	3	2	1
Mizoram	0	0	0	0	1
Nagaland	0	0	0	0	0
Odisha	0	6	0	0	0
Punjab	0	2	2	4	2
Rajasthan	0	1	3	9	4
Sikkim	1	1	0	0	0
Tamil Nadu	2	14	52	50	108
Telangana	0	2	14	6	8
Tripura	0	0	4	1	1
Uttar Pradesh	4	23	45	90	73
Uttarakhand	0	0	0	0	1
West Bengal	2	9	1	1	1
A&N Islands	0	0	0	0	0
Chandigarh	0	0	0	0	0
D&N Haveli and Daman & Diu	0	0	0	0	0
Delhi	0	0	0	0	0
Jammu & Kashmir & Ladakh	0	0	3	2	1
Lakshadweep	0	0	0	0	0
Puducherry	1	0	0	0	0
All India	**40**	**139**	**218**	**316**	**356**

Source: *Crime in India (2016-2020), NCRB*

Disturbingly, the reported cases of cybercrimes committed for an alleged political motive have significantly increased over a period of five years. Beyond just the actual figure, the proportion of these cases compared to the total number of registered cybercrimes has also more than doubled over the last five years. In 2016 at the all-India level, 40 cases (or 0.3 percent of the total cybercrime cases in the year) were categorised as those with a political motive, but the figure in 2020 was 356, or 0.7 percent of the total number of cybercrime cases (Table 2.14). States which show a particularly high trend among this category are Tamil Nadu, Uttar Pradesh and Andhra Pradesh. Five-year trends emerging from the three states are presented in the graph below.

Figure 2.1: Political motive as a percentage of total cybercrimes in Uttar Pradesh, Andhra Pradesh and Tamil Nadu (2016-2020)



Source: *Crime in India (2016-2020), NCRB*

If we look at the trend of registering cybercrime cases as politically motivated in the three states over a time span of five years, we see a clear upward trend in Tamil Nadu and Uttar Pradesh. While in Uttar Pradesh such cases increased from 0.2 percent of the total cybercrime cases in 2016 to 0.7 in 2020, in Tamil Nadu, there was an exponential increase from 1.2 percent in 2016 to nearly 14 percent in 2020. In 2018, the proportion of such cases went up to about 18 percent in Tamil Nadu (Figure 2.1).

It needs to be noted here that "political motive" is a term that is used by the NCRB in its Crime in India report to categorise motives behind cybercrimes, but the term itself is not defined anywhere in the report. In the absence of a clear definition, it is being presumed here that cases of people expressing their political opinions, who are consequently prosecuted under various provisions of law for cybercrime related offences, fall under the category of those with a "political motive".

While these percentages may seem like a small fraction, when seen as actual figures, they can be disconcerting. For instance, in Andhra Pradesh, 88 cases of politically motivated cybercrimes were registered in 2018, despite this being a mere 0.99 percent of the total cybercrime cases registered in the state in that year. Table 2.15 provides the number of people who were arrested for cybercrimes in 2021, along with the chargesheeting and conviction rates for that year.

Table 2.15: State-wise number of people arrested, chargesheeting and conviction rate for cybercrimes in 2021

State	Number of people arrested	Chargesheeting rate	Conviction rate
Andhra Pradesh	363	31.8	14.0
Arunachal Pradesh	5	60.0	-
Assam	6096	15.9	2.2
Bihar	980	50.2	66.7
Chhattisgarh	260	83.0	0.0
Goa	42	52.9	0.0
Gujarat	1395	58.4	0.0
Haryana	647	51.9	7.5
Himachal Pradesh	68	61.8	50.0
Jharkhand	1414	45.4	45.5
Karnataka	615	31.3	12.8
Kerala	447	57.4	5.3
Madhya Pradesh	803	91.2	36.0
Maharashtra	2475	38.4	29.1
Manipur	31	50.0	-
Meghalaya	2	4.4	0.0
Mizoram	31	74.1	100.0
Nagaland	1	0.0	-
Odisha	363	16.2	0.0
Punjab	416	64.4	25.0
Rajasthan	861	30.0	33.3

Sikkim	0	-	-
Tamil Nadu	612	71.0	16.7
Telangana	1478	16.4	44.2
Tripura	8	37.0	-
Uttar Pradesh	6887	45.5	83.2
Uttarakhand	207	59.0	-
West Bengal	246	60.0	70.8
A&N Islands	12	60.0	-
Chandigarh	9	42.9	0.0
D&N Haveli and Daman & Diu	4	100.0	-
Delhi	494	90.8	100.0
Jammu & Kashmir	102	48.5	0.0
Ladakh	0	-	-
Lakshadweep	0	50.0	-
Puducherry	0	-	-
All India	**27374**	**33.8**	**42.5**

Source: *Crime in India, 2021, NCRB*

Table 2.15 shows that UP and Assam had more than 6,000 people arrested under various provisions of cybercrimes laws in 2021, and upwards of 1,000 people were arrested for cyber offences in the states of Gujarat, Jharkhand, Maharashtra, and Telangana. Despite this, the chargesheeting and conviction rates in some of these states are particularly low. In Assam, for instance, the chargesheeting rate for these cases is just about 16 percent, and the conviction rate was nearly two percent in 2021. In Gujarat, the conviction rate for this category of offences was 0 in 2021, and the chargesheeting rate was less than 60 percent. In UP, where 6,887 people were arrested under cybercrime charges, less than half of the cases filed, 46 percent, were chargesheeted. Similarly, in Telangana, the chargesheeting rate for such offences was a meagre 17 percent.

2.4. Watching the police: CCTVs in police stations

In the previous section, we touched upon the issue of direct or indirect police and state surveillance. In this section, we will focus on the coverage of CCTV cameras in police stations, which was mandated by the Supreme Court in 2020 in the landmark case of *Paramvir Singh Saini vs Baljit Singh*. The Court gave specific directions to ensure that CCTV cameras are installed at all entry and exit points in police stations, in all lock-ups and outside the lock-up, in the inspectors' room, and other areas of the police station. The judgement further required that the systems have night vision and include audio as well as video footage, and have a data storage capacity of 18 months. Additionally, the court mandated the formation of a State-Level Oversight Committee (SLOC) and a District-Level Oversight Committee (DLOC) to oversee the functioning of CCTV cameras in police stations and review the footage.

2.4.1. CCTVs in police stations as per BPRD

According to the Data on Police Organisations Report 2022 published by BPRD, information on the implementation of these detailed directives is not available in the public domain. However, the report does provide data on the number of police stations with CCTV cameras as of January 2021.

Table 2.16: Percentage of police stations with functioning CCTV cameras as on 01.01.2022

States	Number of actual/ existing rural/urban/ special purpose police station installed with CCTV cameras	Percentage of overall police stations installed with CCTV cameras
Andhra Pradesh	599	58.3
Arunachal Pradesh	99	92.5
Assam	329	100.0
Bihar	957	90.6
Chhattisgarh	443	97.1
Goa	44	100.0
Gujarat	622	83.5
Haryana	381	96.0
Himachal Pradesh	136	90.1
Jharkhand	126	22.3
Karnataka	1052	99.7
Kerala	538	95.4
Madhya Pradesh	859	74.1
Maharashtra	663	56.8
Manipur	0	0.0
Meghalaya	25	32.9
Mizoram	40	90.9
Nagaland	28	32.6
Odisha	584	90.8
Punjab	425	98.6
Rajasthan	1	0.1
Sikkim	13	43.3
Tamil Nadu	1578	68.8
Telangana	842	99.9
Tripura	73	89.0
Uttar Pradesh	1533	86.0
Uttarakhand	159	98.1
West Bengal	637	100.0
A&N Islands	24	100.0
Chandigarh	17	94.4
D&N Haveli and Daman & Diu	8	100.0
Delhi	0	1941 cameras in 197 police stations (bifurcation not available)

Jammu & Kashmir	51	20.4
Ladakh	7	100.0
Lakshadweep	0	0.0
Puducherry	0	0.0
All India	**12893**	**73.5**

Source: *Data on Police Organisations, 2022, BPRD.*

The table above shows that as of January 1st, 2022, states/UTs such as Ladakh, Dadar and Nagar Haveli and Daman and Diu, A&N Islands, West Bengal, Goa, and Assam have installed CCTV cameras in all police stations. However, in Puducherry, Lakshadweep, Manipur, and Rajasthan, none of the police stations have CCTV cameras. Nationally, approximately one-fourth of police stations did not have CCTV cameras installed. It should be noted, however, that the BPRD report does not indicate whether all specified areas within police stations have CCTV coverage, meaning that the actual percentage of coverage may be lower than reported.

Prior to the release of the BPRD report on CCTV coverage, we submitted several Right to Information (RTI) requests to gather information on the same topic. In response, some states provided updated figures (the BPRD report covers data from 2021, while the RTI requests were filed in 2022). Details from the RTI responses are provided in the following section.

2.4.2. CCTVs in police stations: RTI data

The purpose of the RTI applications was to check the status of the implementation of the Supreme Court judgement in *Paramvir Singh Saini vs. Baljit Singh & Others* dated December 2, 2020. RTI applications were filed with all the States and Union Territories requesting them to provide the status of mandatory installation of functioning CCTV Cameras in all the police stations, district-wise.

Table 2.17: CCTV coverage in police station based on RTI information

State	Total police stations in the state (BPRD's data on police organisations 2021)	Total police stations installed with functioning CCTV cameras (RTI)	
	Figures	Figures	Percent
Andhra Pradesh*	1027	Data not provided	Data not provided
Arunachal Pradesh*	107	70	65.4
Assam	329	73	22.2
Bihar	1056	952	90.2
Chhattisgarh	456	443	97.1
Goa*	44	23	52.3
Gujarat	745	619	83.1
Haryana	397	No response	No response
Himachal Pradesh*	151	73	48.3
Jharkhand*	564	29	5.1
Karnataka	1055	1052	99.7

Kerala	564	Data not provided	Data not provided
Madhya Pradesh	1159	Data not provided	Data not provided
Maharashtra	1168	764	65.4
Manipur	84	No response	No response
Meghalaya	76	20	26.3
Mizoram	44	40	90.9
Nagaland	86	19	22.1
Odisha	643	584	90.8
Punjab	431	Data not provided	Data not provided
Rajasthan	917	No response	No response
Sikkim	30	29	96.7
Tamil Nadu	2292	No response	No response
Telangana*	843	429	50.9
Tripura	82	72	87.8
Uttar Pradesh	1783	No response	No response
Uttarakhand	162	160	98.8
West Bengal*	637	53	8.3
Andaman & Nicobar	24	24	100.0
Chandigarh	18	16	88.9
Dadra & Nagar Haveli and Daman & Diu	8	6	75.0
Delhi	225	190	84.4
Jammu & Kashmir*	250	15	6.0
Ladakh	7	7	100.0
Lakshadweep	16	0	0.0
Puducherry	55	Data not provided	Data not provided
All India	**17535**	**5762**	**32.9**

Source: *Response to RTI applications filed by Common Cause; Data on Police Organisations, 2022, BPRD.*
*Note: These states/UTs have not provided complete information through RTI. Only partial information from selected districts/police stations have been received from these states/UTs until the cut-off date of 10th January 2023.

As the responses are still coming in, the cut-off date to analyse this data is January 10, 2023. It must be noted that the format of data produced by the states that responded to the RTI application with figures was not symmetrical. While this information is published annually by the BPRD, some states responded directly with data, while others forwarded the application to district and police station-level authorities and sent responses accordingly. This indicates a lack of information concerning CCTV-enabled police stations with the state authority and creates a disturbing pattern of subverting or dismissing information-seekers.

According to the Data on Police Organisations 2022 statistics, out of 17,535 police stations, about 74 percent are equipped with CCTV systems (Table 2.16), while RTI responses received as of November 20, 2022, revealed that only about 33 percent of police stations across the country are CCTV-enabled (Table 2.17). Regardless of compliance status, all Union Territories provided some information, while several states either did not respond or responded vaguely. This vast gap in the information provided by the states via RTI, as opposed to the BPRD's statistics, is a serious concern and an impediment to transparency.

A cursory look at the data shows that about a quarter of the total entities (28 states and eight Union Territories) did not provide a proper response to the RTI. Haryana, Manipur, Rajasthan, Tamil Nadu, and Uttar Pradesh did not respond to the application at all, while Andhra Pradesh, Kerala, Madhya Pradesh, Punjab, and Puducherry communicated vaguely but did not provide any data.

Interestingly, Tamil Nadu (2292), Uttar Pradesh (1783), Madhya Pradesh (1159), Andhra Pradesh (1027), and Rajasthan (917) are five of the top 10 states with the highest number of police stations in the country according to the BPRD's Data on Police Organisations 2022 statistics, yet none of these have provided information regarding CCTV coverage under the RTI application. Adequate information about the compliance status was also unavailable through RTI for Jharkhand, Manipur, Rajasthan, and Lakshadweep.

As per the RTI responses, Ladakh and Andaman & Nicobar have been outliers, with 100 percent CCTV-enabled police stations across the country. Other than these, Karnataka, Sikkim, Chhattisgarh, Odisha, Mizoram, Bihar, and Uttarakhand have shown CCTV compliance in over 90 percent of police stations.

Notably, in states and UTs such as Arunachal, Assam, Goa, Himachal Pradesh, Jharkhand, Meghalaya, Nagaland, and Telangana, to name a few, the percentage of police stations with CCTV coverage as reported in BPRD in 2021 is significantly lower than the percentage coverage as reported in the RTI responses. For instance, while BPRD data suggests 100 percent coverage of police stations with CCTV cameras in West Bengal, the RTI data suggests that only about eight percent of the police stations are equipped with CCTV cameras. However, it needs to be noted that in some states and UTs, such as West Bengal, only partial information has been provided by the districts/police stations in a disaggregated form, and therefore this data may be incomplete.

Overall, in 13 states and UTs, the coverage of CCTV in police stations as reported in the RTI data is lower than as reported in the BPRD data. Even though there is a time gap of one year between the two datasets, the differences in percentage coverage, as noted in the above examples, are significant. On the other hand, only in Maharashtra and Sikkim has the CCTV coverage increased as per the RTI data when compared with the BPRD data. In Maharashtra, according to the BPRD report of 2021, nearly 57 percent of police stations had CCTV cameras installed. However, the RTI data of 2022 reveals that the coverage increased to 65 percent. In Sikkim, the CCTV coverage in police stations increased from 43 percent in 2021 (as reported by BPRD) to 97 percent in 2022 (as per RTI). However, among the states for which RTI information is available (26 states and UTs), in half of them, the reported RTI data for 2022 is significantly lower than the data provided by the BPRD for 2021.

This highlights the inconsistency and unreliability of information provided by the states and UTs. Even though complete information on compliance with the SC directive is not provided in either of the sources, the aggregate information being provided is contradictory and possibly misleading. Non-compliance within the designated time period may be seen as a deliberate disregard of the Supreme Court orders, amounting to the contempt of court. While exceptional circumstances such as lightning strikes leading to a police station facing loss of power and becoming non-functional (Bajengdoba Police Station in Meghalaya) may occur, such conditions are not the norm.

Ideally, orders such as these should be implemented promptly and information concerning them should be made available without bureaucratic hurdles. The order is clear and simple, providing a precise guideline for the installation of CCTV systems in police stations. However, several states have evaded accountability by not acknowledging the RTI application or not providing detailed information. This undermines the right to access information, and states are disregarding the Supreme Court's order by not being transparent in their dealings with RTI Applications. This is in clear violation of the spirit of the RTI Act and inhibits public access to government data.

2.5. Use of FRT by the state

There is limited official data available on surveillance technologies used by the state, but some private organisations have been collecting information on these technologies. One such organisation is the Internet Freedom Foundation (IFF), which created the 'Project Panoptic Tracker' that provides comprehensive data on the installation, use, and budgeting of FRTs across the country. The primary source of data for this project is the RTI.

According to the data collected by IFF, 13 FRT systems have been installed at the central level in India, with only one currently in use by the Central Board of Secondary Education for identity authentication. Additionally, several government departments have either installed or are in the process of installing FRT systems for identity authentication, security, or surveillance purposes. These departments include the Ministry of Civil Aviation and DigiYatra Foundation, Supreme Court of India, Gadarwara Super Thermal Power Project, Department of Defence, Research and Development, Ministry of Personnel, Public Grievances and Pensions, Ministry of Railways, Bhakra Beas Management Board, National Crime Records Bureau, South Western Railways, and Indian Army.

Based on available information, the total financial outlay for central-level FRT system installation is estimated to be Rs 770.20 Cr. At the state level, however, data on the extent of FRT installation is limited.

Table 2.18: FRT systems installed by the states

States	Number of FRT systems installed	Number of FRT systems in active utilisation	Estimated financial outlay
Andhra Pradesh	7	0	0
Arunachal Pradesh	1	0	0
Assam	2	0	0
Bihar	5	1	0
Chhattisgarh	2	0	32.02
Goa	1	0	0
Gujarat	8	1	110
Haryana	5	0	6000
Himachal Pradesh	0	0	0
Jharkhand	2	0	0.7
Karnataka	4	1	496
Kerala	6	0	5

Madhya Pradesh	3	0	1.46
Maharashtra	12	2	527
Manipur	1	0	0.5
Meghalaya	2	0	0
Mizoram	0	0	0
Nagaland	3	0	0
Odisha	3	0	87.61
Punjab	4	1	0
Rajasthan	1	0	0
Sikkim	0	0	0
Tamil Nadu	7	2	46.5
Telangana	8	4	3.41
Tripura	0	0	0
Uttar Pradesh	3	1	12500
Uttarakhand	1	1	0
West Bengal	5	0	334
A&N Islands	0	0	0
Chandigarh	1	1	0
D&N Haveli and Daman & Diu	0	0	0
Delhi	11	3	150
Jammu & Kashmir	2	0	0.70
Ladakh	0	0	0
Lakshadweep	0	0	0
Puducherry	1	1	0
Total (state-level)	**111**	**19**	**7172.68**

Source: *Panoptic Tracker: Facial Recognition Systems in India. Internet Freedom Foundation.*

The data reveals that, with the exception of eight small states and UTs, all other states have installed at least one FRT system, bringing the total number of state-level system installations to 111. Of these, 19 are in active use. Maharashtra (12), Delhi (11), and Telangana (8) are the states with the highest number of FRT installations, with Telangana and Delhi also having the highest number of FRT systems in active use, at four and three respectively.

Overall, the states have spent or allocated upwards of Rs 70 crore on these systems, with the highest financial outlays in Uttar Pradesh (Rs 125 Cr) and Haryana (Rs 60 Cr). The estimated total financial outlay for FRT systems at both the central and state levels is Rs 1,464.18 Cr.

It should be noted that this data only provides a partial picture of the extent of FRT installation and use in India, with private organisations such as the Internet Freedom Foundation (IFF) providing additional data on the subject.

Conclusion

The data on the number of cybercrime cells, police stations and social media monitoring cells across Indian states provides some insight into the country's preparedness to tackle cybercrime. While some states have a higher registration of cybercrimes, their infrastructural capacity to handle such cases does not match up to the high volume of registration. Additionally, the presence of a high number of social media monitoring cells in some states raises concerns regarding digital surveillance and the need for proper legal and judicial oversight. Therefore, the availability and capacity of trained personnel for cybercrime investigation is critical and should be given priority.

While the threat of cybercrime is increasing, and it is essential to build specialised physical and human infrastructure to tackle it, this infrastructure must not be used as a tool for surveillance by the state, infringing upon the privacy and freedom of speech of individuals. Analysis of the crime data suggests that the majority of reported cybercrimes are registered under the Information Technology (IT) Act, 2000, at the national level, and the majority of the cases under the IT Act are registered under Section 66D (cheating by personation by using a computer resource) and Section 67 (publication/transmission of obscene/sexually explicit acts in electronic form). This categorisation of cybercrime cases under the IT Act or the IPC is significant politically since several journalists, activists, and human rights defenders being charged with cybercrimes fall under these very provisions. It is crucial to ensure that the freedom of expression is protected while combating cybercrime.

The implementation status of the Supreme Court's directive under *Paramvir Singh vs Union of India* mandating the installation of CCTV cameras in all police stations across the country has also been assessed through RTI applications. The data received through the applications indicates a disturbing pattern of subverting or dismissing information-seekers, with several states and UTs either not responding or providing vague responses. The discrepancy in the data provided by the states and the BPRD's statistics raises serious concerns about transparency and accountability. Although exceptional circumstances may occur, orders such as these should be implemented promptly, and information concerning them should be made available without bureaucratic hurdles. Amongst those for which data has been received, as per RTI data of 2022, in 13 states and UTs the CCTV coverage in police stations is lower than the coverage as reported in 2021 by the BPRD report, Data on Police Organisations. Even though there is a time gap of one year between the two datasets, the differences in percentage coverage are significant in some of the states and UTs.

References

Choudhury, R. (2021, July 23). Manipur Journalist, Arrested Under NSA for "Cow Dung" Post, Released. Imphal, *NDTV*. Retrieved from: https://www.ndtv.com/india-news/manipur-journalist-kishorechandra-wangkhem-arrested-under-nsa-for-cow-dung-post-released-2493251.

Internet Freedom Foundation (n.d.). Facial Recognition Systems in India. The Panoptic Tracker, Retrieved from: https://panoptic.in/.

Jaishankar, K. and Kumar, P.A. (2010). "The Impact of CCTV on Crime in Chennai, India". *International Journal of Criminal Justice Sciences,* 5(1).

Joshi, D. (2022, August 9). What Could the Future of Indian Data Protection Law Look Like? *The Wire.* Retrieved from: https://thewire.in/tech/future-of-data-protection-law-india.

Mishra, R.K. and Gupta, M. (2011). "Evaluating the Impact of CCTV on Crime in Delhi Metro Rail Corporation Trains and Stations". *Journal of Security Administration,* 34 (2).

Paramvir Singh Saini vs Baljit Singh (2020) 7 SCC1

Piza, E.L. (2018). The Crime Prevention Effect of CCTVs in Public Spaces: A Propensity Score Analysis. John Jay College of Criminal

Justice, *City University of New York*. Retrieved from: https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1188&context=jj_pubs.

Selvaraj, A. (2022, March 19). Tamil Nadu: Special Police Unit to Monitor Fake Social Media Posts. Chennai, *The Times of India*. Retrieved from: https://timesofindia.indiatimes.com/city/chennai/tamil-nadu-special-police-unit-to-monitor-fake-social-media-posts/articleshow/90315927.cms.

Singh, P. and Bhandari, L. (2011). "Crime and CCTV in Mumbai: An Evaluation of Public Surveillance Systems". *Institute for Defence Studies and Analyses.*

Tiwari, A. and Rao, U.N.B. (2016). Non-Registration of Crimes: Problems and Solutions. Bureau of Police Research & Development (BPRD), Ministry of Home Affairs, Government of India. Retrieved from: https://bprd.nic.in/content/417_1_Plan.aspx.

The Hindu Bureau (2022, October 12). No More Prosecutions Under Section 66A, Says Supreme Court. New Delhi, *The Hindu*. Retrieved from: https://www.thehindu.com/news/national/no-more-prosecutions-under-section-66a-says-supreme-court/article66002464.ece.

The Wire Staff (2021, June 3). SC Quashes Sedition Case Against Vinod Dua, Says Every Journalist Entitled to Protection. New Delhi, *The Wire.* Retrieved from: https://thewire.in/law/supreme-court-quash-vinod-dua-sedition-case.

Trivedi, S. (2021, February 14). Farmers' Protests: 22-Year-Old Activist Disha Ravi Arrested, Sent to Delhi Police Custody. New Delhi, *The Hindu*. Retrieved from: https://www.thehindu.com/news/national/22-year-old-activist-disha-ravi-arrested-for-sharing-farmers-protests-toolkit-with-greta-thunberg/article61751508.ece.

Chapter 3:

Experts' Perspectives on Surveillance and Privacy in India

Key findings

- In the FGD, the participants broadly agreed that while surveillance is being conducted by various actors—state, private companies as well as individuals—it was the unchecked targeted surveillance by the state and its agencies that was the biggest cause for concern.
- While there was a difference of opinion amongst the participants about the efficiency of mass surveillance technologies such as CCTVs for controlling crime and improving public safety, there was consensus regarding the need to have oversight over such surveillance technologies.
- The FGD participants were of the opinion that support for surveillance technologies amongst the general public stemmed from ignorance about the right to privacy and the dangers of surveillance technologies as well as a general tendency to view surveillance as an effective tool for public safety and national integrity. Some of the participants also pointed out the differences in opinions depending on the class of the citizens, with the poor being less likely to support surveillance by the police or the state.
- Some of the FGD participants as well as serving police officers who were interviewed separately pointed out that the police departments in India lack the necessary infrastructure, capacity and legal mechanism to be able to properly conduct surveillance.
- Some of the FGD participants highlighted the dangers of surveillance technologies by pointing out their inaccuracies and how discrimination within the system can be fed into the technology, translating into a biased algorithm.
- There was a general consensus amongst the FGD participants that targeted surveillance is being used as a tool to curb dissent and surveillance technology is being used to monitor social media and track individuals and groups perceived as a threat to the government. This has a chilling effect on freedom of speech and expression in the country.

CHAPTER 3

Experts' Perspectives on Surveillance and Privacy in India

Despite the prevalence and pervasiveness of surveillance, public debates around it and on the right to privacy seem to be limited to a niche group of people, such as domain experts, rights activists, and practitioners. The scant literature around the issue comes off as polarised, with two clean ends of the spectrum being pro or anti-surveillance, while the larger public in between appears unaware of the scope and seriousness of emerging surveillance technologies as well as public debates around them.

While the later chapters on survey data show a striking lack of awareness around surveillance and the right to privacy – such as the Supreme Court judgement declaring right to privacy as a fundamental right or awareness around the Pegasus phone-tapping scandal – the issue has been a topic of intense debate in India in recent years, at least among specialist circles. India has a long history of government surveillance, dating back to the colonial era, and the issue continues to be a contentious one. The rise of digital technology has only increased the scope

FGD/in-depth interview questions

The questions asked during the FGD and in-depth interviews included, but were not limited to, the following:

1. Is surveillance an infringement of the citizen's right to privacy?
2. Do you think surveillance is a necessary evil?
3. Common citizens often support/justify CCTV surveillance/phone tapping on grounds of national security/public safety. What are your views on it?
4. Are mass surveillance techniques such as CCTVs, FRTs, phone tapping, etc. useful for solving or preventing crimes?
5. Do you think mass surveillance technologies such as those mentioned above have a chilling effect on people's right to expression and dissent?
6. Do you think that the use of surveillance and related technology by the police has a discriminatory impact on minorities and vulnerable groups?
7. Do you think the police have adequate infrastructure/training to carry out surveillance fairly?
8. What kind of legal mechanism should be put in place to ensure grievance redressal in matters of surveillance?
9. What are your own experiences about the impact of surveillance or that of someone you personally know?

and reach of surveillance, and many citizens are concerned about the potential implications on their privacy and personal freedoms. On the other hand, it is equally true that surveillance sometimes becomes necessary for national security and public safety.

While a sample survey is able to map the public opinion, it does not necessarily capture the views of experts and activists because of methodological limitations. In view of this, we conducted focus group discussion and in-depth interviews. The focus group discussion (FGD) and in-depth interviews on surveillance and the right to privacy in India aim to triangulate the survey data and present the perspectives of various specialised groups, such as police officers, journalists, civil rights activists, lawyers, and academics, among others. The FGD was conducted to provide a platform for such experts to share their thoughts and opinions on the issue and offer a valuable opportunity to gather insights into the views of a diverse range of people.

The findings of the FGD and in-depth interviews, in combination with the survey data, provide a nuanced and informed understanding of the complexities of privacy and surveillance in India.

3.1. Methodology

3.1.1. Sample description

For the FGD, it was decided to invite experts from the field. The sample included former police officers who have experience of working in the field of surveillance, technology, and cybercrimes. It also included senior journalists who have covered the issue of surveillance and the right to privacy in India, including some who were allegedly targeted by the Pegasus spyware. The sample also included leading civil society activists working on the issues of digital surveillance, the right to privacy, and data protection in India, as well as academics from both Indian and international universities researching issues related to policing and surveillance in India. A total of 13 domain experts participated in the FGD. The complete list of FGD participants is provided at the end of the chapter.

3.1.2. FGD procedure

The FGD was conducted online via the Zoom platform on 26th September 2022 and was facilitated by the core research team of the SPIR report from Common Cause. The discussion was preceded by a presentation of some of the main findings emerging from the survey with common people on the issue of digital surveillance in India.

Following this, the discussion was divided into three parts. In the first session, a general discussion was held on the broader aspects of the issue, and opinions of all the participants on the larger conceptual understanding of surveillance were sought.

For the second part of the discussion, the participants joined three separate breakout rooms, each with a facilitator and a rapporteur. Each group had representation from various fields, including police personnel, journalists, civil society activists, and academics. This discussion focused on more in-depth understandings and opinions regarding the questions posed. The breakout sessions also took note of newer issues and themes emerging from the discussion.

In the concluding third session, all the participants re-joined the larger group for a more free-flowing discussion to allow room for sharing their concluding thoughts with conceptual and experiential knowledge.

3.1.3. Data collection

Since the FGD was conducted online, the entire discussion was recorded. Following this, the research team transcribed the recording in detail. The transcription was manually categorised thematically and used for data analysis.

3.1.4. Data analysis

After several rounds of careful reading of the transcription, manual coding and labelling were done of the main themes emerging from the FGD. The participants' opinions about these themes were categorised and grouped. Notable examples, anecdotes, or outlier opinions about the sub-themes were listed separately. Following this, the categorised data was analysed to draw larger trends and patterns, and these were interpreted with the original research questions.

3.2. Findings

3.2.1. Defining surveillance

Theme	Probed areas	FGD responses/comments
Defining surveillance and its broader impact	What are the different forms of surveillance that need public attention and oversight?	• While some participants felt that technologies such as CCTVs used by individuals were more a matter of public safety than surveillance, others considered it a part of classical surveillance that needs to be critically analysed. • Even though the respondents agree that surveillance is being regularly employed by both private companies as well as the government, it was felt that government surveillance, particularly targeted surveillance, was more worrisome, as itwas being used to stifle the freedom of speech.
	What is the broader impact of surveillance on society?	• All respondents were in consensus that unregulated surveillance by the government has a chilling effect on freedom of speech and is undermining democracy in India. • Some respondents also pointed out how the private players and the government are working together to use surveillance against any form of dissent and to influence electoral outcomes.

The focused group discussion (FGD) highlighted the difficulties around defining the word "surveillance" and emphasised the importance of building a shared understanding of the concept. The participants defined surveillance as a process of monitoring, collecting, and analysing data to observe and track the behaviour, actions, and movements of individuals or groups. They identified various forms of surveillance, such as physical, digital, and behavioural surveillance. Participants acknowledged that surveillance could be conducted by various actors, such as governments, private companies, and individuals, and could be used for different purposes, such as national security, law enforcement, and marketing. They also highlighted the importance of informed consent, transparency, and accountability in conducting surveillance.

During the discussion, one participant initially considered private persons or entities deploying equipment such as CCTVs as more a matter of public safety than surveillance. According to him, state-enabled targeted surveillance, such as Pegasus, is the more worrisome surveillance that needs to be discussed, debated and checked. However, another participant believed that CCTVs are a classical example of mass surveillance. The participants dissected the concepts of surveillance based on whether it was the state or non-state agencies behind such surveillance. This tension was brought out succinctly by an academic when he states:

> ***"What is interesting for me is that surveillance is being pitted against the right to privacy here. That tension in a sense for me is interesting, rather than pitting it against the idea of public interest here..."***

The group largely agreed that while there is also private surveillance, it is the surveillance by the state, particularly targeted surveillance aimed at inhibiting people's right to expression and curbing dissent, that is much more nefarious and worrisome. They also pointed out that while surveillance by individuals is commonplace, surveillance by private companies often goes beyond marketing purposes and it can be driven by political motives aiding to inhibit people's right to expression. A senior journalist, himself an alleged victim of the Pegasus spyware, noted how the spyware was developed by a private company in Israel, NSO, which was then sold to governments across the globe.

The FGD began with a presentation of the key takeaways from the survey with the general public about their perceptions regarding surveillance. The participants agreed that the public in general had few concerns about surveillance and infringement of the right to privacy, largely due to the lack of awareness. Several participants pointed out that often, surveillance, particularly forms of mass surveillance such as the use of CCTVs, is pitted against public safety and law and order, due to which the public tends to be supportive of the use of such technologies. However, it is not common knowledge that no studies have shown a strong correlation between the presence of CCTVs or other similar surveillance

3.2.2. General public's awareness of surveillance

Theme	Probed areas	FGD responses/comments
People's awareness of surveillance	What are the reasons for the general public's support for surveillance?	• Respondents generally agreed that the public in general is not concerned with surveillance technology or issues related to the right to privacy because of the lack of awareness and contextual differences. • When surveillance is seen as a deterrent to crime, people are likely to support it. However, when it starts entering into people's private spheres, the level of support will go down. • There is a difference between the middle class and the rich public's perception, who are more likely to support surveillance. The poor people, on the other hand, are more likely to view it critically, perhaps, because they are more often at the receiving end of the state's ire.
	What can be done to improve public dialogue around surveillance in India?	• Majority support for an issue (as against constitutional position on it) may not always be a good benchmark for policy-making, since the majority is often found to be supporting illegal acts. • Data, or the lack of it, can be an argument to show that more surveillance does not have an impact on public safety and levels of crime in a locality.

technologies and a reduction in the rate of crime in an area. Thus, this is a common misconception held by the larger public when they associate the presence of such surveillance technologies with public safety. A senior media studies academic noted the tension between surveillance and the right to privacy in the context of public perceptions about surveillance.

The participants also noted that public perceptions are likely to vary depending on the context in which surveillance is conducted. People are likely to support it in contexts where it is seen as a deterrent against crime. However, when surveillance starts entering into the private spheres of people's lives, their perception towards it is likely to change. The low levels of understanding of issues such as privacy and the absence of local terminologies for such issues were noted by a civil society representative:

A former police officer highlighted that the majority's opinion about an issue may not necessarily align with the legal or humanitarian side of the argument. He noted how even in incidents that were in clear violation of the law, such as the Bhagalpur blinding case[1], the larger public opinion was in favour of the accused police officers (Amnesty International India, 2019). Therefore, majoritarian public opinion need not always be taken at face value or seen as a justification for acts that go against human rights and constitutional values.

The lack of literacy on the issue of privacy, particularly among the middle class in India, was also discussed. A senior journalist noted that those who are supposed to be more aware are less aware, and it is the poor (who understand the relationship between them and the police better) who are more cautious of their use of surveillance technologies.

> ***"Common citizens often support and justify surveillance on grounds of national security and public safety. This has also been our experience when we have done civic literacy campaigns. Around that, there is quite often wide popular support for public safety and national security.... We've discovered, those are themes that are already well-understood by large populations. Everyone understands their safety, and national security. Privacy, surveillance, digital technologies and their impact have been much more expert-led conversations. It does not have adequate vocabulary itself. When we attempted translations in local languages, we noticed that people have somewhat of a spirited conversation – does privacy mean secrecy, or confidentiality in their local language? Does it mean a right? And so on... There's also geographic disparity. We made local language explainers for several states in 10 languages, for which there was a greater degree of sharing and support in Punjabi and Bengali, but Hindi by itself did not do that well."***

[1] In the early 1980s in Bihar, police officials blinded over 30 under-trial prisoners by pouring acid into their eyes during interrogation, allegedly to extract confessions. The incident became known as the "Bhagalpur Blindings" and drew widespread condemnation from human rights organisations and civil society. The case was investigated by various human rights organisations, including the People's Union for Civil Liberties (PUCL) and the Bihar State Human Rights Commission. The PUCL also filed a public interest litigation (PIL) in the Supreme Court of India, which led to the formation of a commission to investigate the matter. The commission, headed by Justice N.N. Singh, submitted its report in 1986, which indicted several police officials for their involvement in the blinding of the prisoners.

3.2.3. Impact and misuse of technology

Theme	Probed areas	FGD responses/comments
Impact and misuse of technology	What are the known loopholes of existing surveillance technologies?	• The law is unable to keep pace with the growing surveillance technologies and therefore the government is not held answerable for misuse. • Interception-based surveillance goes beyond the legal scope. • Surveillance technology is inaccurate on many occasions and can be discriminatory based on the pre-existing biases entered into its algorithm.
	How is surveillance technology being misused? What are some ways of preventing misuse?	• Metadata can be more dangerous than data itself because of its huge potential for misuse • Despite having some infrastructure for surveillance technology, the police and state agencies do not have the capacity, skills or resources to handle these technologies. • However, police and other state agencies have wide discretion over the use of such technologies and the power to manage them, which makes it dangerous—both because of the possibility of misuse by the state as well as due to the lack of infrastructure to protect public data gathered through surveillance. • There is a need for transparency in the way these technologies are being used, oversight and accountability measures.

During the discussion, some participants pointed out that technology has made surveillance easier and more widespread, while others expressed concerns about its potential misuse and the need for regulations to prevent it. A former police officer highlighted the relationship between the police and technology. He pointed out that despite having the infrastructure for surveillance, the police did not have the capacity or training to handle it, even for the most basic forms of technology such as CCTVs. He also expressed concern about low levels of awareness among people conducting such surveillance on behalf of the government, leading to the misuse of technologies in the absence of proper oversight. He emphasised that if technology is being used for the safety of the public, there is nothing wrong with it. What is problematic is interception-based surveillance which goes beyond the legal scope:

"I think but for Hyderabad, which might be better than the rest, the saving grace is most of the CCTVs are not working. And nobody has any idea of what they are doing. The suspect list, the modus operandi and the people whom you're looking for, that list itself is not there. If you go to any CCTV network in the country which is run in the public domain primarily by the police or connected agencies, it's not there... And the 2800 crores under the Nirbhaya fund, to what worth it has been put can be left to every person's imagination.... You'll find any number of people in the government who don't understand what is Pegasus at all. Point is, people who are running the whole show don't understand it. If you ask people to define metadata, they do not know. And that metadata can be a billion times more dangerous than the data, the content itself."

Another participant said while there is a lack of state capacity on the one hand, the state has immense power to conduct surveillance because of the progress in technology. A senior journalist pointed out how the progress of technology has been so fast that the law is unable to keep track of it, allowing the government to not be held answerable to the public when it conducts even targeted surveillance outside the scope of constitutional values and in infringement of people's fundamental right to privacy.

The discussion also highlighted the inaccuracy of the technology used in surveillance, leading to false accusations. A civil society representative mentioned that when there is a pre-existing bias in the criminal justice system, it leads to a flawed database that is discriminatory against certain groups and communities and this is going to translate into bias in the surveillance technology used by the police or the government departments. This is particularly true concerning facial recognition technology (FRT) and other Artificial Intelligence (AI)-based technologies.

Participants emphasised the need for more transparency in how surveillance technology is used, and data collected and stored, especially in FRT and other Artificial Intelligence (AI)-based technologies.

A senior academic pointed out the difficulty in drawing the line between good and bad surveillance. It was noted that data protection and privacy are more technical than legal matters, and there is opacity about how metadata is being used. The police cannot provide safety without understanding the proper legal use of such technologies.

Overall, the discussion suggested a complex relationship between technology and surveillance, with both benefits and risks. While technology has made surveillance easier and more effective in some ways, there are also concerns about the potential for misuse and abuse. Participants expressed a need for transparency, oversight, and accountability measures to prevent these risks from materialising.

3.2.4. Private and government surveillance

Theme	Probed areas	FGD responses/comments
Private and government surveillance	What are the risks entailed in private surveillance?	• FGD respondents were unanimous in their concern for the increasing levels of surveillance by private companies and the collection of personal data for advertising or marketing purposes. • Some respondents pointed out how the government uses private companies for surveillance purposes to monitor and curb dissent, such as in the Pegasus controversy where a private company, NSO, sold spyware to governments across the world. • Private companies also use the data collected by them for influencing electoral outcomes.
	What are the risks entailed in government surveillance?	• Targeted surveillance by the government, such as interception of mobile phones and other communication devices, monitoring of social media activity, etc. is of particular concern. • The government has historically used surveillance, even in physical forms, to target and control certain sections of the community. For instance, police maintain history sheets for "known criminal" de-notified and nomadic tribes and criminalise these groups and control their movement.
	What level of surveillance is required/ justified?	• Some respondents were of the view that some level of private surveillance, such as CCTVs, is required for safety. Others believed that these technologies do not prevent crime or improve safety • Some of the participants felt that some form of surveillance that is regulated can be useful in crime investigation. For instance, phone tapping in some cases has helped the police build a strong case against criminals, particularly in cases of organised crime. However, the processes for permitting such surveillance need to be transparent, accountable and stringent.

The participants expressed concerns about the increasing use of private surveillance by companies to collect personal data for advertising purposes. They mentioned that companies are collecting data through mobile applications and social media platforms. The participants also discussed the use of CCTV cameras by private entities, such as shopping malls and residential complexes, for security purposes. Although some participants suggested that certain forms of private surveillance can be beneficial, others were concerned about the potential for misuse.

A journalist and privacy rights activist pointed out the nexus between private and public surveillance. He stated:

"Surveillance is a ubiquitous term that includes CCTV or it includes data flow that takes place to and from any device. So both are surveillance, but what we could focus on, is the surveillance by the state of the citizens, which could be one focus. But let's not forget surveillance capitalism, which is big companies surveilling us, is as much a part of surveillance as digital surveillance by the state. And because the state has a backchannel communication with big monopoly capital which does surveillance capitalism—Google, Facebook or Amazon or Adani or Ambani, for instance—you could therefore talk about surveillance as more than just what the state does... That's why I think it's correct that we put them both together as a larger picture of surveillance and focus on what are the elements of it that we should look at."

Regarding state surveillance, the participants expressed concerns about the government's surveillance practices, including the interception of phone calls, monitoring of social media activities, and the use of CCTV cameras in public places. Several participants, particularly journalists, academics, and civil society representatives, were against any form of unregulated government surveillance and compared it to an Orwellian surveillance state. However, some former police personnel believed that limited surveillance by the state, with proper legal and oversight mechanisms, was necessary for public safety and national security.

For example, a former police officer mentioned a study conducted in Himachal Pradesh, where CCTV cameras were installed and publicised, and their installation was found to have a deterrent effect on crime in that locality. He also noted that different categories of surveillance, such as the collection of metadata and the interception of the contents of communication, require different approaches to define what can be collected, what is legal or illegal, what information can be retained, and what oversight is necessary. He further gave the example of the ten agencies that have the power to intercept, and how the existing legal provisions categorising these agencies provide ample discretion to a large group of agencies and individuals to intercept communication with only weak administrative oversight. He gave the example of the UK, which has passed the Regulation of Investigatory Powers Act, of 2000 to check misuse of surveillance, and reiterated the need for India to enact a similar law.

Another participant emphasised the need to clearly define the scope of government surveillance and the characteristics and context for placing individuals under surveillance. One participant noted that the government and police have historically used surveillance against the public, citing the example of history sheets maintained by the police for "known criminals", which is a very loosely defined term for those who have been charged with cases or are suspects, and the discrimination inherent in including de-notified and nomadic tribes in the list. Such forms of surveillance have historically been a part of the police system in India, even though they are non-digital.

Overall, the participants had mixed views on the use of private and state surveillance. While some believed that certain forms of surveillance can be beneficial, others were concerned about the potential for misuse and the need for proper oversight and regulation.

3.2.5. Targeted surveillance by the government as a tool to curb dissent

Theme	Probed areas	FGD responses/comments
Surveillance as a tool to curb dissent	Does the government use surveillance as a tool to curb dissent in India?	• All of the FGD participants were unanimous in their opinion that, in the absence of clear legal oversight, surveillance is used as an excuse to suppress dissent and silence opposition. • When it comes to the police, while the use of surveillance technology by them is often inefficient and rudimentary, what it tends to do is have a chilling effect on people's freedom of speech and expression • There is also fear of violence from fundamentalist and reactionary sections of the population. • Two of the respondents, who suspect that they are being surveilled by the government said that this has a chilling effect on freedom of expression, yet the government refuses to be held accountable.
	How can target surveillance by the government be addressed?	• In targeted surveillance, the lack of awareness about being surveilled makes it difficult to seek any kind of legal redressal. It also has a chilling effect on journalists, activists and anyone voicing their dissent of the government due to the constant possibility of them being surveilled by the government without being able to verify it. • While hacking is different from surveillance and is undeniably illegal, it is also being used by the government for surveillance, such as the Pegasus spyware. Even for these illegal activities, the state refuses to be answerable.

During the focus group discussion (FGD), participants discussed the issue of targeted surveillance by the government as a tool to curb dissent. Many participants expressed concern about this practice and felt that it is a violation of basic human rights. They discussed cases where individuals or groups have been targeted by the government for their political views, social activism or other reasons. Participants also highlighted the use of surveillance technology to monitor social media and communication platforms to track individuals and groups perceived as a threat to the government.

All of the FGD participants were unanimous in their opinion that, in the absence of clear legal oversight, surveillance is used as an excuse to suppress dissent and silence opposition. One of the participants pointed out that while the use of surveillance technology by the police is often inefficient and rudimentary, what it tends to do is have a chilling effect on people's freedom of speech and expression.

One of the participants noted a vital difference between mass and targeted surveillance, in that, in the former, the subject is generally aware of being surveilled, while in the latter, the subject is not aware. This lack of awareness not only makes it difficult to seek any kind of legal redressal but also has a chilling effect on journalists, activists and anyone voicing their dissent of the government due to the constant possibility of unverified surveillance.

A former police officer pointed out how surveillance necessarily requires targeting and cannot be broad-based data collection. He gave the example of CCTV cameras to illustrate how, despite being a tool of mass surveillance, the analysis of the data collected using CCTV cameras has to be targeted in nature.

Two of the participants believed that they were under surveillance through the Pegasus spyware, and one of them, a senior journalist, explained how it has a chilling effect not only from the side of the government but also because of the fear of violence on the part of fundamentalist and reactionary elements. As stated by him:

> ***“I understand that my phone was compromised with Pegasus. It was revealed by the Citizen Lab in Toronto. We have a situation where the government of India and its agencies are refusing to cooperate with the Supreme Court of India and the technical committee appointed by the Supreme Court of India, headed by a retired judge of the Supreme Court. The government is not even answering a straight question—has any agency of the government of India purchased Pegasus or not? Yes, no? The complete refusal to answer this question, what does it mean? There are several governments across the globe, including the government of Israel where this private firm called NSO developed and designed this software, are themselves looking into this matter. Why, is a bigger question. But I’m coming into this with the whole notion of spyware, the kind of which nobody has seen in the history of humankind. In such a scenario, what is privacy, and what is surveillance? You can go into anybody’s phone at any point in time without that person knowing it, whether that phone is shut or not shut…. This is an issue that concerns several people across the world. The question is, in India, is it a matter of public concern? Should it be a matter of public concern?”***

Another senior journalist pointed out how several forms of surveillance used by the state could be considered strictly illegal and thus cannot even be termed “surveillance”. One such example is the hacking of the personal devices of individuals by the state or its agencies. However, even for these illegal activities, the state refuses to be answerable to the courts or is in complete denial of the act itself. In such a situation, as pointed out by a third participant, the distinction between hacking and surveillance gets blurred.

An international academic added to this point and said that not only is the line between hacking and surveillance blurred but so is the line between policing and punishment. Furthermore, such surveillance is often centralised and discriminatory.

Another academic further elaborated on the discriminatory aspect of targeted surveillance by giving an example from the US. In New York, the police would station unmarked cars outside mosques and Muslim neighbourhoods following the 9/11 terrorist attack, and they would take photographs of those entering the mosques or the locality.

3.2.6. Crime and surveillance

Theme	Probed areas	FGD responses/comments
Crime and surveillance	What are some of the dangers of using surveillance technology for tackling crime?	• Surveillance technology, particularly AI-based technology can be inaccurate as well as discriminatory. • Some participants felt that while such technology may be useful for curbing crime against certain vulnerable groups or particular types of crimes, the extent and process for use of these technologies need to be made very stringent. • Some participants felt that the technology may be useful for crime investigation if properly regulated.
	Does the police have the capacity to use these technologies for controlling crime?	• Police do not have the requisite training or capacity to continuously monitor or properly use the surveillance technologies. • There is a lack of knowledge regarding the proper use of the most basic forms of surveillance technologies such as CCTVs. • Budgeting for such technologies also needs to be questioned. The government invests in technologies such as CCTVs for women's safety although, in a majority of sexual assault cases, the offenders are known to the victim. The effectiveness of such investments needs to be studied.

There were differing opinions among the participants on the usefulness of surveillance technology in curbing crime. Some participants believed that there is no evidence to show that surveillance is effective in reducing crime in society, and that police in India lack the capacity to use these technologies to improve law and order. However, others believed that surveillance technology can be useful in preventing and investigating crimes.

Some participants noted the distinction between crime prevention and crime investigation. A former police officer suggested that surveillance technology, such as phone tapping, can be useful in building a case against an accused and charging criminals, particularly in organised crime such as drug rackets. However, they cautioned that the problem arises when the data is aggregated and the state uses the technology to track individuals of interest in an unchecked manner. Another participant agreed, noting that metadata can be more dangerous than the data itself.

A senior journalist pointed out the physical difficulty of using surveillance for crime prevention, as it requires continuous monitoring and the state lacks the necessary infrastructure and human resources. A former police officer highlighted the lack of legal oversight over intelligence agencies in India, which have been created through administrative orders and lack transparency in their functioning.

Another former police officer stressed the importance of surveillance for national security, personal safety, community safety, and the safety of women and children. However, they also called for clear demarcation of the boundaries of such surveillance and suggested that the system for putting individuals on technical surveillance needs to be reviewed and made more stringent to prevent misuse.

She noted how during her time serving in the police, individuals could be put on technical surveillance for a period of three days, after which the police were required to seek permission from the home ministry and then from the central government. She added that this system needs to be reviewed and made extremely stringent to prevent any misuse.

One participant questioned the usefulness of investing in public surveillance, citing the example of the Nirbhaya fund, which was used for installing CCTV cameras in public areas and transport. They argued that, since government data suggests that over 90 percent of sexual assault and rape incidents involve the victim knowing the abuser, such surveillance may not be effective in preventing these crimes.

A civil society representative cautioned against the police's use of technology for preventing or solving crimes. She stated:

> ***"One important point that we should also remember is that these databases that the police have already are the databases on which the technology is being built. So if there is bias in those databases, and discriminated communities have been included in them, the bias is also going to come into the technology. I'm talking specifically about facial recognition and other AI surveillance technologies here."***

Overall, the participants recognised the potential benefits and drawbacks of surveillance technology in addressing crime, emphasising the need for clear boundaries, legal oversight, and transparency in its use.

3.2.7. Right to privacy and oversight

Theme	Probed areas	FGD responses/comments
Oversight	What are some of how the misuse of surveillance technology can be addressed through legal mechanisms?	• While the participants of the FGD unanimously agreed with the *Puttaswamy* judgement, several participants questioned the applicability of the legal precedent in the absence of a proper legal statute supporting it. • One of the participants thought that the Data Protection Bill proposed by the government was not meant for surveillance reforms, but was instead simply aimed at getting consent from individuals for accessing and sharing their data. • Some of the participants suggested that there should be judicial oversight over any form of surveillance by the government in India to minimise discretion by police officers and other state agencies. • However, another participant noted the lack of awareness amongst the judiciary as well on issues regarding surveillance and the right to privacy, especially amongst the lower judiciary. • One of the participants suggested a grievance redressal model which included participation not just from the state and the judiciary, but also from the citizens, including the media and civil society representatives. The aggregate data on surveillance by the government should be made transparent for better scrutiny by all stakeholders.

While the participants of the FGD unanimously agreed with the judgment of the Supreme Court in the *Justice (Retd.) Puttaswamy vs Union of India* case of 2017, several participants questioned the applicability of the legal precedent in the absence of a proper legal statute supporting it.

The FGD participants emphasised the need for transparency and accountability in the surveillance process and suggested that individuals should have the right to access information about surveillance activities. They expressed concerns about the lack of an effective grievance redressal mechanism in place for addressing cases of misuse of surveillance and the need for an independent body to oversee complaints related to surveillance. They also discussed the role of civil society organisations in providing support and legal assistance to individuals facing surveillance-related issues. The participants emphasised that there should be legal remedies available for individuals who have been subjected to unlawful surveillance and that the legal system should be more responsive to complaints related to surveillance.

Some of the participants suggested that there should be judicial oversight over any form of surveillance by the government in India to minimise discretion by police officers and other state agencies. The police should seek warrants from the judiciary before carrying out any kind of surveillance activity, as pointed out by a former police officer.

As suggested by a former IPS:

However, another participant noted the lack of awareness amongst the judiciary as well on issues regarding surveillance and the right to privacy, especially amongst lower judiciary.

Regarding the attempts by the government to introduce data protection laws, one participant noted that the Bill introduced by the government was never about surveillance reforms. Instead, it only focused on the consensual sharing of information. It aimed at getting consent from individuals for accessing and sharing their data upon receiving notice from the government or private companies. However, the right to privacy against government surveillance was not covered in the Bill.

One of the participants suggested a grievance redressal model which included participation not just from the state and the judiciary, but also from the citizens, including the media and civil society representatives. He highlighted the lack of capacity of both administrative as well as judicial bodies to be able to regulate and monitor surveillance in keeping with the spirit of the *Puttaswamy* judgment. He mentioned how the aggregate data on surveillance should be made public to enable citizen oversight and prevent misuse.

Another participant stated that the issue of grievance redressal will only come up once proper procedures are laid down for surveillance by any state authority. Adding to this, another participant further problematised the issue of the lack of state capacity to have a grievance redressal system

"My personal view is that surveillance for national security, for personal safety, the safety of the community, the safety of women and children is doable, is accepted. For that also, the boundaries should be demarcated. But when it infringes upon the privacy of an individual, the processes need a review and need to be made very stringent. So that citizens who appreciate surveillance in their interest, in the interest of the community and nation are not fooled into devices and methods which infringe upon their privacy. Processes of surveillance should be very clearly defined, be very stringent, and also … judicial oversight should be introduced in India for any kind of surveillance."

that is both immediate and fair and how it can be taken down to the local level.

Overall, the participants stressed the importance of having a robust grievance redressal mechanism to protect individuals' rights and ensure accountability in the surveillance process.

3.3. In-depth interviews with police officers

Along with the focused-group discussions with subject-matter experts, some in-depth interviews were also conducted with high-ranking serving police officers. Attempts were also made to speak to senior police officers in other states but it seemed unfeasible within the time frame of the study. Officers of the ranks of ADGs handling the cybercrime units and law and order cells of two states were interviewed for this study. The names of the two states have been redacted here.

3.3.1. Functioning of the cybercrime cells

We spoke with a representative of the police department to understand the functioning of cybercrime cells in the state. Here are the key takeaways from the interview:

- **Types of cybercrimes:** A majority of the cybercrimes registered in the state pertain to financial fraud followed by sextortion. Many of these cases originate from the Mewat region of Rajasthan and Haryana.
- **Forensic labs and partnerships:** The construction of cyber forensic labs in each police station and one digital lab in the headquarter is in progress and will be inaugurated soon. Some of the police projects under the cybercrime unit are conducted in partnership with private companies such as Samsung, Paytm, and HCL. The state government also assists the police department by providing cyber experts.
- **Interception and permissions:** The cybercrime unit does not have permission to intercept any kind of digital communication. The permission is only granted via the Central government, who designates certain persons such as the Principal Secretary to grant such permissions. On a case-to-case basis, the principal secretary may grant permission for an interception to IG-level and field officers for a period of two to three days.
- **Training and awareness programs:** Across the state, more than 5,000 police officers have been trained to deal with cybercrimes. Sometimes, technical matters are outsourced to technical experts. The police department organises a cyber awareness program every month for the public at different locations. Efforts are underway to train Inspectors and SIs in a phased manner so that every police station can deal with cybercrimes independently.

3.3.2. Surveillance and law-and-order

Upon interviewing a representative of the law-and-order department of a state police department, we got insights into the state's approach to monitoring social media and maintaining law and order. The expert shared that there are social media monitoring cells in all the districts, field units, range headquarters, and police zones. These cells monitor rumours online, identify the groups spreading the rumours, sensitise people on such issues, and collect field information.

The expert cited a few examples of successful social media monitoring by the police, including a 2017 rumour of caste-based conflict, which was controlled by the police, and multiple cases filed against an Indian journalist and co-founder of Alt News, Mohd. Zubair, which was monitored by the police[2]. The expert

[2] Mohammed Zubair, the co-founder of a fact-checking website called AltNews was arrested by the Special Cell of the Delhi Police in June 2022 for allegedly hurting religious sentiments after a complaint by a social media user with regard to a tweet from 2018. His arrest was heavily criticised by various groups and bodies, including Editors Guild of India. For more details, see: https://www.outlookindia.com/national/arrest-of-journalist-mohammad-zubair-what-happened-and-how-media-and-opposition-reacted-news-205195.

also mentioned the police's use of artificial intelligence for monitoring social media, with funds for these technologies provided by the state (Anand, 2022; Outlook, 2022).

The expert talked about an incident in March 2016, where fake information was being spread on social media, causing a communal disturbance in the state. The quick response by the social media unit prevented the violence from spreading.

Regarding phone interception, the expert shared that for any kind of phone interception, the police need to seek permission from the 'ADG zones', who further seek permission from the highest-level officers, and there is a strict chain of command that needs to be followed to do any kind of phone interception of an accused or suspect.

The expert also shared that the police undertake physical surveillance regularly and maintain a crime register, which includes wanted persons, habitual offenders, and history sheeters. Physical verification of all these categories of people is done by the police.

The expert, a serving police officer, opined that police should have the discretion to conduct surveillance in the interest of law and order and public safety. However, in the state, there are no rules framed under the Criminal Procedure (Identification) Act, of 2022.

When it comes to technology for law and order and *'bandobast'* purposes, the police mandatorily deploy drones. However, Facial Recognition Technologies (FRTs) are not being used by the department, although they are included in the plan under the 'Safe City Project'. The CCTVs installed on the streets by the government are managed and monitored by the Local Nagar Nigam. The expert also shared that while in Telangana, it is mandatory to link the CCTV feed of private players with the police department, no such provision exists in the state, inhibiting police access to information.

The expert also mentioned that the police department have their fact-checking handles as well as an NRI handle on platforms such as Twitter, and the response time on these handles is eight minutes.

The interviewee believes that police should have the discretion to conduct surveillance in the interest of law and order and public safety.

3.3.3. State of surveillance and law-and-order

The interviewee stressed the need for a national intelligence law similar to that of the UK, where all organisations, including intelligence agencies, are brought under the same banner and proper oversight is ensured over the kind of surveillance being undertaken by these agencies. He also emphasised the need for a specific data protection law in India that includes the data collected by police departments across the country.

According to the interviewee, the police in India currently lacks the capacity, infrastructure, or necessary permissions to conduct intensive surveillance on citizens. He pointed out that police often send notices to online social media platforms to access digital communication information, but they receive no response. He believes that it is necessary to study why the platforms regularly fail to respond or provide information to the police.

Regarding gathering information about an accused or a suspect, the interviewee mentioned that in an adversarial system like India, the police are not required to seek judicial warrants. However, he believes that the police should not overreach their basic mandate and should use discretion to resolve matters. He is also against the idea of women's cells, as he believes it is not the job of the police to counsel people. Instead, the police should limit their functioning to the registration and investigation of cases, and the registration of FIRs should be done without any discretion on part of the police.

The interviewee mentioned that during investigations, the police maintain a properly documented paper trail for the investigation, and there is internal supervision over such investigations, which works well in the police department. For any kind of surveillance over an accused or suspect, such as phone tapping, the police need to seek permission from the Home Ministry, which has a Review Committee for oversight into these kinds of cases.

The interviewee stated that while the police lack the infrastructure or the capacity to undertake any kind of surveillance, it is regularly done by non-regulated political intelligence agencies.

The interviewee stated that there is no discrimination by the police against any community or group in India since there is sufficient representation from all communities in the police department. There is a higher representation of inmates from certain communities, such as the de-notified tribes (DNTs) in prisons because historically, they are more inclined to commit crimes. There are no illegal arrests or detentions undertaken by the police, in his view. He mentioned that the police cannot use data, such as fingerprints, available with the UIDAI (Unique Identification Authority of India), for crime investigation purposes.

Regarding cybercrime, the interviewee suggested enforcing the KYC (Know Your Customer) mandate for opening any kind of digital or financial profile. This will enable the police to track and identify the accused. After working for six years in the cyber cell of the police, the interviewee found that there is no political pressure for undue surveillance of citizens, in his view. He felt that to enact the Criminal Procedure (Identification) Act, of 2022, a proper infrastructure needs to be built to ensure data storage and protection.

Conclusion

The issue of digital surveillance in India is a complex and multifaceted one. Thus, for this study, experts' opinions, perceptions and experiences have also been sought so as to put some of the survey findings into context and fill some of the gaps in the data.

While survey findings show a lack of concern regarding surveillance and infringement of privacy among the general public, experts' opinions, perceptions and experiences reveal a deep concern over unchecked surveillance, particularly by the government. Even as there was a difference of opinions regarding the utility of technologies such as CCTVs for crime prevention and investigation, the participants were unanimous in their opinion that in the absence of legal oversight, the government is using surveillance as a tool to silence opposition and suppress dissent, which can have a chilling effect on freedom of speech.

The FGD participants also pointed out the lack of proper understanding of the issue and its context amongst the general public, particularly in framing concerns related to the right to privacy. Issues such as the right to privacy are not properly understood by the public in usual circumstances. However, when it comes to their own private spheres, people's support for surveillance is bound to decrease. They also highlighted the class differences in the level of understanding, with the poor being less likely to support intrusion in the form of surveillance.

The participants cautioned against the use of surveillance technologies by the police or other pillars of the criminal justice system due to their inaccuracy and inherent bias, and called for clearer and more stringent oversight mechanisms to prevent any misuse of the discretionary powers available with the police. On the other hand, both the retired police personnel who participated in the FGD as well as serving police personnel who were interviewed separately highlighted the lack of the technical as well as human resources within the police to be able to carry out even the most rudimentary forms of digital surveillance. They stated that the police departments in India lack the knowledge, the necessary infrastructure and skills as well as the requisite legal framework to be able to undertake any surveillance or to be able to intelligently parse through the information within the existing surveillance systems such as CCTVs.

However, all FGD participants were concerned about the lack of legal oversight in the police interception of communication devices and monitoring of individuals' online activities. While all of the FGD participants felt that clearer and more stringent oversight mechanisms need to be put in place to prevent any misuse of the discretionary powers available with the police, contrary views emerged from the in-depth interviews with serving police personnel. The latter were of the opinion that police does not have any discretion in the interception of communication devices or social media monitoring and instead pointed to the administrative oversight already in place, which in their opinion was sufficient to prevent any misuse.

Overall, the FGD participants reiterated the impact of unsupervised surveillance on people's freedom of speech and expression and right to privacy, and called for judicial oversight to prevent such misuse and minimise discretion by the police. The issue of digital surveillance in India is a critical one that requires a balance between the benefits of technology and individual rights and freedoms.

List of participants in the Focused Group Discussion

1. Anushka Jain, Policy Counsel, Internet Freedom Foundation
2. Apar Gupta, Executive Director, Internet Freedom Foundation
3. Arvind Verma, former IPS officer and Professor, Criminal Justice, Indiana University
4. Beatrice Jauregui, Associate Professor, Centre for Criminology & Sociolegal Studies, University of Toronto
5. Gagan Sethi, Vice-Chairperson, Centre for Social Justice
6. Manoj Mitta, senior journalist
7. Meeran Borwankar, former IPS officer
8. Nandkumar Sarvade, former IPS officer
9. Osama Manzar, Founder and Director, Digital Empowerment Foundation
10. Paranjoy Guha Thakurta, senior journalist
11. Prabir Purkayastha, Editor, NewsClick, and Advisory Board Member, Software Freedom Law centre
12. Sanjay Sahai, former IPS officer and Director, TechConPro Pvt Ltd
13. Vibodh Parthasarthi, Professor, Media Studies, Jamia Milia Islamia University

List of serving IPS officers interviewed

1. Brijesh Singh
2. Prashant Kumar
3. Subhash Chandra

References

Amnesty International India. (2019). Bhagalpur Blinding Case. Retrieved from https://www.amnesty.org.in/bhagalpur-blinding-case/

Anand, U. (2022, July 19). Supreme Court Restrains UP Police from Arresting Mohammed Zubair in New Case. New Delhi, *Hindustan Times*. Retrieved from: https://www.hindustantimes.com/india-news/sc-restrains-up-police-from-arresting-zubair-in-new-case-101658170618682.html

Outlook Web Desk. (2022, June 28). Why Was Mohammed Zubair Arrested? Here's Why Press Bodies Are Calling It 'Disturbing'. *Outlook*. Retrieved from: https://www.outlookindia.com/national/arrest-of-journalist-mohammad-zubair-what-happened-and-how-media-and-opposition-reacted-news-205195.

Chapter 4:

Surveillance in the Media: Analysis of News Coverage on Digital Surveillance

Key findings

- Nearly three out of four selected news items on surveillance rely on government agencies as their primary source.
- One out of four news stories on surveillance have a supportive or pro-surveillance approach.
- Times of India and Dainik Jagran were more likely to have pro-government stories on surveillance, The Wire was most critical of the government.
- Nearly two out of three news items are on the use of surveillance technology for public safety and order. Just about one-fourth of the selected news stories on surveillance are primarily focused on human rights.
- Stories on CCTVs and drones least likely to include debates around their legality or right to privacy.
- Of the total sampled stories on surveillance, less than 14 percent mention right to privacy or legality of the surveillance.

CHAPTER 4

Surveillance in the Media: Analysis of News Coverage on Digital Surveillance

Digital technologies that have transformed our lives have also compromised our personal and financial security. The technology used for surveillance has been changing so fast over the past decade that it is tough for citizens, academics and civil society groups to keep track of new methods, networks, equipment, etc. and their evolving implications.

Even as the surveillance net increases, there is little information freely available in the public domain to examine its impact. It is also difficult to make sense of surveillance through legal processes because fewer cases come up in the courts and the law always takes time to catch up with emerging technology. Government agencies and their information networks share very little information and Right to Information (RTI) queries are often turned down in the name of public safety or national security (Chauhan, 2022; Bhatnagar, 2022).

In such an environment of a near data and information vacuum, day-to-day media coverage of surveillance and related issues provides a valuable source of information about society's daily encounters with technologies and mechanisms related to surveillance. While media outlets are often divided on their opinions and attitudes about surveillance, a certain amount of daily news emanates from the use of surveillance methods such as CCTV cameras, drones, Facial Recognition Technology (FRT), and phone tapping of individuals.

It is common to find statements of politicians and other authority figures talking about the benefits of such technologies or making claims about their deployment in the news. Delhi Chief Minister, Arvind Kejriwal, has on multiple occasions claimed credit for the national capital having the highest number of CCTV cameras in any metro city in the world (The Hindu, 2021). The police also make claims in press conferences about solving crimes with the use of surveillance technologies. Media often carry visuals and pictures of in situ use of such technologies which provide a clue to things that are not readily available in the public domain. They also carry occasional news items, editorials or opinion pieces about privacy and constitutionality which offer a glimpse of the public discourse on the subject.

As surveillance technologies become ubiquitous in both public as well as private spheres, the depiction of surveillance in the media follows suit. Hence the media coverage of digital surveillance, whether by the state, the police or private entities, provides a unique opportunity to get an idea of the larger public opinion and public discourse regarding the use of such technologies. An analysis of the media content on the issues can thus triangulate many of the findings from other sources on public opinions and perceptions in order to enhance our understanding of these issues.

In this chapter, we study the media portrayal of surveillance technology usage by the state and the police. The attempt here is to use the media as an instrument to understand different aspects of surveillance through the lenses of human rights, national security, public safety, and technology use. The primary objective of this chapter is to make sense of surveillance through the eyes of the media and try to unravel its omissions and commissions in the process of day-to-day coverage.

This chapter is divided into the following sub-sections:

Section 1 provides a brief overview of the data selection process and the methodology used for the media analysis. For further details regarding the methodology, please refer to Appendix.

Section 2 provides details of the frames used for the analysis of selected media reports

Section 3 reports broad findings relating to the agencies involved in surveillance, as per media reports; the linkages between surveillance and criminal justice agencies; and the slant of the stories selected in the sample.

Section 4 presents the findings under the human rights frame on issues such as illegal surveillance of activists, journalists, and those opposing the government, mobile surveillance, social media surveillance, misuse of surveillance technology, and the coverage of issues such as the Pegasus scandal

Section 4 includes findings under the national security frame such as the role of surveillance in ensuring national safety and integrity

Section 5 presents findings on the role of surveillance vis-à-vis crime, law and order, and public safety, as reported by the media

Section 6 is about the reportage of new forms of surveillance technology, their installation in various public, semi-public, and private places and their proclaimed efficiency as well as legitimacy.

4.1. Data selection and methodology

For this analysis, news items from six media outlets were selected for the sample-- two English and Hindi mainstream newspapers each, and one English and Hindi digital-only outlet each. The newspapers were selected mainly on the basis of their circulation and reach. News stories from the *Times of India* and *The Indian Express* were identified and selected in English, and *Dainik Jagran* and *Dainik Bhaskar* in Hindi. It needs to be noted, however, that only digital archives from the newspapers' websites were used during the sampling process. Amongst the digital-only media outlets, *The Print* from English and *The Wire* from Hindi were selected. However, no reliable source for the ranking of digital-only media outlets was available.

For data collection, a pool of keywords was created in both Hindi and English. These keywords were used to search for relevant news items from the selected media outlets. The time frame for the sample was one year, beginning from July 1, 2021, to June 30, 2022. An elaborate coding sheet was created after multiple brainstorming sessions to analyse stories for a pilot. Inputs from the pilot were further used to improve the coding sheet. The process was repeated twice prior to the final data entry.

A total of 1,162 news items were selected from the six media outlets. Prior to the analysis, the data was vetted and cleaned after weeding out duplicate entries and non-relevant stories.

Post data cleaning, the final sample size reduced to 1,113 news items, which were used for the final analysis as presented below. The distribution of the sample across the various media outlets is provided in Table 4.1.

4.2. Frames for content analysis

Media scholars have relied on 'frames' to understand, interpret, and evaluate information emanating from media coverage. Organising diverse story themes under frames helps set parameters that create clusters and

Table 4.1: Sample share of media outlets

Language	Media outlets	Number of stories	Percentage share
English	The Times of India	205	18%
English	The Indian Express	208	19%
English	The Print	183	16%
Total sample share of English Media		**596**	**53%**
Hindi	Dainik Bhaskar	194	17%
Hindi	Dainik Jagran	192	17%
Hindi	The Wire	131	12%
Total sample share of Hindi Media		**517**	**46%**
Total overall sample		**1113**	**100%**

typologies around happenings or public events as depicted in their media coverage. It's an interpretive process for selecting aspects of reality as perceived by the media.

As a communications research method, media framing analysis unravels media coverage by looking at media's routine selection processes, i.e., how certain issues are picked up at the expense of certain other issues, and what factors are built into media's routine work skills and practices which influence such decisions. To frame an issue, according to Entman, is to select some aspects of a perceived reality and make them more salient over others in ways that promote certain types of definitions, evaluations or interpretations (Entman, 2010).

An important part of media's professional skillset is to select and prioritise its sources, theme or location in ways that bring into play the prevalent social, cultural, or economic conditions and the society's dominant ideologies and belief systems. The frames help audiences in locating, perceiving, identifying, and labelling the information disseminated by the media (Greenberg & Hier, 2009; Semetko & Valkenburg, 2000). The methods of media framing research combine qualitative and quantitative aspects of content analysis techniques.

With this understanding, the analysis identified four broad frames within which a certain type of news items and the themes covered in them could primarily be categorised. These are human rights, national security, public safety, and technology. A broad definition of these frames is as follows:

1. Human rights frame: This included stories that primarily raised issues of citizens' fundamental rights such as the right to privacy, spying on individuals, social media monitoring, controlling or criminalising dissent, legality or constitutionality of digital surveillance, and the deliberate use of hate speech.
2. National security frame: This included stories that referred to digital surveillance in the context of cross-border or maritime security, separatism, insurgency, internal conflict, Maoism, Naxalism, incitement to violence, public unrest, cyberattacks, and intelligence gathering.
3. Public safety frame: Stories mentioning the use of surveillance technologies for public order and safety, the safety of women and children, crime reduction or prevention, investigation, road safety, and prevention of police misconduct were categorised under this frame.
4. Technology frame: This included stories that focused on technological aspects of various types of surveillance methods such as drones, CCTV cameras, FRT, etc.

Table 4.2: Nearly two out of three news items are on the use of surveillance technology for public safety and order

News items categorised by type of frame		
Frames	**No. of stories**	**Percent**
Human Rights Frame	297	27
National Security Frame	92	8
Public Safety Frame	696	63
Technology Frame	377	34

Note: The total number of cases in the frames is greater than the sample size as some of the stories share more than one frame.

Table 4.3: Most selected news outlets likely to report on surveillance through the lens of public safety

Name of the outlet	Human rights	National security	Public safety	Technology
Times of India	21	4	64	39
The Indian Express	22	11	64	36
The Print	30	14	63	26
Dainik Bhaskar	11	5	76	37
Dainik Jagran	9	8	78	37
The Wire	89	7	14	26

Note: All figures are in percentages and are rounded off. The aggregate of frames is greater than the total sample size as multiple frames occurred in one story.

As seen in Table 4.2, the highest proportion of stories fell in the public safety frame (63%) while the lowest was reported in the national security frame (8%). A lesser proportion of stories primarily covered human rights-related issues (27%) and, technological innovations and advancements (34%). It needs to be noted that some stories had more than one primary frame, thus the total number of stories as categorised under each frame is higher than the total selected sample size.

Except for The Wire, all other news outlets reported a high proportion of stories on public safety issues. As compared to other frames, the number of stories under national security frames remained quite low. Out of the six outlets, The Print and The Indian Express made an exception by contributing the highest proportion of stories under this frame (Table 4.3).

4.3. Broad findings

4.3.1. Institutions and actors conducting surveillance, primary sources and main actors

State actors played a key role in targeted as well as mass surveillance (though a segregated analysis of the two issues was not undertaken). Across agencies or institutions that are involved in digital surveillance, more than half of the stories reported state actors as the key players (Table 4.4).

Primary sources and main actors of the news story set the definition of the subject matter being discussed. The government (30%) and police (38%) are the most frequently cited primary sources for the sampled stories. Only eight percent of stories quoted studies/reports and around six percent of stories quoted civilians and civil society organisations as their primary source (Table 4.5). Hence media

Table 4.4: Two out of five news stories refer to the government and the police as key players conducting surveillance

Institutions playing key role in conducting surveillance	Percentage
State actors	
Government	39
Police	42
Other state agencies	19
Politicians	5
Non-state actors	
Civilians/Individuals/RWAs	7
Private bodies/organisations	3
Foreign agency/government	1

Note: All figures are in percentages and are rounded off. As the question had multiple choices, hence, the total percentage is greater than the sum of sample size. Other State agencies include hospitals, educational institutions, zoos, fire stations security agencies, armed forces and prison authorities etc.

coverage of surveillance is largely driven by information provided by state agencies such as the police which is likely to have a bearing on the overall slant of the stories.

Consistent with the above trend, the news items studied were significantly more likely to cite the government and its various agencies as the main actors in the news items, compared to private or other non-government actors. As seen in Table 4.6, more than half of the stories cited the government as the main actor in such stories, 74 percent cited the police, prisons, and intelligence agencies and another 29 percent cited other state actors as the main actors in the story. In contrast, nearly one out of three stories mentioned private actors as the main actors and as few as eight percent mentioned experts or civil society as main actors.

Table 4.5: Nearly three out of four selected news items on surveillance rely on government agencies as their primary source

Primary sources as quoted in the stories		Percent
Private sources	Studies/Reports	8
	Civilians and civil society organisations	6
	Corporate/Business entities	2
Total private sources		**16**
Government sources	Government	30
	Police	38
	Politicians	4
	Defence officials	1
Total government sources		**73**
	Foreign government	1
	Without or unidentified source	11
Total other sources		**12**
Total primary sources		**100**

Note: All figures are in percentages and are rounded off.

Table 4.6: Three out of four of the selected news stories on surveillance focused on government agencies such as the police, prisons, and intelligence agencies as the main actors

Main actors depicted in the stories	Percent
Police, Prison & Intelligence Agencies	74
Government	51
Private Actors	33
Other State Actors	29
Politicians	15
Judiciary	12
Security Forces	11
Experts and Civil Society Organisations	8
Foreign Governments	4
No Agents Specified	3
Extremist/ insurgent organisations such as left-wing extremists, etc.	2
Other	1

Note: All figures are in percentages and are rounded off. It was a multiple-choice question with the option of selecting more than one main actor. Hence, the total of actors who appeared is greater than the sample size (N). (N=1113). Others include the administration of different religious places i.e. temples, mosques, gurudwara etc.

Figure 4.1: Translated - Jodhpur integrated CCTV control and command room. (Dainik Bhaskar, Aug 8, 2021)

4.3.2. Surveillance and the criminal justice system

Despite the fact that the data selection process did not involve the deliberate use of terms related to the police or other criminal justice agencies, the analysis revealed that 63 percent of the sample referred to the police in some form. On the other hand, other institutions within the justice system, the judiciary (17%) and prisons (6%), had a markedly lower representation in the media stories that included surveillance of some kind. Overall, a significant majority of the sampled stories, more than 85 percent, referred to either of the three institutions in their reporting of digital surveillance, while 14 percent had no reference to any of the three institutions.

Table 4.7: Nearly two out of three stories on surveillance mentioned the police

Institutions	Proportion of news items that referred these institutions		
	Yes	No	Unclear
Police	63	37	1
Judiciary	17	83	0
Prison	6	94	0

Note: All figures are in percentage and are rounded off.
Questions Asked: Are the following mentioned in the story?

4.3.3. Type of news coverage and slant

Across the categories of news items on surveillance, the highest proportion of stories were hard news stories (48%), followed closely by new features (39%). On the other hand, just about six percent of the sample were editorials/op-eds or opinion features, thus indicating that the issue of surveillance rarely becomes a matter of deeper deliberation by the media through public discussion or debate, and instead, its coverage in the media is to a large extent based on just factual news.

The analysis revealed that 26 percent of the sampled news items had a pro-surveillance slant, while 20 percent had an anti-surveillance slant. The majority of the sample, however, fifty-four percent, did not have any discernible slant (Table 4.8).

Table 4.8: One out of four news stories on surveillance have a supportive or pro-surveillance approach

Slant of media coverage on the issue of surveillance	Percent
Supportive or pro-surveillance approach	26
Critical or anti-surveillance approach	20
No discernible approach	54

Note: All figures are in percentages and are rounded off.
N=1113.

More than one out of ten news items (12%) had an anti-establishment slant, as against eight percent which had a pro-establishment slant. Here again, though, a majority of the sample, 80 percent, did not have any discernible slant (Table 4.9).

Table 4.9: Eighty percent of the news items on surveillance did not have any discernible political slant vis-à-vis the government

Political slant of the news items on surveillance vis-à-vis the government	Percent
Clear pro-government slant	8
Clear anti-government slant	12
No discernible slant	80

Note: All figures are in percentages and are rounded off.
N=1113.

Across the selected media outlets, aside from The Wire, the agencies were most likely to have no discernible slant. The Wire, on the other hand, had more than 57 percent of stories with a critical slant vis-à-vis the government. Amongst print media, The Times of India, Dainik Jagran, and Dainik Bhaskar were most likely to have a pro-government slant, with more than 10 percent of their sampled proportion reflecting a clear pro-government slant (Table 4.10).

Table 4.10: Times of India and Dainik Jagran were more likely to have pro-government stories on surveillance, The Wire most critical of government

Name of the outlet	Items with a pro-government slant	Items with a critical slant to government	Items with no discernible slant
Times of India	13	9	79
The Indian Express	5	8	88
The Print	4	14	81
Dainik Bhaskar	11	0.5	89
Dainik Jagran	13	0.5	87
The Wire	0	57	43

Note: All figures are in percentages and are rounded off.

When we look at the approach of individual news outlets towards the overall issue of surveillance, we find that the Times of India was most likely to have a pro-surveillance approach (51%), while The Wire was most likely to have a critical approach towards surveillance (76%). All other media outlets reported more than half of their stories without any discernible approach vis-à-vis surveillance (Table 4.11).

4.3.4. Mode of surveillance

The most frequently reported mode of surveillance was the CCTV camera, with more than one out of two stories (56%) referring to it. This was followed by a much smaller proportion of coverage to the Pegasus spyware (16%) and drones (12%). It is significant that a negligible number of the stories (4%) referred to a slightly more advanced surveillance technology of facial recognition (Table 4.12). Stories containing targeted surveillance mostly tended to be about nabbing a criminal using surveillance technology i.e., tracing phone location, and accessing CCTV footage.

In one case reported by The Indian Express, gait analysis technology was used in a criminal case to identify the pattern of the body gestures which helped the police prove charges in a case of murder and rape which eventually led to conviction and death sentence (Modak, 2022). Even as the level of accuracy of such technologies is unproven and still under debate, its increasing use by the police and other government agencies appears to be largely unquestioned in the media coverage on surveillance.

Table 4.11: Over half of analysed Times of India stories are pro-surveillance

Name of the Outlet	Pro-surveillance	Critical towards surveillance	No discernible approach
Times of India	51	16	34
The Indian Express	22	17	61
The Print	20	24	56
Dainik Bhaskar	25	2	73
Dainik Jagran	27	4	69
The Wire	0.8	76	23

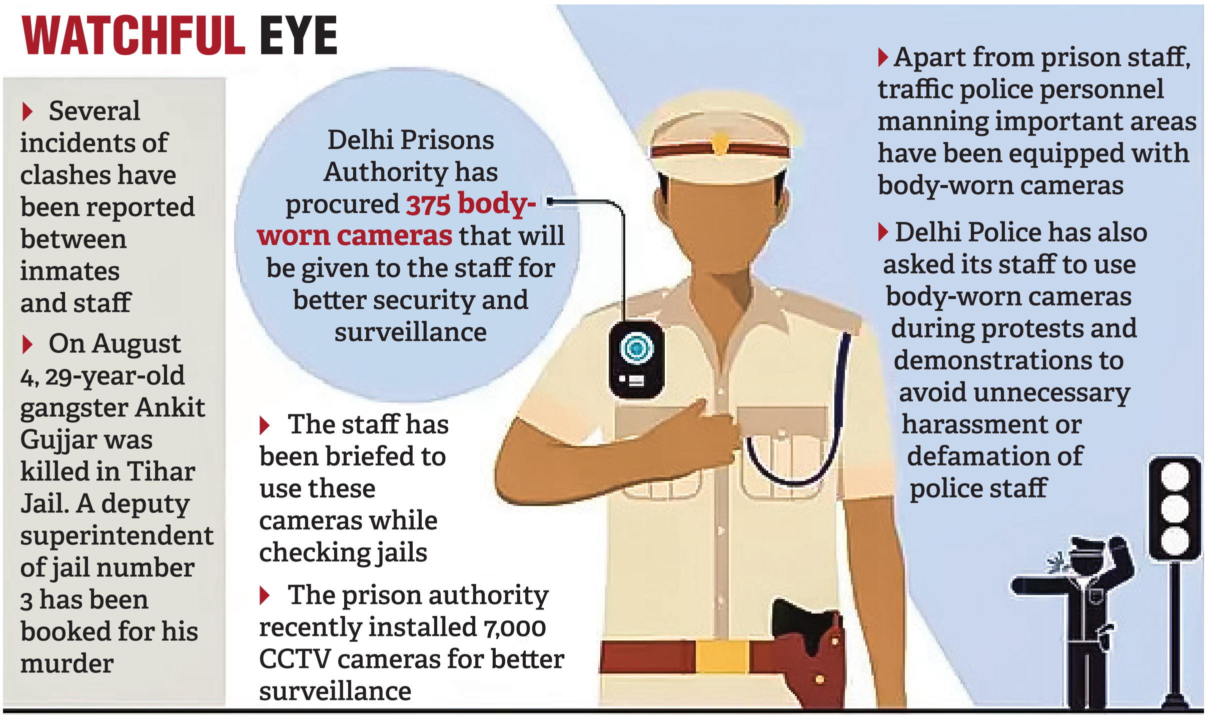
Note: All figures are in percentages and are rounded off.

Table 4.12: More than half the news items on surveillance focus on the use of CCTV cameras as the primary mode of surveillance

Most frequently reported mode of surveillance in news items.	Percent
CCTV	55
Pegasus	16
Drones	12
Spywares, malwares, other tools of hacking/personal devices	10
Hacking phone/personal devices/ websites	9
Illegal phone tapping	7
GPS/IP/Phone location tracing	5
FRT	4
Video surveillance in personal spaces/through hacking of personal devices	3
Authorised phone tapping	2
GPS on vehicles	2
Aadhaar	2
Others*	12

Note: All figures are in percentages and are rounded off. Since this was a multiple-choice question, the sum total will be greater than 100 percent. N=1113.

*The category 'Others' include surveillance modes that were reported in one percent or less of the sample. These are: Fasttags, algorithms, biometric data, automatic number plate recognition, body cameras, physical surveillance, Central Control Command Centre, fabrication of evidence, social media monitoring, artificial intelligence, technical surveillance, cybercrime, cyber security, cyber-attacks, etc.



WATCHFUL EYE

- Several incidents of clashes have been reported between inmates and staff
- On August 4, 29-year-old gangster Ankit Gujjar was killed in Tihar Jail. A deputy superintendent of jail number 3 has been booked for his murder

Delhi Prisons Authority has procured **375 body-worn cameras** that will be given to the staff for better security and surveillance

- The staff has been briefed to use these cameras while checking jails
- The prison authority recently installed 7,000 CCTV cameras for better surveillance

- Apart from prison staff, traffic police personnel manning important areas have been equipped with body-worn cameras
- Delhi Police has also asked its staff to use body-worn cameras during protests and demonstrations to avoid unnecessary harassment or defamation of police staff

Figure 4.2: Description of the body cams. (TOI Oct 13, 2021)

For several specific forms of surveillance, which are under-reported in the media, the use by police and other agencies may have a bearing on citizens' rights and the functioning of the justice system. For instance, while the fabrication of evidence by state agencies is mentioned in less than one percent of the sampled stories (Table 4.12), its use to curb the right to dissent has been covered, though sparsely, in individual reports. Activists Surendra Gadling and Rona Wilson, as reported by The Wire, were surveilled by the police and false evidence was reportedly planted against them by these agencies. The stories quoted the fact-finding research done by American forensic firm Arsenal and cyber security firm Sentinel One. The report noted that the false evidence was planted through the hacking of private gadgets of the rights activists (The Wire Staff, 2022; Shanta, 2021) as early as two years before their arrest.

4.4. Surveillance and human rights

The media, often referred to as the fourth pillar of democracy, is bestowed with the responsibility to keep a check on the state by reporting on the misuse of authority and violations of human rights. Therefore, in this analysis, we study the media coverage of surveillance through the lens of human rights. As in the case of any other state activity, particularly the functioning of the police and other pillars of the criminal justice system, digital surveillance too has vast potential for misuse by the state and its agencies and thereby the potential to infringe upon individuals' human rights and citizens' right to expression and dissent.

4.4.1. Human rights violation

The analysis reveals that more than a quarter of the sampled news stories (26.4%) referred to some form of human rights violation by the state or the police using surveillance technology. For instance, as reported by the Times of India (2022), a petition was filed by SQ Masood, a Hyderabad-based social activist, who contended that the police in May 2015 stopped him in traffic and took his photos without consent even though there were no existing criminal charges against him. "The continued use of Facial Recognition Technology by the police violates the privacy of individuals which was upheld by the Supreme Court's Aadhaar judgment. The use of such technology without any authorisation from the law should be declared unconstitutional and illegal", the news item quoted K Manoj Reddy, the counsel of Masood as saying (Times of India, 2022).

Table 4.13: More than 80 percent of the news stories within the human rights frame cover issues related to individual's privacy

News items reporting on surveillance with respect to Human Rights concerns	Percent
Individual's privacy/snooping/spying	81
Data privacy	48
Freedom of expression	38
Dataprotection	35
Legality/constitutionality	34
Freedom of movement	29
Controlling political opposition	21
Controlling/criminalising dissent	18
Aadhaar	7
Discrimination against/targeting minority	3

Medical information	2
Discrimination against/targeting caste	2
Discrimination against/targeting Women	2
Violation of freedom of religion/faith	2
Others*	2

Note: All figures are in percentages and are rounded off. Since this was a multiple-choice question, the final sum of percentages will be greater than 100. (N=297).
*Others includes sub-categories with one percent or less frequency. These are: falsely implicating someone by planting digital evidence, social media monitoring, hate speech, discrimination against or targeting of gender/sexual minorities, and discrimination against or targeting of the poor.

As seen in Table 4.13, the largest proportion of stories under the human rights frame covered issues related to individuals' privacy, snooping or spying (81%), followed by issues of data privacy (48%). Notably, however, even within the stories that covered human rights related issues, just one in three touched upon the legal or constitutional aspects of such surveillance.

Issues such as discrimination against or targeting of certain communities or individuals, such as religious minorities, received extremely scarce media coverage, even within the human rights frame. This omission is significant in the context of increasing state or police surveillance, particularly in crime prevention and investigation.

While overall a significant proportion of the sample reports fall under the human rights frame, when we disaggregate the data by various news outlets, a skewed picture emerges. Amongst all the news outlets studied, The Wire was most likely to report on human rights issues vis-à-vis surveillance technology, with as much as 11 percent of the overall stories falling under this frame (Table 4.14).

Table 4.14: The Wire most likely to report on human rights aspects of surveillance

Name of the outlet	Stories covered under human rights frame
The Wire	11
The Print	5
Times of India	4
The Indian Express	4
Dainik Bhaskar	2
Dainik Jagran	2

Note: All figures are in percentages and are rounded off. N=1113.

A typical story in Dainik Bhaskar talks about the efficacy of CCTV surveillance. The screengrabs of the footage show angry dissenters vandalising public property. The youth were protesting against 'Agnipath Scheme' related to recruitment in defence services brought by the central government (Dainik Bhaskar, 2022). The CCTV footage later on was used to single out those involved in protest demonstrations. A similar story was reported by The Wire. Police used CCTV footage to make posters of the dissenters who were protesting against incendiary comments on Prophet Mohammad. One of the embedded tweets in the thread reads, "In the incident of June 10, cases were filed under 29 serious sections. 92 yet arrested. 40 named in FIRs, spotted in CCTV footage are absconding & being chased. If they don't surrender, warrants will be issued, houses will be auctioned under relevant sections of law: SSP Prayagraj." (The Wire Staff, 2022)

4.4.2. Gagging dissent and opposition

Freedom of expression and the right to dissent are integral components of our constitution. However, some stories noted that the surveillance technology installed for improving law and order and the overall safety of people can also be used for supressing dissent. For instance, CCTV surveillance technology was used for monitoring the 2020-21 farmers'

Figure 4.3: Police issued posters of 59 accused of stone pelting incident after Friday prayers on Atala and Noorullah road in Allahabad city. (Photo_PTI) (The Wire, June 16, 2022)

protests on the outskirts of Delhi (Dainik Bhaskar, 2021).

Overall, however, stories about controlling or criminalising dissent and political opposition by using surveillance technology appeared only in around five percent of the coverage studied. However, when seen as a percentage of the stories that focused mainly on human rights issues, this emerged as a significant theme, with 18 percent of the stories with human right as the primary frame reporting on controlling or criminalising dissent, 21 percent reporting on controlling political opposition, and 38 percent covering issues related to freedom of expression (Table 4.15).

The use of surveillance technology for controlling dissent has also been commonly used in other parts of the world, most recently in Hong Kong, where protesters used masks and umbrellas to stay anonymous (Smith, 2019). Such selective targeting is bound to have a chilling effect on the people participating in any protests or voicing dissent. As seen in Chapter 6, the survey findings reveal that about one in five persons is very scared of expressing their social or political opinions online for fear of legal action and another 45 percent are somewhat scared.

4.4.3. Phone tapping and misuse of surveillance

Phone tapping is a type of surveillance that has a long history, and is in fact legalised for specific circumstances with the prior permission of the government under Rule 419A

Table 4.15: Nearly two out of five stories within the human rights frame refer to issues related to freedom of expression

Media coverage of the use of digital surveillance to control dissent	Percentage of reported stories in the overall sample*	Percentage of reported stories within the Human Rights frame**
Controlling/criminalising dissent	5	18
Controlling political opposition	6	21
Freedom of expression	10	38

Note: All figures are in percentages and are rounded off.

*N=1113; **N= 297

Table 4.16: Seven percent of the overall stories on surveillance are on illegal phone tapping

Reports on phone tapping in the media	Percentage in the overall sample*	Percentage within the Human Rights frame**
Illegal phone tapping	7	28
Authorised phone tapping	2	8

Note: All figures are in percentages and are rounded off.

*N=1113; **N= 297

of the India Telegraph (Amendment) Rules, 2007. However, because of the opaqueness in the extent of its use by the government, there are also suspicions of illegal phone tapping by state and non-state entities. The media analysis reveals references to illegal and authorised phone tapping in about seven and two percent of the stories sampled respectively (Table 4.16).

Evidently, illegal phone tapping received wider media coverage than those which were authorised. The Times of India features the history of phone tapping (TOI, 2021,) in one of its stories. Media reports often cover instances of ruling parties abusing their power through illegal phone tapping. Some recent coverage is of instances of alleged phone tapping of Maharashtra Congress President and MLA Nana Patole, as reported by Times of India (Jain, 2021). The story points out, "According to rules, it is necessary to secure permission from the competent authority for phone surveillance, and the name of the person whose phone would be under surveilance has to be clearly stated, along with the purpose of surveillance." Similarly, another piece talks about phone tapping that is associated with Rajasthan's horse-trading of ruling party MLAs (Times of India, 2021).

As seen above, while surveillance has usually been reported positively by the media, a significant portion of the stories sampled (23%) have also reported its possible misuse which may adversely impact individuals, groups or communities. Amongst these stories, 62

Figure 4.4: The Gorakhpur police is on alert regarding the violence that broke out after Friday prayers in several districts of UP state. SP City is patrolling in Kotwali Tiwaripur and Rajghat area of the city. At the same time, drones are being monitored in sensitive areas of the city. (Dainik Jagran, June 12, 2022)

Figure 4.5: FRT_Graphics: The equipment, including registration kiosks and face-recognition cameras has been installed (Times of India, April 10, 2022)

percent reported the impact of surveillance on individuals and more than 28 percent reported the differential impact on the groups and communities. For instance, The Print published an opinion piece on how the Muslim community is likely to be affected, particularly by FRT surveillance. Raising questions of efficiency, surveillance, and police bias, the author writes, "We mapped police station jurisdictions and found that in Delhi, Muslims are more likely to be targeted by the police if FRT is used" (Vipra, 2021.) In the context of riots triggered by incendiary comments on Prophet Mohammad by a politician, Dainik Bhaskar (June 10, 2022) also reports that Muslim areas were under surveillance through drones.

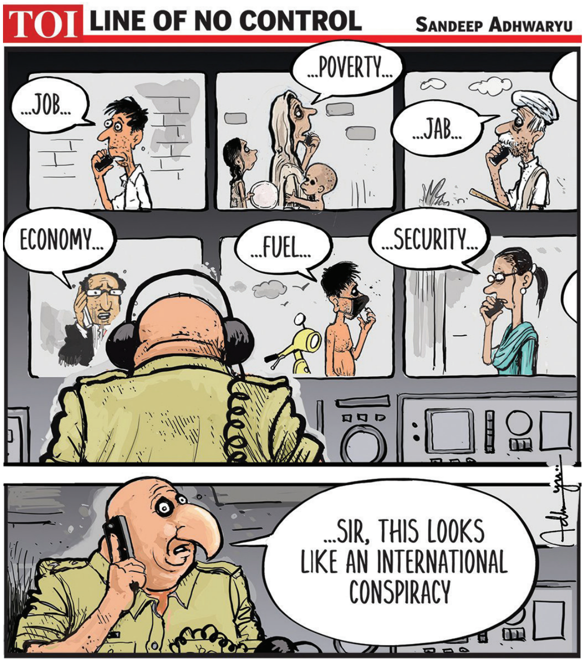


Figure 4.6: Sandeep Adhwaryu (Times of India, July 20, 2021)

4.4.4. Social media surveillance

It is common these days to come across reports of tracking, monitoring, and surveillance of social media activities of individuals by various entities, and with various intents. A 2019 Freedom House report estimates that about 89 percent of the world's internet users are being actively monitored. The big data gathered from users' online activity can have manifold implications—from profiling consumer preferences to influencing voting patterns, as was the case in the Cambridge Analytica scandal in the US (Cadwalladr and Graham-Harrison, 2018).

In India, an estimate by Kepios indicates that there are a whopping 467 million social media users as of January 2022. This number, when seen in the context of widespread reports of surveillance over online activities by private and state entities, should make us worried. In March 2022, Union Minister of State for Home,

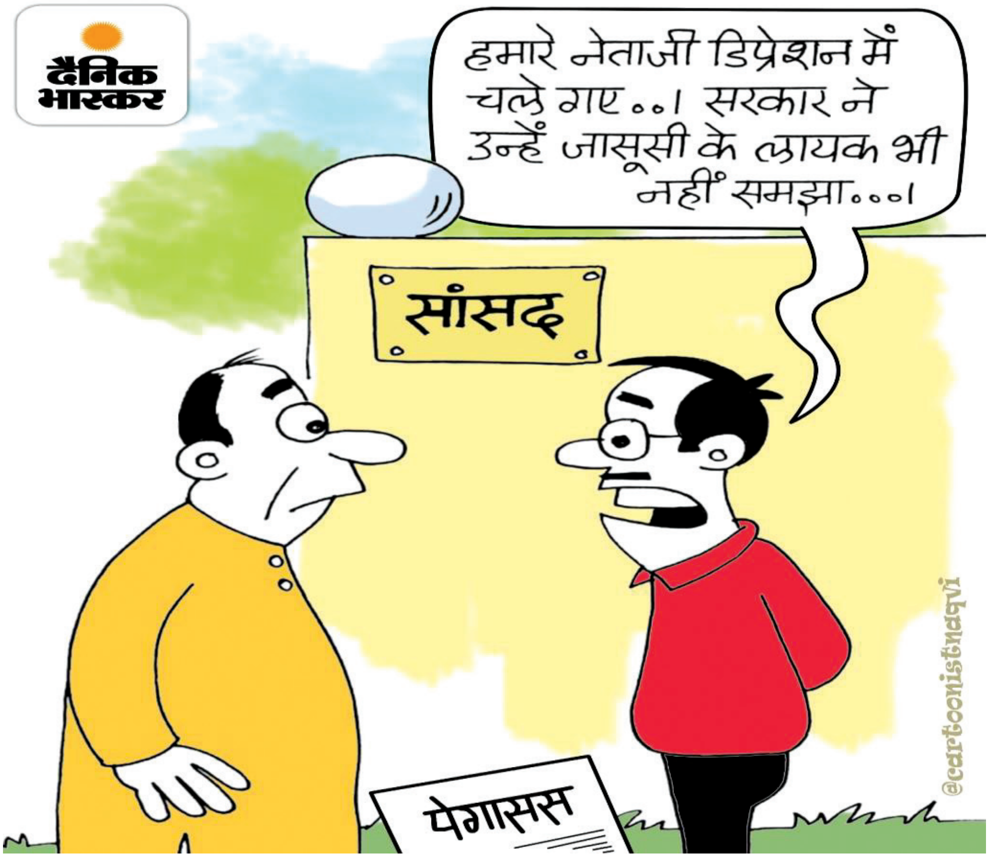

दैनिक भास्कर
हमारे नेताजी डिप्रेशन में चले गए..। सरकार ने उन्हें जासूसी के लायक भी नहीं समझा...।
सांसद
पेगासस
@cartoonistnaqvi

Figure 4.7: Translation - Our Leaders has gone into depression.... Government did not find them fit for spying upon even. (Dainik Bhaskar, 2021) The cartoon is in context of Pegasus.

Ajay Misra Teni informed the Rajya Sabha that law enforcement agencies regularly monitor social media platforms to check for “misuse” (India Today, 2022).

However, despite the prevalence of such surveillance, only under two percent of the sampled stories made a reference to them. In one such story by The Wire Hindi (Mahaprashast, 2021) Tripura Police intends to file cases against 68 Twitter accounts, 32 of Facebook and two of Youtube. In another such story by The Wire-Hindi (Staff, 2021) a Kashmiri school teacher was fired over a controversial post on her Instagram account and was later released on bail.

4.4.5. Pegasus

Amnesty International’s 2021 research report on Pegasus defines it as a spyware developed by the Israeli cyber-arms company NSO Group. It can be covertly installed on mobile phones and is allegedly being used by various governments across the world for targeted surveillance. Rights activists, journalists and leaders of oppositions have alleged that the Government of India used Pegasus for surveilling their devices. It is believed that the spyware can hack electronic devices without leaving a trace even when they are switched off. Amnesty International traces the first use of Pegasus back to the year 2016.

In July 2021, a joint investigation was conducted by 17 media organisations across the world. The investigation revealed that the Pegasus spyware was used to target and spy on heads of state, rights activists, journalists, and dissidents. The NSO group claims that it only sells its technology to recognised governments and private companies cannot purchase it. After the publication of the report, a public interest litigation and several writ petitions were filed in the Indian Supreme Court against Pegasus, seeking a court-monitored SIT probe. The Express quoted a plea filed by advocate ML Sharma, “The Pegasus scandal is a matter

The controversy, the plea says, also raises questions about the integrity of democratic institutions. "A system in which political opponents, officials of the Election Commission, and political colleagues could be subject to this kind of surveillance (Pegasus), will inspire less confidence," it says.

(The Indian Express, July 23, 2021)

of grave concern and a serious attack upon Indian democracy, judiciary and country's security. The widespread and unaccountable use of surveillance is morally disfiguring." The Government of India has neither rejected nor accepted the claims (The Indian Express, 2021).

Our analysis found that the media outlets studied devoted one percent or less of their coverage on surveillance to the Pegasus issue with the exception of The Print where three percent of the analysed articles covered the story and The Wire which carried 10 percent coverage. Dainik Jagran, in particular, stood out by reporting just 0.20 percent of the total number of stories samples on the Pegasus issue. This shows that the issue of illegal phone tapping of journalists, dissenters, bureaucrats, opposition leaders etc. was not treated as a significant issue by India's mainstream news outlets. Despite the global outrage created by the illegal spying scandal, only 16 percent of the sampled stories mentioned Pegasus.

Across the selected media outlets, there was wide variation in the reportage of the issue, with The Wire being an outlier and reporting the maximum proportion, nearly 10 percent, of the stories on Pegasus. This may be attributed to the fact that The Wire was among the 17 international media organisations which formed a consortium to investigate and consequently report on the issue (Forbidden Stories, 2021). In one of its stories, The Wire provided a list of 174 individuals including politicians, journalists, activists, and students as well as two of its editors who were reported to be among the victims of targeted phone tapping in India. (The Wire Staff, 2021)

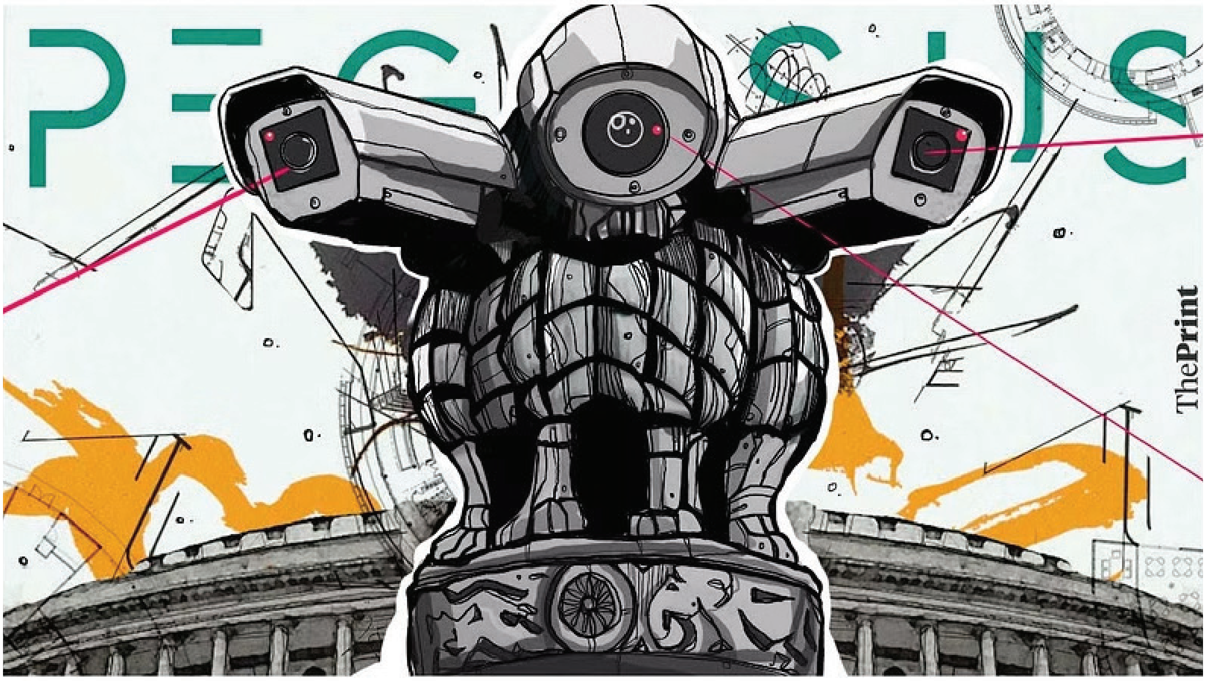


Figure 4.8: Illustration Soham Sen (The Print, February 2, 2022)

4.5. Surveillance and national security

National security is one of the most important issues for a sovereign nation. It is surprising, therefore, that only eight percent of the total number of stories on surveillance and related issues were under the national security frame.

Out of the total number of stories reported under this frame, the largest number of stories (51%) centred on cross-border issues followed by stories related to terrorism (28%) and incitement to violence (20%) (Table 4.17). The Indian Express and The Print reported the maximum number of stories under this frame. Many stories covered issues related to drone attacks.

The Wire reports, "In a letter dated November 3, 2021, the West Agartala police station had initially written to Twitter requesting the social media platform to block at least 68 accounts and provide personal information about them, while divulging that a case under section 13 of the UAPA has been filed against the said accounts holders"

Ajoy Ashirwad Mahaprashasta
(The Wire, November 7, 2021)

Notably, however, one out of five stories on the issue of national security refers to actors inciting violence or public unrest, which may not necessarily include foreign agents but individuals of particular communities charged with specific to nebulous offences under national security statutes. For instance, several activists and protestors participating in protests against government policies or laws have been charged with inciting violence under the Unlawful Activities (Prevention) Act, 2008 which essentially deals with cases involving the integrity and sovereignty of India. Thus, several reported cases of national security, particularly those falling under the category of 'inciting violence or public unrest', may in fact be cases of voicing dissent or opposition to government policies. In one such case in Tripura, 102 people were booked under UAPA provisions for protesting or talking about the 2021 communal violence in

Table 4.17: Over half of the stories on national security vis-à-vis surveillance relate to cross border security

Sub-categories appeared under national security frame	Percentage within the national security frame
Cross border security	51
Terrorism	28
Inciting violence/public unrest	20
Cyberattacks	18
Data protection	14
Internal conflict	12
Separatism/Insurgency	8
Debarring or preventing trespassing of unauthorised persons	6
Maoism/Naxalism	5
Maritime security	4
Intelligence gathering	1

Note: All figures are in percentages and are rounded off. This was a multiple-choice question and thus the sum of percentages could be greater than 100. N=92 the state on social media platforms. A The Wire Hindi reports reads:

“तीन नवंबर 2021 को लिखे गए एक पत्र में पश्चिम अगरतला थाने ने ट्विटर को उसके प्लेटफॉर्म से कम से कम 68 खातों को ब्लॉक करने और उनकी व्यक्तिगत जानकारी देने का अनुरोध करते हुए बताया कि इनके खिलाफ यूएपीए की धारा 13 के तहत प्राथमिकी दर्ज की गई है। विपक्ष ने इसे लेकर सत्तारूढ़ भाजपा पर निशाना साधा है।”

(In a letter dated November 3, 2021, the West Agartala police station had initially written to Twitter requesting the social media platform to block at least 68 accounts and provide personal information about them, while divulging that a case under section 13 of the UAPA has been filed against the said accounts holders) (Mahaprashast, 2021).

In the stories on cross-border security, some described the use of drone for smuggling explosives from Pakistan. For instance, an Indian Express (May 14, 2022) headline reads, “BSF troops open fire at Pakistani drone near IB in Jammu, force it to return”. Officials said the Pakistani drone was spotted by the border guards around 4.45 am and some eight rounds were fired by them to bring it down.

4.6. Public safety and surveillance

Technology, and in particular surveillance technology, is often touted as a means to ensure public and individual safety. Surveillance technologies such as CCTVs purportedly provide a sense of security, as is also evidenced by the survey findings of this report, in Chapter 5. While the actual efficacy of several of these surveillance technologies in crime prevention or even investigation may be debatable, the larger opinion appears to positively associate surveillance technologies with better safety and law and order. Similar trends also emerged from the analysis of media reports on surveillance, with more than 60 percent of stories reporting on surveillance from a public safety point of view.

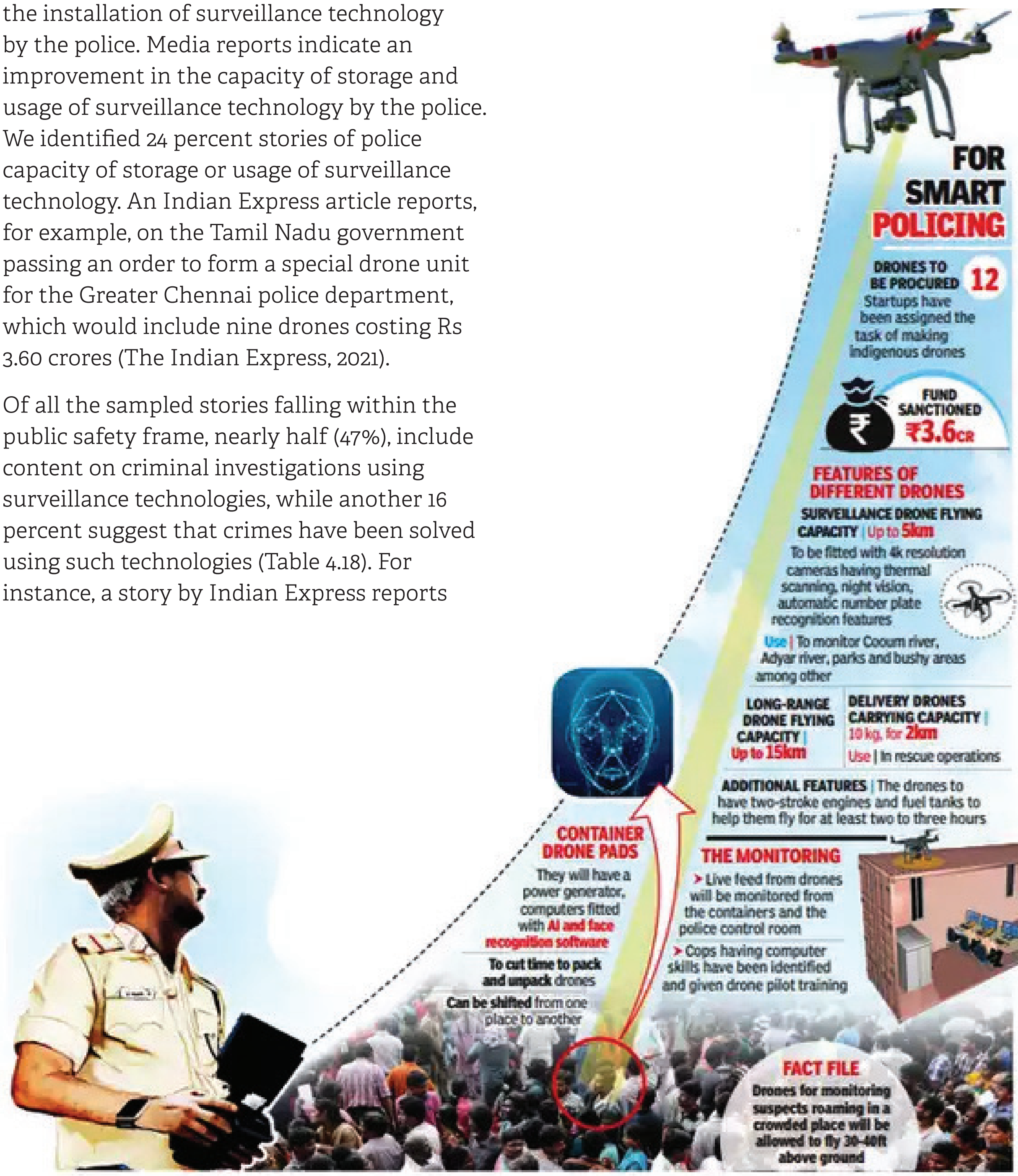
Out of the total sample, 42 percent of stories found police in leading roles conducting surveillance, particularly for ensuring public safety and order. Multiple news items also suggest that such surveillance technologies are being efficiently used by the police for criminal investigations. A careful reading of the news coverage on surveillance from the perspective of public safety presents a largely

Figure 4.9: Translation - Action has been taken against eight people littering on the road in Varanasi as their act was caught on camera. The police action has triggered a discussion among common people. (Dainik Jagran, May 26, 2022)

positive image of surveillance technologies in ensuring public safety and thus furthers the argument for the establishment of more surveillance technologies by the state and police.

In several states, police are setting up integrated control command rooms with a network of CCTVs in urban spaces for keeping an eye on the desired landscape. Thirty-four percent of analysed stories talked of the installation of surveillance technology by the police. Media reports indicate an improvement in the capacity of storage and usage of surveillance technology by the police. We identified 24 percent stories of police capacity of storage or usage of surveillance technology. An Indian Express article reports, for example, on the Tamil Nadu government passing an order to form a special drone unit for the Greater Chennai police department, which would include nine drones costing Rs 3.60 crores (The Indian Express, 2021).

Of all the sampled stories falling within the public safety frame, nearly half (47%), include content on criminal investigations using surveillance technologies, while another 16 percent suggest that crimes have been solved using such technologies (Table 4.18). For instance, a story by Indian Express reports how drone surveillance helped police bust illegal liquor dens in Gujarat. Quoting police newspaper writes, “operation “Special Bhatti” was conducted in three talukas of Amreli district on Saturday using a drone equipped with a high-definition camera for surveillance to bust illicit country liquor manufacturing dens and nab the accused” (Jan 11 2022).



FOR SMART POLICING

DRONES TO BE PROCURED 12

Startups have been assigned the task of making indigenous drones

FUND SANCTIONED ₹3.6CR

FEATURES OF DIFFERENT DRONES

SURVEILLANCE DRONE FLYING CAPACITY | Up to 5km

To be fitted with 4k resolution cameras having thermal scanning, night vision, automatic number plate recognition features

Use | To monitor Cooum river, Adyar river, parks and bushy areas among other

LONG-RANGE DRONE FLYING CAPACITY | Up to 15km

DELIVERY DRONES CARRYING CAPACITY | 10 kg, for 2km

Use | In rescue operations

ADDITIONAL FEATURES | The drones to have two-stroke engines and fuel tanks to help them fly for at least two to three hours

CONTAINER DRONE PADS

They will have a power generator, computers fitted with AI and face recognition software

To cut time to pack and unpack drones

Can be shifted from one place to another

THE MONITORING

> Live feed from drones will be monitored from the containers and the police control room

> Cops having computer skills have been identified and given drone pilot training

FACT FILE

Drones for monitoring suspects roaming in a crowded place will be allowed to fly 30-40ft above ground

Figure 4.10: Chennai - Illustrates the usage of drones with built in facial recognition technology. (TOI, April 01, 2022)

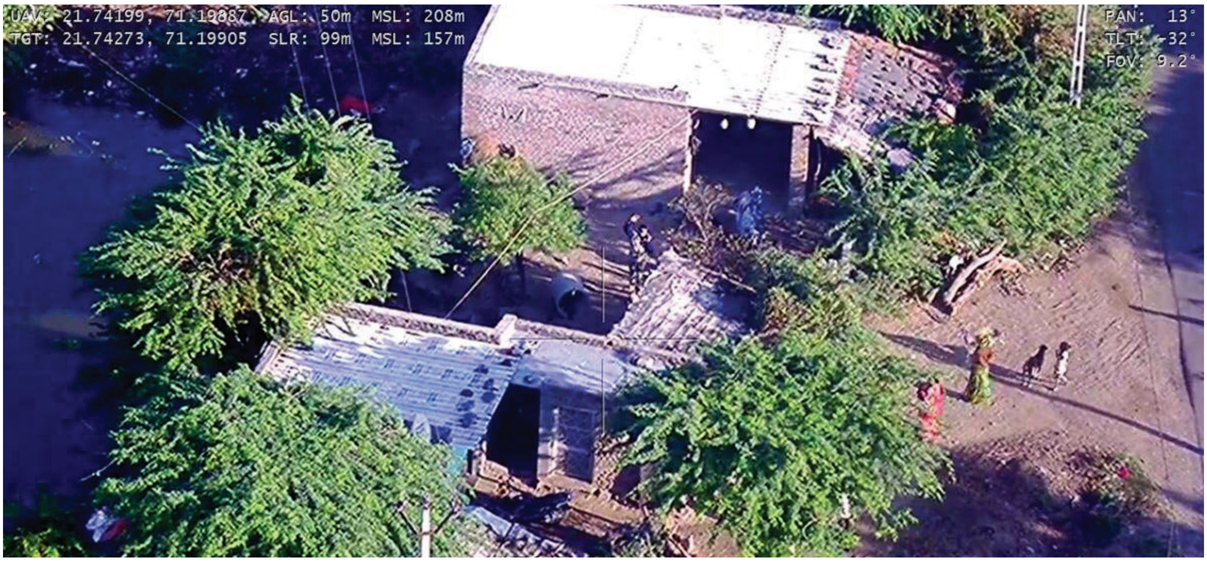

UAV: 21.74199, 71.19887, AGL: 50m MSL: 208m
TGT: 21.74273, 71.19905 SLR: 99m MSL: 157m
PAN: 13°
TLT: -32°
FOV: 9.2°

Figure 4.11: An image from the drone that helped police bust nine illegal country liquor manufacturing dens in Amreli Saturday (The Indian Express, January 11, 2022

Another story gives an account ofhow a power company uses drones to detect power theft and to penalise offenders (The Indian Express, 2022).

Figure 4.12: A grab of surveillance video recorded by drone camera. (Courtesy_PGVCL) (The Indian Express, March 17, 2022)

Table 4.18: Nearly one out of two stories on public safety focused on crime investigation using surveillance technologies

News items reporting on surveillance from the public safety perspective	Percentage within public safety frame
CCTV footage access/storage	52
Criminal investigation	47
Crime prevention	33
Crime solved using surveillance technology	16
Demand for surveillance for public safety	11

Crime reduction	10
Women's safety	9
Children's safety	7
Drone footage access/storage	7
Cybercrimes	7
Road safety	7
Others	5
Compromising medical/financial/sensitive data of an Individual	3
Contact tracing applications	2

Note: All figures are in percentages and are rounded off. As the question was multiple choice, aggregate may appear greater than the aggregate of percentage of the public safety frame. N=696
Others include those sub-categories which have a frequency of one percent or less. These are: crimes against sexual/gender minorities, use of big data for crime prevention, physical surveillance, social media monitoring, Central Control Command Centre and police misconduct.

Burking or non-registration of crimes by the police is a common problem in India, as evidenced by various studies (Tiwari and Rao, 2016). While there may be a general presumption that surveillance technology such as CCTVs may help victims lodge a complaint, this doesn't necessarily apply, as is evidenced by some media reports. Such an attitude is reflected in an incident reported by Indian Express where a young woman was the victim of sexual harassment on the platform of Delhi Metro and she alleged that neither the policeman on the platform nor others in the CCTV control room helped her. The police took action only after she vented out her disappointment on a social media platform (Prasad, 2022).

While a majority of the sampled stories fall under the public safety frame, notably, not even a single typical story talks about the due process of surveillance—authorities involved or chain of command for permission to surveil an individual or organisation were missing from the news stories reported on crime. More often than not, the stories only mentioned the role of cyber cells, glorifying police efficiency. A story in Dainik Jagran, for instance, reports on how efficiently the police cracked the case using phone surveillance (Bajpai, 2022). The story reveals how in a case of a love triangle leading to a man's murder, his wife was charged for the crime using surveillance technology. The police put the woman's mobile number under surveillance to solve the case and its contents were later used as technical evidence in the court.

However, it also needs to be noted that CCTV is the most preferred and frequently used form of surveillance technology by the police for public safety, going by the media coverage, while more advance technologies have not become so commonplace as yet. More than half of the news items under the public safety frame focused on the access or storage of CCTV footage by the police.

A victim of sexual harassment at DMRC Jor Bagh Platform claims in her tweet, "The entire incident was captured on camera but we saw him get into a different train and leave. I asked them to do something about it but instead they started victim blaming me and said that I should've created a scene and there was nothing they could do since he had managed to leave."

Malavika Prasad (The Indian Express, June 4, 2022)

Table 4.19: Nearly half of the news items on the installation or description of new surveillance technology refers to CCTV technology

News items within the technology frame on surveillance	Percent
CCTVs	49
Drones surveillance	18
Pegasus	15
Others advanced surveillance technologies	12
Spyware, malware, etc	9
Phone tapping	9
Facial recognition technology	4
GPS tracking	4
Other video surveillance devices	3
IP tracing	3
Hacking and jammers	3
Algorithm	2
Artificial intelligence	2
Biometric data	2
Aadhaar	2

Note: All figures are in percentages and are rounded off. Aggregate percentage is greater than 100 because it was a multiple-choice question. N=377
Other advanced surveillance technologies include those with a frequency of one percent or less. These are: tracing of individuals via metro cards, Fastags, gait analysis, IOT, automatic number plate recognition, smart cities, interception of SMS/email, unauthorised access to personal cameras, fingerprints, police body cameras, audio surveillance, night vision cameras, contact tracing applications, anti-drone technology, big data, thermal scanners, behaviour analysis, space technology, traffic monitoring, panic buttons and Central Control Command Centre.

4.7. Surveillance technology and its legitimacy

In more than 30 percent of the sampled stories, the content was limited to a description of or news about the installation of some form of surveillance technology, by either the state or non-state entities. Such stories were typically categorised under the technology frame. These included more commonplace surveillance technologies such as CCTVs, to more sophisticated ones such as FRT, voice recognition, and gait analysis, to name a few.

Stories under the technology frame focused on the advancements and innovations taking place in the field of surveillance technology. The incorporation of high-resolution night vision AI-based cameras for traffic management and heavy-lifting drones were some of the frequently discussed examples in the news items. Further, the frame also includes some stories on legal provisions regarding the use of such technologies, especially the use of drones, which may carry an inherent risk to national security and integrity. For instance, a news story published by The Wire Hindi (The Wire, 2021) highlights the ban on the sale, storage, transport, and usage of all kinds of drones following an attack on an airbase in Jammu. The headlines read,

“जम्मू कश्मीर वायु सैनिक अड्डे पर ड्रोन हमले के हफ्ते भर बाद श्रीनगर में भी ड्रोन पर पाबंदी” (Jammu and Kashmir: A week after the drone attack on the air base, ban imposed on the use of drones in Srinagar as well).

Similarly, The Indian Express reports, “Week after Jammu attack, Srinagar administration bans drones. The Srinagar administration warned that the sale, possession, storage,

Figure 4.13: Iris scans are part of biometrics data collection under the Criminal Procedure Act, 2022_Wikimedia Commons (The Print, April 22, 2022)

use and transport of drones would invite action"(Masood, 2021).

Predictably, under this frame, a majority of the stories were regarding common forms of mass surveillance such as CCTVs, as seen in Table 4.19. While CCTVs are mentioned in nearly half of the stories under this frame, it is followed by news regarding drone surveillance (18%) and Pegasus (15%).

Upon bifurcating various types of surveillance technologies by the agency conducting surveillance it was found that the police (72%), prison authorities (84%), and other state agencies (84%) were most likely to use CCTVs for mass surveillance. In stories that include mention of security agencies and armed forces, there is a higher proportion of targeted surveillance technologies, including those that at least at face value, fall outside the legal ambit. These include illegal phone tapping (35%), hacking phones/personal devices/ websites (39%), Pegasus (42%) and spyware/ malware, etc. (40%), to name a few. On the other hand, stories on prisons are likely to include mentions of surveillance technologies such as CCTVs (80%), drones (20%), and biometric data (20%). As for the police, aside from the mention of CCTV usage, the only other considerable use of surveillance technology mentioned in the sampled stories is drones (16%) (Table 4.20).

Table 4.20: Around two out of four sampled stories suggest that security agencies and armed forces are involved in conducting targeted surveillance in the form of hacking, Pegasus and spyware or malware

Selected forms of surveillance technology	Government	Police	Security agencies/ armed forces	Other state agencies	Private bodies/ organisations	Prison authority
Illegal phone tapping	12	4	35	1	26	0
Authorised phone tapping	3	3	6	1	0	0
CCTV	51	72	25	84	43	80

FRT	8	5	7	6	9	0
Drones	14	16	21	5	0	20
Hacking phone/ personal devices/ websites	11	4	39	3	34	0
Pegasus	20	2	42	2	37	0
Spywares, malwares, other tools of hacking/personal devices	11	3	40	1	34	0
Video surveillance in personal spaces/ through hacking of personal devices	5	2	15	0	17	0
Biometric data	2	1	4	1	6	20

Note: All figures are in percentages and are rounded off. Data for only selected modes of surveillance technologies has been presented.

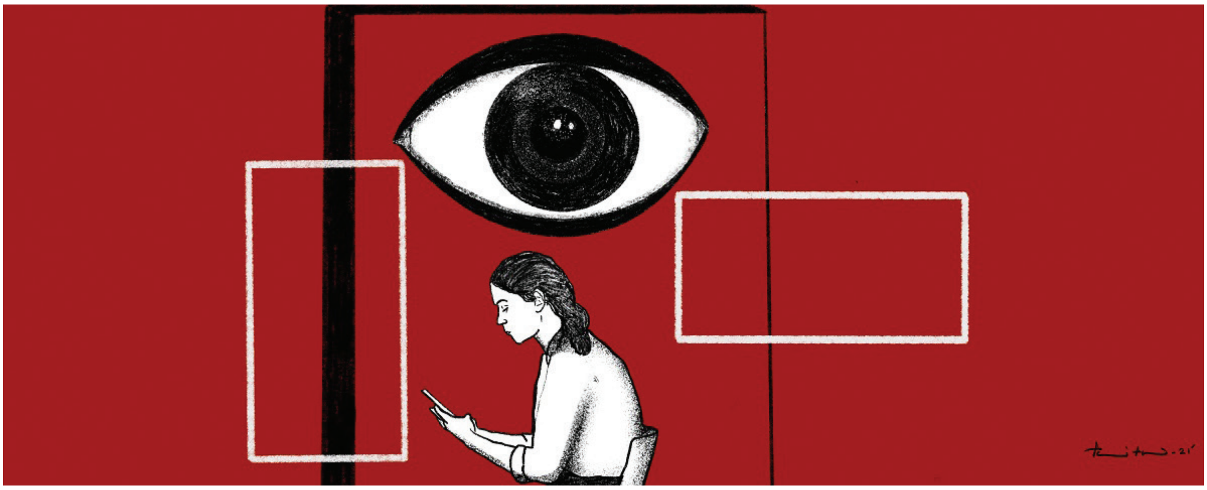


Figure 4.14: Pegasus-Mobile-snooping-Illustration-Pariplab (The-Wire, 22 Jan, 2022)

Every advancement in science and technology can be interpreted as a step towards modernity. Technology also brings new changes in the lifestyle of the masses and enhances their living standard. Surveillance technology may also have a similar effect if used in fair and legal means. The pros and cons of surveillance technology are part of the ongoing debate on its use and efficacy. However, there is a public perception that surveillance technology makes lives safer. Also, wide ambiguity and vacuums exists in the domain of legality governing these technologies.

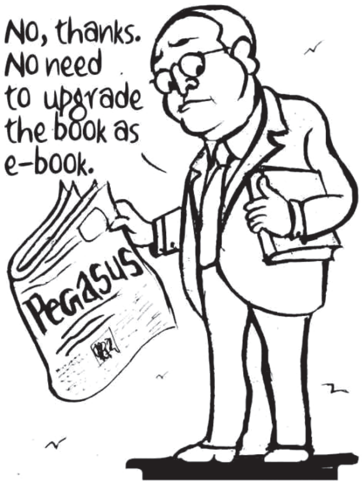


Figure 4.15: Depicting the chilling effect of the digital surveillance. (The Print, July 20, 2021)

Table 4.21: Stories on CCTVs and drones least likely to include debates around their legality or right to privacy

Mode of surveillance (N)	Critical approach to surveillance	Legality of surveillance	Right to privacy	Constitutionality of surveillance
Illegal phone tapping	66	57	48	37
Authorised phone tapping	25	21	17	17
CCTV	5	4	3	2
FRT	48	43	36	21
Drones	6	5	0	0
Hacking phone/ personal devices/ websites	52	40	38	29
Pegasus	74	55	52	31
Spywares, malwares, other tools of hacking/personal devices	70	49	43	31
Biometric data	46	54	39	31
Aadhaar	12	12	0	12

Note: All figures are in percentages and are rounded off. Data pertaining to only selected surveillance technologies has been presented here. Here, N=1521

The fundamental right to equality before law requires that individuals, institutions, and government functionaries abide by the law of the land and the provisions of the constitution. Thus, in this analysis, we enquired into how much weightage the media outlets gave to concerns over the legality of surveillance technology.

Only five percent of all stories discussed both technology and legality of surveillance together. While descriptive stories focussed on the technical aspects of various modes of surveillance, most of them did not refer to the corresponding legal aspect. There was, thus, an evidently glaring gap in the media coverage of the introduction of new technology wherein they largely failed to get into the issue of the legal backing required for such installations and their use.

As seen in Table 4.21, while in the case of Pegasus, illegal phone tapping, spyware and malware, and biometric data, more than half the news stories get into the legal aspects of surveillance, but when it comes to more commonplace mass surveillance technologies such as CCTVs and drones, less than five percent of the sampled stories cover these issues.

More than half of the sampled stories which were reporting on illegal phone tapping also discussed its legal aspects and people's right to privacy, while one-third of such stories questioned the constitutionality of such surveillance infrastructure. Two out of three stories on illegal phone surveillance also had a critical approach to surveillance, which is significantly higher than the overall sample.

However, when it comes to other surveillance technologies, namely CCTVs, and drones this critical perspective appears to be largely missing in the reportage, as is evident from the above table. While nearly half of the stories on FRTs do question the legal aspects of this surveillance and contain references to issues such as the right to privacy, the numbers plummet dramatically when it comes

The right to privacy cannot be subject to the ever growing possibilities of technological and psychological intrusions by the state. Further, the right to privacy is not lost merely because the individual is in a public place.

(The Indian Express, July 21, 2021).

to reports on CCTVs and drones (Table 4.21). Legality seems to become an issue only when a matter is taken to the court.

In a rare example of critical approaches to surveillance vis-à-vis CCTV cameras, the Times of India reported a story where Delhi High Court asked the Delhi government to respond to a plea challenging the decision to install CCTV cameras in school classrooms. The report quotes the plea, "Expressing concerns over the privacy of students and preservation of their dignity under Article 21 of the Constitution, the associations approached the high court and said that the installation of CCTV cameras and consequent live-streaming of footage to unauthorised persons would infringe upon the students' right to privacy" (TOI, 2022). Indian Express gives an account of such a challenge in Punjab and Haryana Court over the range of CCTV cameras installed by one of the neighbours of a retired judge, Justice NK Sodhi. "The petition respectfully submits that the installation and use of the high-resolution sophisticated CCTV cameras at the official residence of the Hon'ble Chief Justice of this Hon'ble Court is a direct invasion of the privacy of the petitioner.... Individual dignity and privacy are linked... The right to privacy cannot be subject to the ever-growing possibilities of technological and psychological intrusions by the state. Further, the right to privacy is not lost merely because the individual is in a public place", the petition reads as quoted by the outlet (The Indian Express, 2021).

An exception to this trend, however, is the reporting on the Pegasus issue, wherein more than three out of five stories covered the legal, constitutional, and privacy aspects related to the issue and also viewed the surveillance from a critical perspective. It needs to be noted, however, that the overall reporting on the Pegasus issue is largely restricted to only one of the selected media outlets—the Wire, as mentioned in the above section. Thus, this trend of getting into the legal and constitutional aspects of the Pegasus surveillance may not be universal, but may indeed be largely reflective of just The Wire's reporting, ostensibly because of its editorial policy of carrying more stories critical of government actions or policies.

Overall, however, across the total sample of news items, any mentions of the legality or constitutionality of surveillance, or its impact on the right to privacy are severely limited. As seen in Table 4.22, 14 percent or less of the stories on surveillance mention the right to privacy or its legal aspects, while just eight percent of the sample reviews such issues from the perspective of constitutionality.

Table 4.22: Of the total sampled stories, less than 14 percent mention right to privacy or legality of the surveillance

Elements of legitimacy in surveillance	Response		
	Yes	No	Unclear
Legality	14	84	2
Right to privacy	13	85	2
Constitutionality	8	90	2

Note: All figures are in percentages and are rounded off.

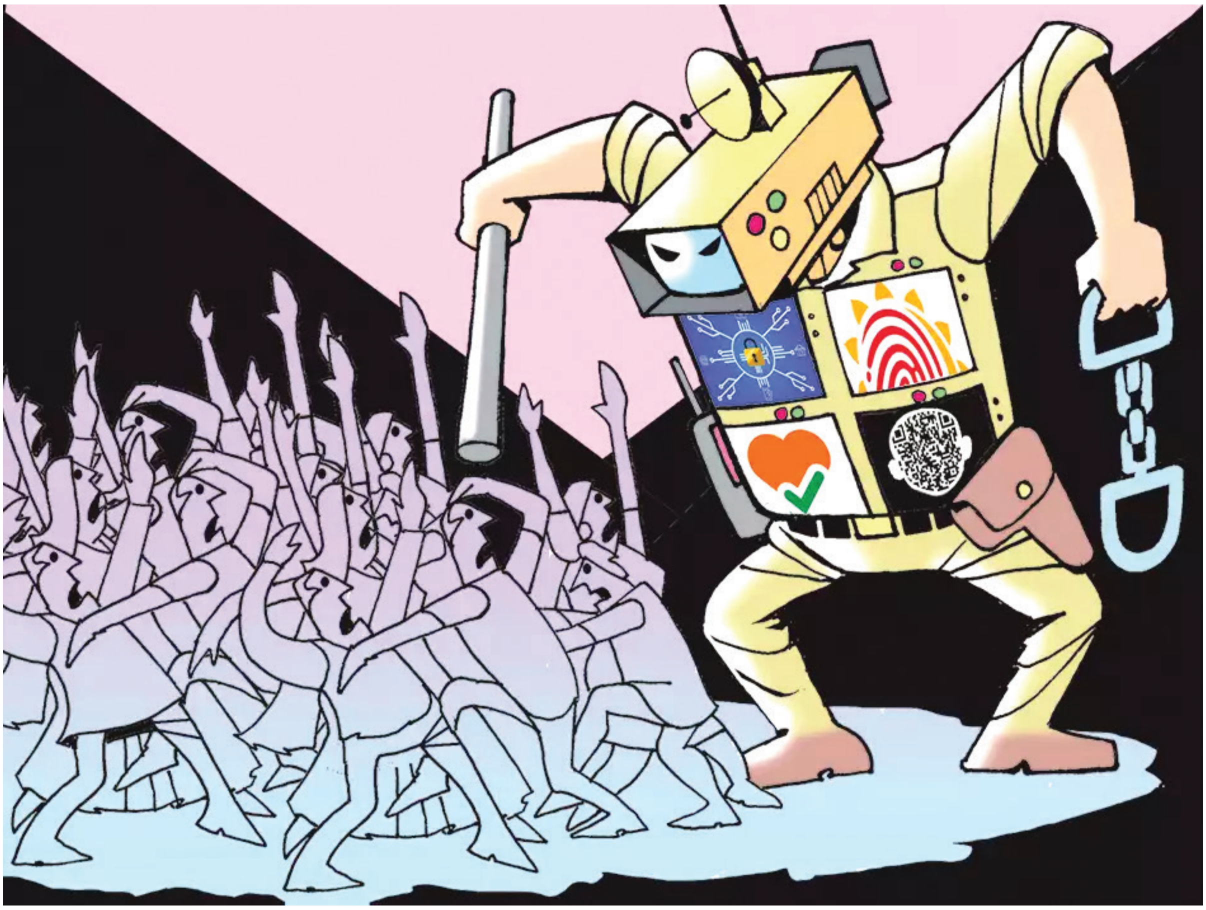


Figure 4.16: Cartoon-Surveillance Nation, (TOI, April 16, 2022)

Conclusion

This analysis of media reporting on surveillance and its related issues is a dipstick attempt at understanding the landscape of surveillance through the lens of mainstream media since this reporting can both be influencing as well as influenced by public opinions on these issues. While in many ways this analysis triangulates popular opinions regarding the issue of surveillance, as seen in the chapters pertaining to the survey data (Chapters 5-10), the study itself does not necessarily endorse the larger views or trends in the mainstream media. Rather, this is an attempt at mapping the trends of what aspects of surveillance have been highlighted by the media. In doing so, it also underlines what has been omitted and needs a more robust public debate around it.

While the digital surveillance infrastructure in place in India, particularly employed by the police and the criminal justice system, may not be as sophisticated or omnipresent as in Western countries, the larger trends show an aspiration to reach those levels. However, the corresponding critical review of surveillance technologies appears to be missing in the Indian media discourse. Numerous studies worldwide have pointed out loopholes in surveillance technologies and indicate that there is reason to be wary of over-dependence on them, especially when it comes to their use in the criminal justice system.

However, such nuances of discourse appear to be scarce and uneven in the media coverage of the issue in India, with just about 13 percent of the sampled stories looking at surveillance from the perspective of the right to privacy. In contrast, the media appears quick to applaud the benefits of such technology vis-à-vis the police and criminal investigation etc in nearly half the stories within the public safety frame. One of the reasons for such an uncritical approach could be the fact that the government and the police are most often the primary sources, the main actors and the most preferred subjects of the stories covered on surveillance.

When it comes to the reporting of human rights issues, such as misuse of surveillance methods, and the technology being used to curb or control dissent or political opposition, the reportage in the overall sample is negligible-less than five percent. Even issues of international concern, such as the Pegasus controversy which allegedly involved surveillance of not only activists and journalists, but also state actors such as judges, ministers, and leaders of the opposition, received limited media coverage of around 16 percent of the sampled stories. Of this, just one media outlet published 11 percent, while the remaining five selected outlets all put together published the remaining five percent of the stories on Pegasus. It is, therefore, not an exaggeration to say that the Indian mainstream media largely ignored the issues of illegal phone tapping by state agencies.

The analysis of media coverage of surveillance technology and related issues needs to be understood at two levels, i.e., the media's commissions and omissions. At one level, it indicates the salience of certain issues in the media's daily construction of reality, while at another level it points out a near absence of questioning the authorities over round-the-clock scrutiny of citizens or about illegal tapping of their phones. It appears that while many of the issues may have been ignored by the mainstream media at the cost of many others, the legality and constitutionality of government actions regarding surveillance have been largely taken for granted. It must also be mentioned that even as the actual number of cases of human rights violation or misuse of surveillance technology may altogether be small, the gravity of such cases may not be adequately reflected in the aggregated numbers of the stories covered. We also acknowledge that this is, at best, a rudimentary analysis of media coverage of surveillance and a wider understanding of its nuances and intricacies would require deeper, and more qualitative research.

Reference

Amnesty International. (2021, July 18). Forensic Methodology Report: How to catch NSO Group's Pegasus. Amnesty International. Retrieved fromhttps://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/. Accessed on 5th July, 2022.

Audit Bureau of Circulations (2022). Highest Circulated Daily Newspapers, January- June 2022. Retrieved from: http://www.auditbureau.org/files/JJ%202022%20Highest%20Circulated%20(language%20wise).pdf. Accessed on 18th December, 2022.

Bajpai, S. (2022, February 24). प्रेमिका ने आशिक से मांगा था पति की मौत का तोहफा, आशिक ने मुस्कुराते हुए दिया ऐसा गिफ्ट. *Jagran.* https://www.jagran.com/bihar/bhagalpur-aashiq-gifts-girlfriend-her-husband-dead-body-in-the-new-year-5-arrested-including-chumki-22494855.html Accessed on 18th June, 2022.

Bhatnagar, G. V. (2022, March 8). Govt Denied Information Under RTI on Frivolous Grounds During 2020-21: CIC Analysis. The Wire. https://thewire.in/government/govt-denied-information-under-rti-on-frivolous-grounds-during-2020-21-cic-analysis

Cadwalladr, C. and Graham-Harrison, E. (March 17, 2018). Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian.* Retrieved from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed on 5th July, 2022.

Chauhan, C. *(2022, March 5). 83% increase in rejection of RTI applications on national security grounds: Data.* Hindustan Times. https://www.hindustantimes.com/india-news/83-increase-in-rejection-of-rti-applications-on-national-security-grounds-data-101646469748249.html

Dainik Bhaskar. (2021, September 9). करनाल में किसानों का धरना LIVE: लघु सचिवालय पर लगातार तीसरे दिन डटे किसान, प्रशासन CCTV से नजर रख रहाय; 11 सितंबर को फिर महापंचायत. Retrieved fromhttps://www.bhaskar.com/local/haryana/karnal/news/farmers-protest-outside-mini-secretariate-karnal-the-administration-opened-the-main-gate-for-the-general-public-with-the-consent-of-the-protesters-128905756.html.Accessed on 17th June 2022.

Dainik Bhaskar. (2022, June 10). फतेहपुर में घरों की छत पर ड्रोन से तलाशी; डीएम–एसपी ने भीड़भाड़ वाले बाजार का लिया जायजा, चप्पे–चप्पे पर तैनात रही पुलिस.... Retrieved fromhttps://www.bhaskar.com/local/uttar-pradesh/fatehpur/news/dm-sp-took-stock-of-crowded-market-police-stationed-everywhere-129921103.html.Accessed on 20th June, 2022.

Dainik Bhaskar. (2022, June 17). 'अग्निपथ' उपद्रव के CCTV फुटेज सबसे पहले भास्कर में... ग्वालियर में तोड़फोड़ कर हंस रहे थे युवक; ले रहे थे सेल्फी, अबतक 45 पकड़ाए. Retrieved from https://www.bhaskar.com/local/mp/gwalior/news/the-miscreants-were-laughing-on-the-road-were-taking-selfies-so-far-34-caught-129946423.html. Accessed on 20th June 2022.

Entman, R.M. (2010). Media framing biases and political power: Explaining slant in news of Campaign 2008. *Journalism*, 11(4), 389-408. Accessed on 22 Jan 2023.

Forbidden Stories. (2021). About The Pegasus Project. Retrieved fromhttps://forbiddenstories.org/about-the-pegasus-project/.Accessed on 14th December, 2022.

Freedom House (2019). Freedom on the Net 2019: the Crisis of Social Media. Retrieved from:https://www.freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf. Accessed on 18th December, 2022.

Greenberg, J. & Hier, S. (2009). CCTV Surveillance and the poverty of Media Discourse: A Content Analysis of Canadian Newspaper Coverage. *Canadian Journal of Communication*, 34, 461-489. Accessed on 23rd July, 2022.

Jain, B. (2021, July 10). Maharashtra: DGP-led panel set up to probe Nana Patole's phone-tapping claims. *Times of India.* Retrieved fromhttps://timesofindia.indiatimes.com/city/mumbai/mumbai-dgp-led-panel-set-up-to-probe-patoles-phone-tapping-claims/articleshow/84283386.cms. Accessed on 22nd June, 2022.

Kemp, Simon. (2022, February 15). Digital 2022: India. *Kepios.* Retrieved from: https://datareportal.com/reports/digital-2022-india. Accessed on 18th December, 2022

Mahaprashast, A. A. (2021, November 07). त्रिपुरा: सांप्रदायिक हिंसा पर सोशलमीडिया पोस्ट के लिए 102 लोगों पर यूएपीए के तहत केसदर्ज. *The Wire-Hindi.* Retrieved fromhttps://thewirehindi.com/192477/tripura-violence-police-books-102-people-under-uapa-for-social-media-posts/. Accessed on 15th July, 2022.

Masood, B. (2021, July 5). Week after Jammu attack, Srinagar administration bans drones. *The Indian Express.* Retrieved fromhttps://indianexpress.com/article/cities/srinagar/week-after-jammu-attack-srinagar-admin-bans-drones-7388971/. Accessed on 5th July, 2022.

Media Research Users Council India (2017). Indian Readership Survey, 2017: Key Trends. Retrieved from:https://mruc.net/uploads/posts/a27e6e912eedeab9ef944cc3315fba15.pdf Accessed on 18th December, 2022.

Modak, S. (2022, June 4). Gait analysis validated identity of convict sentenced to death. *The Indian Express.* Retrieved fromhttps://indianexpress.com/article/cities/mumbai/gait-analysis-validated-identity-of-convict-sentenced-to-death-7951842/. Accessed on 15 July, 2022.

Prasad, M. (2022, June 4). Delhi: Metro takes cognizance after woman alleges sexual harassment at Jor Bagh station. *The Indian Express.* Retrieved fromhttps://indianexpress.com/article/cities/delhi/metro-takes-cognizance-after-woman-alleges-sexual-harassment-at-station-7951925/. Accessed on 18th June, 2022.

Sandhu, K.K. (2022, March 30). Agencies Monitor Social Media Platforms Regularly to Check for Misuse: Government in Rajya Sabha. *India Today.* Retrieved from:https://www.indiatoday.in/india/story/algorithms-violence-communal-hatred-facebook-twitter-instagram-1931457-2022-03-30 Accessed on 19th December, 2022.

Semetko, H. A., & Valkenburg, P. M. (2000). Framing European Politics: A Content Analysis of Press and Television News. *Journal of Communication*, 93-109. Accessed on 19th August, 2022.

Shanta, S. (2021, July 07). सुरेंद्र गाडलिंग का कंप्यूटर हैक कर डाले गए थे आरोपी ठहराने वाले दस्तावेज: रिपोर्ट. *The Wire – Hindi*. Retrieved fromhttps://thewirehindi.com/176790/elgar-parishad-surendra-gadling-cyber-attack-documents-planted/. Accessed on 18th June, 2022.

Smith, T. (2019, October 22). In Hong Kong, Protestors Fight to Stay Anonymous. *The Verge*. Retrieved fromhttps://www.theverge.com/2019/10/22/20926585/hong-kong-china-protest-mask-umbrella-anonymous-surveillance. Accessed on 18th December, 2022.

The Hindu. (2021, December 4). Delhi ranks number one globally in CCTV coverage: CM. Retrieved from: https://www.thehindu.com/news/cities/Delhi/delhi-ranks-number-one-globally-in-cctv-coverage-cm/article37833081.ece. Accessed on 18th June 2022.

The Indian Express. (2021, July 21). Punjab: HC disposes of plea seeking CCTVs' removal. Retrieved fromhttps://indianexpress.com/article/cities/chandigarh/punjab-hc-disposes-plea-cctvs-removal-7414832/. Accessed on 18th June, 2022.

The Indian Express. (2021, July 23). Pegasus row: Plea in Supreme Court seeks court-monitored SIT probe. Retrieved fromhttps://indianexpress.com/article/india/plea-sc-sit-probe-pegasus-snooping-allegations-7416757/. Accessed on 18th June, 2022.

The Indian Express. (2021, November 18). Chennai police to get special drone unit | Cities News.https://indianexpress.com/article/cities/chennai/chennai-police-to-get-special-drone-unit-7629059/. Accessed on 18th June, 2022.

The Indian Express. (2022, January 11). Gujarat: Using drone, police bust 9 liquor dens, arrest 44. Retrieved fromhttps://indianexpress.com/article/cities/ahmedabad/gujarat-using-drone-police-bust-9-liquor-dens-7716898/. Accessed on 12th August, 2022.

The Indian Express. (2022, March 17). Gujarat: PGVCL detects power theft worth Rs 48L using drones. Retrieved fromhttps://indianexpress.com/article/cities/rajkot/pgvcl-detects-power-theft-worth-rs-48l-using-drones-7823479/. Accessed on 17th June, 2022.

The Indian Express. (2022, May 14). BSF troops open fire at Pakistani drone near IB in Jammu, force it to return. Retrieved fromhttps://indianexpress.com/article/india/bsf-troops-open-fire-at-pakistani-drone-near-ib-in-jammu-force-it-to-return-7916737/. Accessed on 18th June, 2022.

The Wire Staff. (2021, August 4). Pegasus Project: 174 Individuals Revealed By The Wire On Snoop List So Far. *The Wire*. Retrieved from https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance. Accessed on 24th October, 2022.

The Wire Staff. (2021, December 20). जम्मूकश्मीर: जनरल बिपिन रावत को 'युद्ध अपराधी' कहने वाली शिक्षक अपने ही स्कूल से बर्खास्त. *The Wire-Hindi*. Retrieved fromhttps://thewirehindi.com/197555/jk-educator-who-called-bipin-rawat-a-war-criminal-sacked-from-school-she-founded-report/. Accessed on 18th June, 2022.

The Wire Staff. (2021, July 05). जम्मूकश्मीर: वायु सैनिक अड्डे पर ड्रोन हमले के हफ्ते भर बाद श्रीनगर में भी ड्रोन पर पाबंदी. *The Wire Hindi*. Retrieved fromhttps://thewirehindi.com/176570/drones-banned-in-srinagar-a-week-after-the-attack-on-the-air-base-in-jammu/. Accessed on 18th Jul, 2022.

The Wire Staff. (2022, February 11). कार्यकर्ता रोनाविल्सन को 10 सालों के साइबर जासूसी प्रयासों के बाद निशाना बनाया गया:रिपोर्ट. *The Wire Hindi*. Retrieved fromhttps://thewirehindi.com/204862/rona-wilson-targeted-in-10-year-cyber-espionage-effort-by-2-groups-report/. Accessed on 18th June 2022.

The Wire Staff. (2022, June 10). उत्तरप्रदेशः इलाहाबाद में 10 जून को हुई हिंसा के संबंध में पुलिस ने 59 आरोपियों के पोस्टर जारी किए. *The Wire - Hindi.* Retrieved fromhttps://thewirehindi.com/218103/uttar-pradesh-allahabad-police-releases-posters-of-59-persons-accused-of-violence/. Accessed on 19th June, 2022

Times of India. (2021, July 21). Phone tapping is as old as Indian politics (Pegasus just a new kid on the block). Retrieved fromhttps://timesofindia.indiatimes.com/india/phone-tapping-is-as-old-as-indian-politics-pegasus-just-a-new-kid-on-the-block/articleshow/84587203.cms. Accessed on 20th June, 2022.

Times of India. (2021, July 21). Rajasthan CM Ashok Gehlot should reveal details of phone tapping: Rajendra Singh Rathore. Retrieved fromhttps://timesofindia.indiatimes.com/city/jaipur/gehlot-should-reveal-details-of-phone-tapping-rathore/articleshow/84600436.cms. Accessed on 20th June, 2022.

Times of India. (2022, Feb 22). HC asks Delhi govt to respond to plea challenging decision to install CCTV cameras in classrooms. Retrieved fromhttps://timesofindia.indiatimes.com/city/delhi/hc-asks-delhi-govt-to-respond-to-plea-challenging-decision-to-install-cctv-cameras-in-classrooms/articleshow/89753159.cms. Accessed on 22nd June, 2022.

Times of India. (2022, Jan 4). Telangana HC notice to state cops for using face recognition tech. Retrieved fromhttps://timesofindia.indiatimes.com/city/hyderabad/hc-notice-to-state-cops-for-using-face-recognition-tech/articleshow/88676220.cms. Accessed on 20th June, 2022.

Times of India. (2022, January 4). HC Notice To State, Cops For Using Face Recognition Tech. Retrieved fromhttps://timesofindia.indiatimes.com/city/hyderabad/hc-notice-to-state-cops-for-using-face-recognition-tech/articleshow/88676220.cms. Accessed on 18th June, 2022.

Tiwari, A. and Rao, U.N.B. (2016). Non-Registration of Crimes: Problems and Solutions. *Bureau of Police Research and Development, Ministry of Home Affairs, Government of India.* Retrieved from:https://bprd.nic.in/content/417_1_Plan.aspx. Accessed on 18th December, 2022.

Vipra, J. (2021, August 19). Muslims more likely to be targeted by Delhi Police if facial recognition technology is used. *The Print.* Retrieved fromhttps://theprint.in/opinion/muslims-more-likely-to-be-targeted-by-delhi-police-if-facial-recognition-technology-is-used/718092/. Accessed on 23rd June, 2022.

Chapter 5:

Privacy in an Age of Video Surveillance: People's Opinions about CCTVs

Key findings

- One out of two people said that CCTVs have been installed in their households/colonies.
- While high-income groups are more than three times more likely to have CCTV coverage in their residential areas, compared to slums and poor localities.
- The government is three times more likely to install CCTV cameras in slums/poor localities, compared to higher-income localities.
- The poorest are least likely to support the installation of CCTVs at any location— entry of homes, inside the house or at places of employment.
- One out of four people strongly feel that CCTVs carry a risk of illegal mass surveillance. On the other hand, nearly three out of four people also strongly believe that CCTVs help monitor and reduce crimes.
- People with higher levels of education are more likely to believe that CCTVs help in crime reduction, investigation and public safety and are less likely to believe that CCTVs can be misused for illegal mass surveillance.
- Two out of five people are aware of incidents of CCTV footage tampering or manipulation.
- Forty-four percent of people believe that CCTV cameras in police stations are very helpful in preventing human rights violations against those in custody. Close to half of the respondents strongly believe that interrogations by the police should be recorded on CCTVs.
- Over half of the respondents strongly justify the government's use of CCTV cameras for controlling protests. Those from Gujarat most likely to justify this, those from poor backgrounds and small cities least likely to support.
- Sikhs and Muslims least likely to support government use of CCTVs to control protests, Hindus most likely to support it.

CHAPTER 5

Privacy in an Age of Video Surveillance: People's Opinions about CCTVs

A Closed-Circuit Television (CCTV) system is a mode of camera surveillance that is widely used by various institutions, individuals and government agencies for the purported purpose of the safety of people, security of their assets and the maintenance of law and order. It is extensively being used by private individuals within their common and intimate spaces and by private companies and law enforcement agencies, mostly in public spaces, as a deterrent against crimes and other unlawful activities. It also has several other potential applications for public safety such as aiding the investigation of offences, improving response to emergencies, assisting in the management of places and reducing public fear of crime (Ashby, 2017).

However, the very nature of this technology also makes it vulnerable to misuse, particularly with respect to individuals' right to privacy. Because of this, some fear that CCTV systems may be used for surveillance of specific individuals and communities, and against those who disagree with governmental policies and ideology. While it can bring a sense of security for some, the same technology also raises concerns of breach of privacy and undue surveillance for others, particularly in specific locations and domains.

CCTVs have an inherent potential to be used as a tool of mass surveillance, leading to fears of the data being used to impinge on citizens' right to privacy and freedom of expression. The trade-off between security and privacy is the dilemma that people face with the advent of new technology while the law is still catching up.

There has been an exponential increase in the use of CCTV in urban areas in recent times. According to Forbes, two Indian cities– New Delhi and Chennai, are the most surveilled cities in the world. New Delhi tops the list with 1,826.6 cameras per square mile, while Chennai has 609.9 per square mile and is the third most surveilled city worldwide (Forbes, 2021). This is a glaring indication of how, in contemporary times, CCTVs have become an integral part of the urban environment (Dee, 2000).

This chapter tries to delve deeper into the pervasiveness of CCTVs in urban spaces in India. The chapter has been divided into the following sections:

- **Section 1** examines the coverage of CCTVs in the surveyed states across India. This assessment is based on people's responses on whether CCTV cameras are installed around their households, places of employment, public areas, etc., or not.
- **Section 2** looks at the agency (government, private or individual) which was involved in installing CCTVs.
- **Section 3** gauges people's support for the installation of CCTV cameras at different locations in their surroundings.
- **Section 4** investigates the fear and suspicion of CCTVs being used as a tool for mass surveillance among people. This

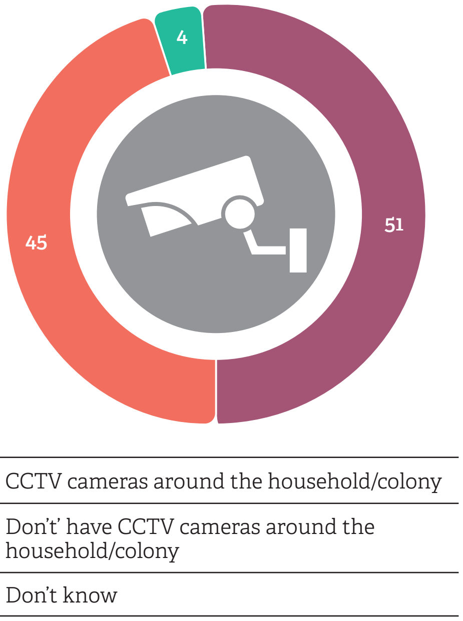
section also reports people's perceptions on whether such technology can be a threat to the privacy and safety of women in urban spaces.

- **Section 5** throws light on whether people would be comfortable sharing the data/ footage with different agencies.
- **Section 6** examines the role of CCTVs in the maintenance of law and order. It analyses the extent to which people believe that CCTVs help control crimes and violence, and facilitate police investigation.
- **Section 7** analyses people's opinion on CCTVs being used as a tool to curb political dissent and movement.

5.1. The extent of CCTV coverage in urban India

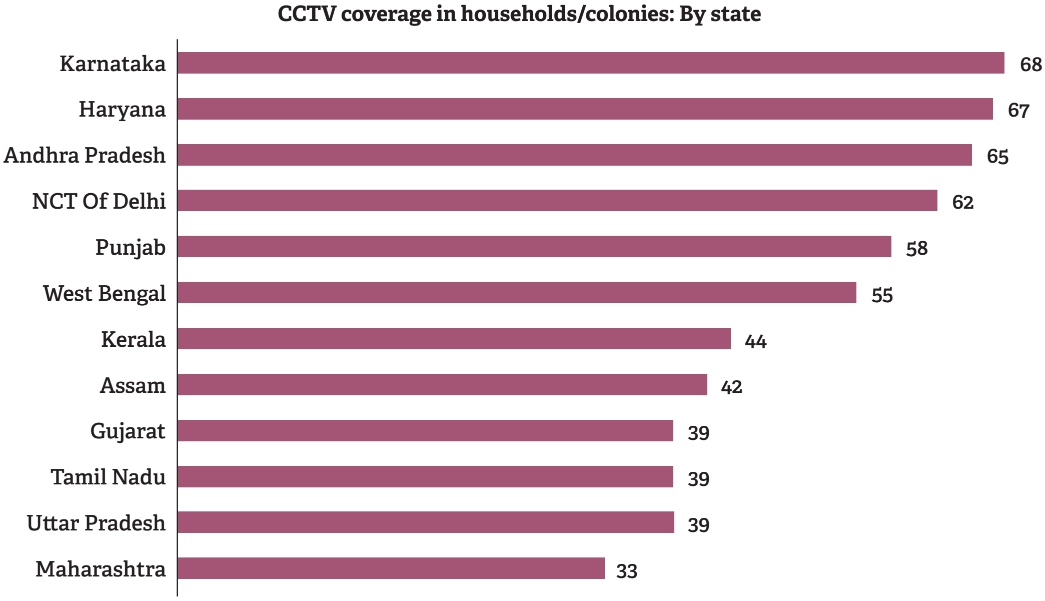
'You are under CCTV surveillance' is a commonly sighted warning sign in public places as well as in various residential areas. In this survey, respondents were asked about the pervasiveness of CCTV cameras in their locations, both public and private. A little over half (51%) of the respondents reported that their household or residential colony has CCTV coverage. The other half claimed that either there are no CCTV cameras around their residential area or they are not aware of it (Figure 5.1).

Figure 5.1: One out of two people said that CCTVs have been installed in their households/colonies



Note: All figures are in percentages.
Question asked: Do you have CCTV cameras around the household/colony you live in?

Figure 5.2: Two-thirds households in Karnataka, Haryana and Andhra Pradesh under CCTV coverage

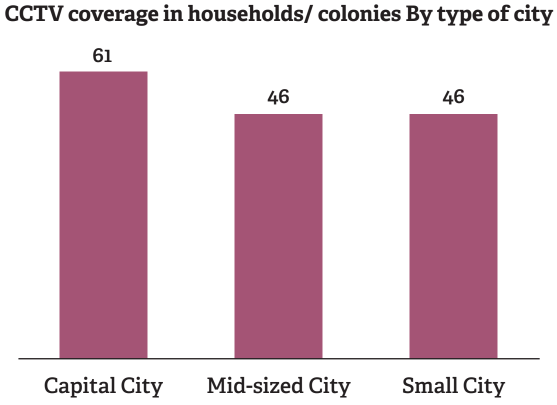


Note: All figures are in percentages. Only the percentages of those who responded "yes" has been presented.
Question asked: Do you have CCTV cameras around the household/colony you live in?

The highest proportion of respondents reporting CCTV coverage in their residential areas were from the states of Karnataka, Haryana, and Andhra Pradesh. Well over 60 percent of respondents from the NCT of Delhi said that their residential areas have CCTV coverage. On the contrary, the least coverage was reported in Maharashtra, where one-third said that their households or residential colonies had CCTV cameras (Figure 5.2).

There are important variations in responses across urban areas. The sampled cities have been categorised into three different groups – capital cities (except Andhra Pradesh, Haryana and Assam; in Andhra Pradesh, the capital city is replaced with Hyderabad, in Haryana, the capital city is replaced with Gurugram and in Assam with Guwahati)[3], mid-sized cities and small cities. As per the survey findings, CCTV coverage is highest in capital cities, with six of every ten (61%) respondents reporting the presence of CCTVs in their households/colonies, whereas, in mid-sized and small cities, a little less than half the respondents (46%) reported surveillance coverage (Figure 5.3).

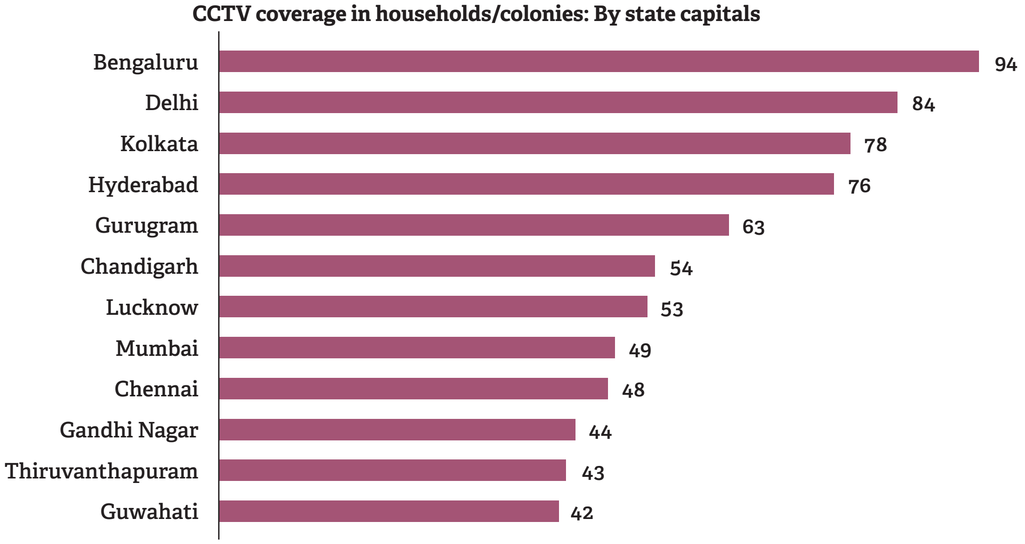
Figure 5.3: Three out of five respondents from capital cities reported CCTV coverage of their houses or colonies



Note: All figures are in percentages. Only the percentages of those who responded "yes" has been presented.
Question asked: Do you have CCTV cameras around the household/colony you live in?

In most major metropolitan capital cities, a high proportion of respondents reported CCTV coverage in their households/colonies. Bengaluru had the highest proportion of respondents reporting so, with nine of every ten (94%) respondents saying so, followed by

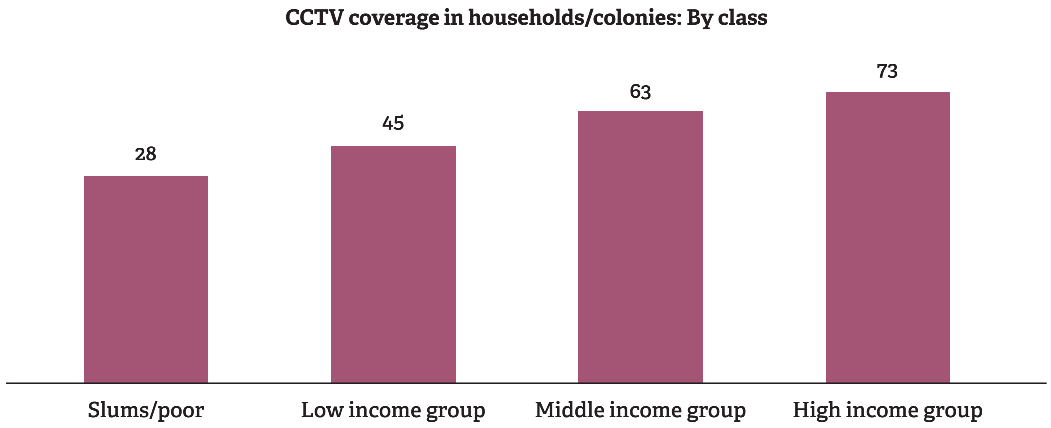
Figure 5.4: Ninety-four percent of respondents from Bengaluru reported CCTV coverage of their households/colonies



Note: All figures are in percentages. Exceptions to state capitals are Hyderabad, Gurugram and Guwahati, which have replaced the capitals of Andhra Pradesh, Haryana, and Assam respectively for this survey. Only the percentage of respondents who answered "yes" to the question has been presented in the graph.
Question asked: Do you have CCTV cameras around the household/colony you live in?

[3] Please refer the method note for the reshuffling.

Figure 5.5: High-income groups are more likely to have CCTV coverage in their residential areas, compared to slums and poor localities



Note: All figures are in percentages. Only the percentages of those who responded "yes" has been presented.
Question asked: Do you have CCTV cameras around the household/colony you live in?

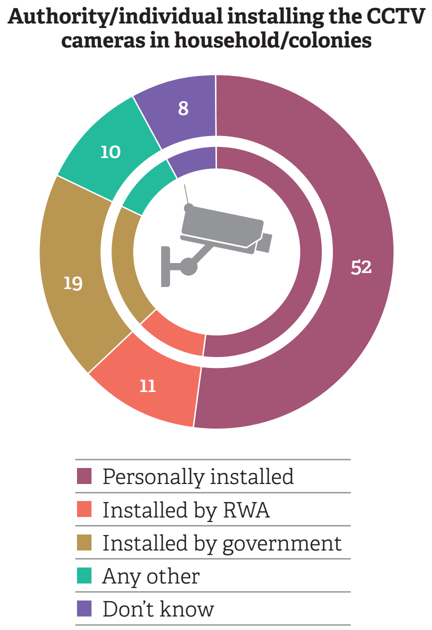
Delhi (84%), Kolkata (78%), and Hyderabad (76%). On the other hand, the lowest coverage was reported from Thiruvananthapuram (43%) and Guwahati (42%) (Figure 5.4).

An analysis of CCTV coverage by type of locality reveals that CCTV coverage increases with rising income levels. The socio-economic realities of people determine the degree of coverage (Figure 5.5). The coverage in slums or poor areas is just over one-fourth (28%), which is significantly lower than the low-income group's coverage of close to half (45%). As one moves towards the middle and high-income residential localities, CCTV coverage increases to six of every ten (63%) and seven of every ten (73%) respectively.

5.2. Who installed the CCTV camera?

People were asked about the agency involved in the installation of CCTV. Respondents were asked whether the authority involved in the installation of cameras was the government, their Resident Welfare Association (RWA) or if it was installed by the respondent for private use. Over half (52%) of the respondents answered that CCTV cameras have reportedly been installed by private individuals themselves. One out of five (19%) respondents said that the CCTVs in their residential area were installed by the government (Figure 5.6).

Figure 5.6: One out of two respondents personally installed CCTV cameras in their households/colonies

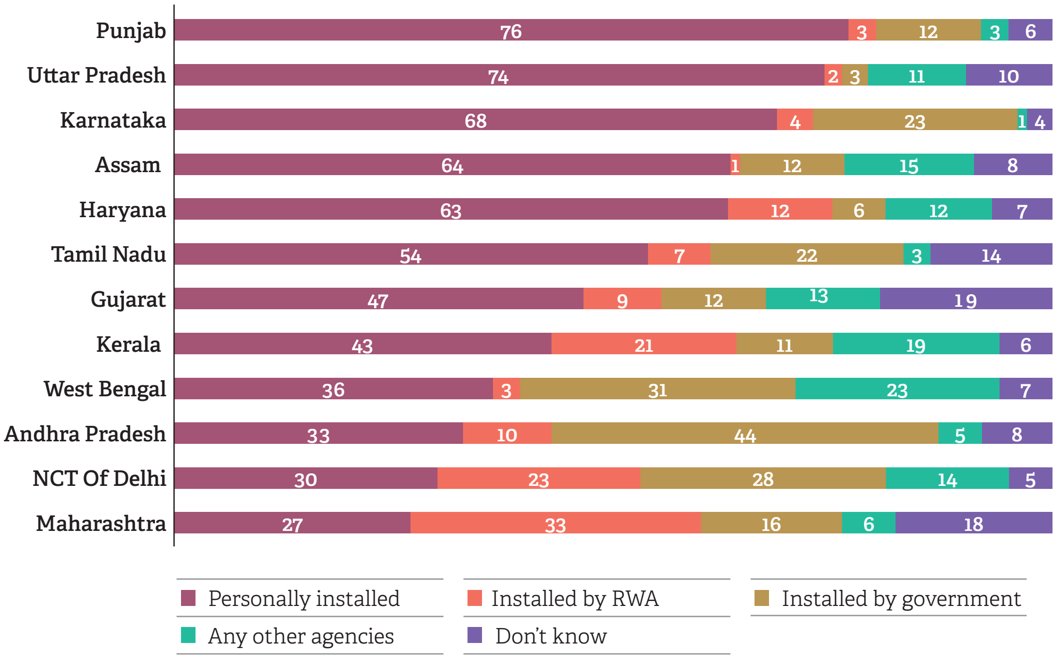


Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/residential localities.
Question asked: Were they installed by you or some other authority?

In states like Punjab, Uttar Pradesh, Karnataka, Assam, and Haryana, the majority of respondents reported personally installing CCTV cameras in their houses/colonies. Close to two-thirds in Karnataka, Assam, and Haryana reported doing the same. Whereas in Andhra Pradesh, West Bengal, and the

Figure 5.7: Across states, individuals most likely to install CCTVs in their houses/colonies than the government, except Andhra Pradesh

“Who installed the CCTV camera in your house/colony?”: By State

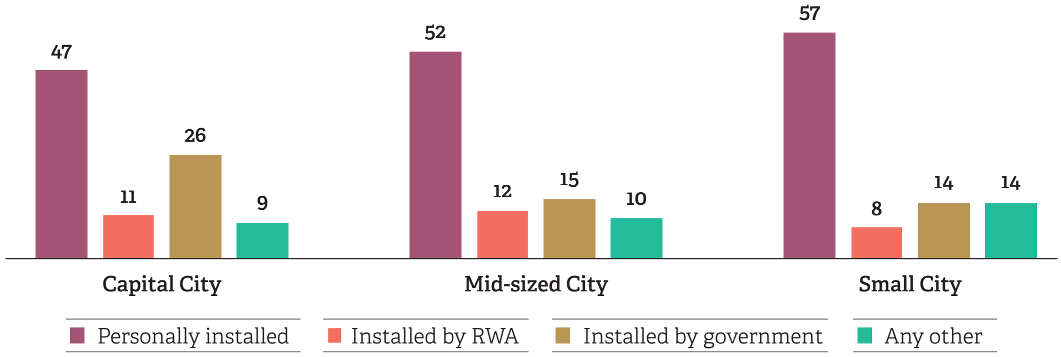


Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/residential localities.
Question asked: Were they installed by you or some other authority?

NCT of Delhi, the government is the leading authority involved in the installation of CCTV cameras in residential areas, with 44 percent, 31 percent and 28 percent of respondents respectively reporting so. On the other hand, in Uttar Pradesh and Haryana, merely three and six percent of people respectively said that the cameras in their residential localities were installed by the government. In Maharashtra, one-third of the respondents (33%) said cameras in residential areas were installed by the RWAs. Our data show that in West Bengal and Kerala, other agencies such as market committees and other unions are more likely to have installed the cameras (Figure 5.7).

Figure 5.8: Government more likely to install CCTV cameras in residential areas in the capital cities, compared to mid-sized and small cities

Who installed the CCTV camera in your house/colony?”: By Type of City



Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/ residential areas. Rest did not respond.
Question asked: Were they installed by you or some other authority?

In capital cities, one-fourth (26%) of the respondents said that the CCTV cameras in their residential areas were installed by the government, which is higher than in other urban areas. In all categories of urban areas –be it capital cities, mid-sized cities or small cities, a majority of the cameras were installed by private individuals (Figure 5.8).

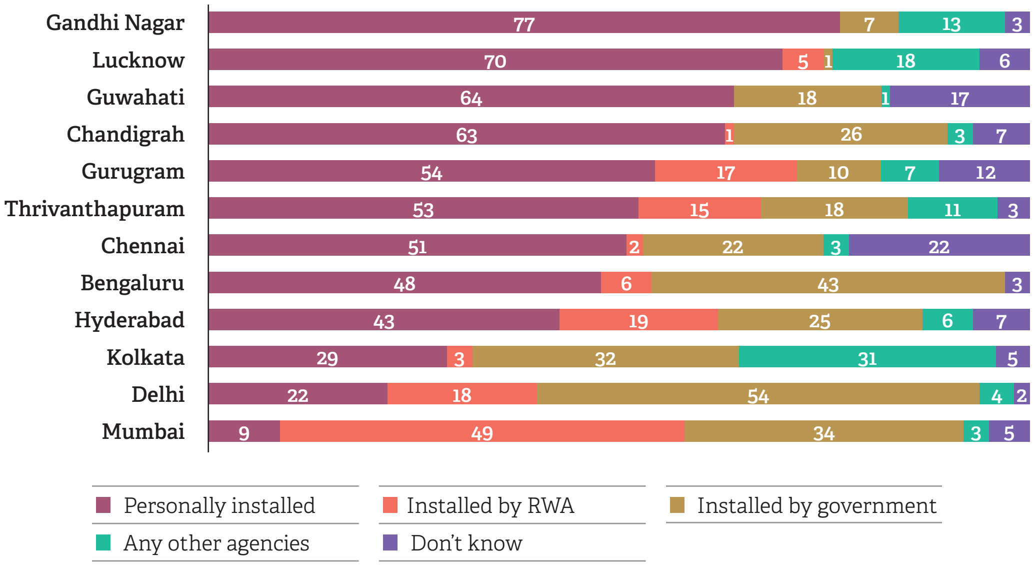
While examining capital cities, it was found that those from Delhi reported the highest proportion (54%) of government-installed CCTVs in their residential localities. This was followed by Bengaluru, where a little over two-fifths (43%) said that the government had installed the cameras in their localities. At the other end of the spectrum, in Gandhinagar, more than three-fourths (77%) and in Lucknow seven of every ten (70%), said that they had personally installed CCTV cameras in their localities. Conversely, in Mumbai, one in every ten people (9%) stated that they had installed cameras in their areas. Instead, close to half of the respondents in Mumbai named RWAs as the agency which had installed the cameras (Figure 5.9).

Just as CCTV cameras are more likely to be installed in high-income localities compared to slums or poor localities, similarly, we found that respondents from high-income residential areas were almost twice as likely to have personally installed CCTV cameras compared to other respondents. Conversely, the government is nearly three times as likely to install CCTVs in slums and poor localities than in high-income localities. While 31 percent of respondents from lower-income areas said that the government had installed CCTVs in their households or residential colonies, just about nine percent of the respondents from high-income groups said so (Figure 5.10).

Even though there is no evidence to suggest that the police or the government in India actively use CCTVs in residential areas to surveil people from poor or vulnerable localities, however, the widespread presence of cameras in such localities can be a potential cause for concern and needs to be further analysed. Academic literature from across the world has noted that policing is often more proactive and aggressive in vulnerable and

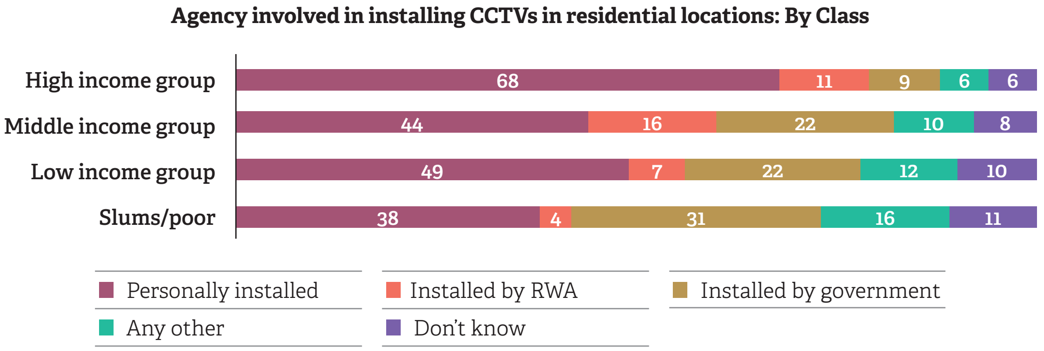
Figure: 5.9: One out of two people from Delhi said that the CCTVs in their localities were installed by the government

"Who installed the CCTV camera in your house/colony?": Capital Cities



Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/ residential areas. Rest did not respond.
Question asked: Were they installed by you or some other authority?

Figure 5.10: Government three times more likely to install CCTV cameras in slums/poor localities, compared to higher-income localities



Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/ residential areas.
Question asked: Were CCTVs installed by you or some other authority?

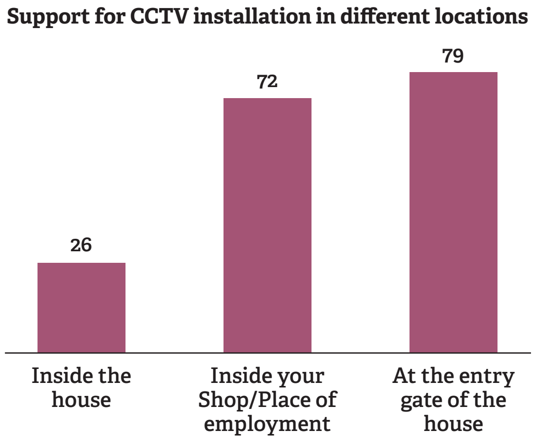
poor localities. With the advent of technologies such as CCTVs, video surveillance has also been used to target and surveil marginalised communities and localities in several countries (Neusteter & Khogali, 2018; Nwadike, 2020; O'Brien, 2021). Seen in this context, the misuse of technology by the government and the police to further marginalise already vulnerable communities needs to be studied carefully. The Status of Policing in India 2018- A Study of Performance and Perceptions found that while the rich are most likely to have contacted the police themselves, the poor are twice as likely to have been contacted by the police, thus suggesting an already tenuous relationship between the police and the poor. If surveillance technology were to be potentially used by the police or the government for targeting specific groups in India, then this data would suggest a rising trend of over-surveillance in poor localities.

5.3. Public versus private spaces: Location of CCTV cameras

The survey also asked people where they feel a CCTV camera should be installed– inside their house, at the entry of their house or inside a place of work or employment. More than three-fourths of the people were in support of the installation of CCTV cameras at the entry of their house (79%) or inside their shop/place of employment (72%). However, when it comes to presence of cameras in one's personal space, the support dropped down to just above a quarter (26%) (Figure 5.11). This indicates that while people are largely comfortable with having CCTVs in semi-public areas such as the entry of their house or workplaces, when it comes to intimate and personal spaces, there is a stronger inclination for the preservation of the right to privacy.

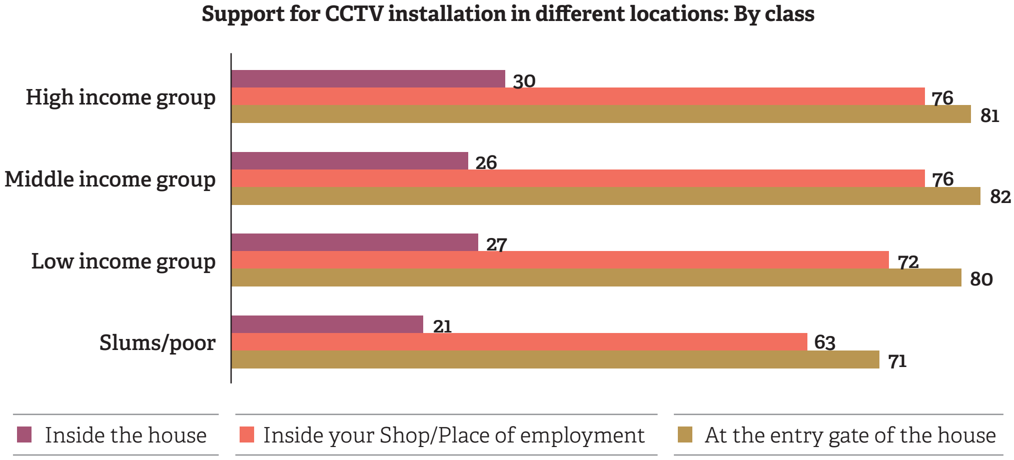
Additionally, a linear trend was found between those supporting the installation of cameras and the type of locality. Respondents from all income groups are more likely to support

Figure 5.11: Four out of five people support the installation of CCTV cameras at the entry gate of their houses



Note: All figures are in percentages. Rest of the respondents did not support the installation of cameras or did not answer.
Question asked: Would you support the installation of CCTV cameras at these places?

Figure 5.12: Poor least likely to support installation of CCTVs at any location—entry of homes, inside the house or at places of employment

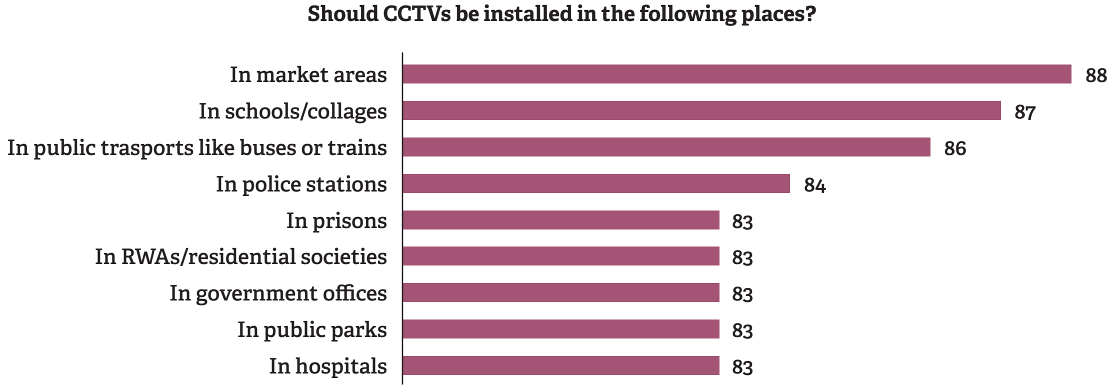


Note: All figures are in percentages. Rest of the respondents did not support the installation of cameras or did not answer. Question asked: Would you support the installation of CCTV cameras at these places?

the installation of CCTVs either at their entry gate or inside their shop or place of employment, and less likely to support its installation inside their homes. Those from slums or poor localities were less likely to support the installation of CCTVs at any of the locations—whether inside their homes, at the entry gates of their houses, or in places of their work or employment. Nearly eight of every ten respondents from high, middle and low-income localities expressed their preference for CCTV installation at the entry of their house, but this number fell to seven of every ten (71%) among the poor-income groups. Notably, the support for placing CCTV cameras inside the home is more in the high-income groups. Nearly a third (30%) of the surveyed people residing in high-income localities were comfortable with cameras inside their homes whereas only two of every ten from the poor-income localities said that they would want CCTV cameras inside their homes (Figure 5.12).

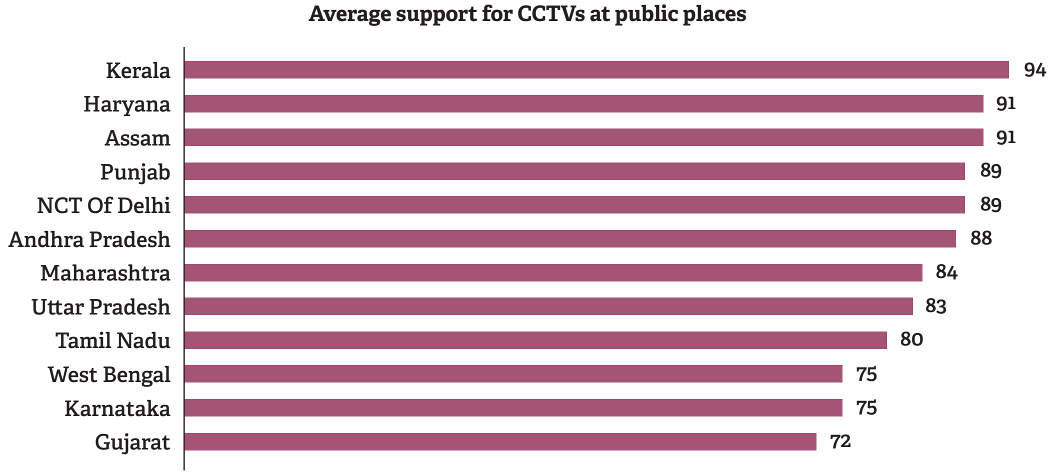
The survey also posed a question about the installation of cameras in public places – marketplaces, educational institutions, buses or trains, hospitals, parks, within societies or in other public places. Eight of every ten respondents supported the installation of cameras in all of these public spaces, with the highest levels of support for installation in markets (88%) (Figure 5.13).

Figure 5.13: More than eight out of ten people feel that CCTVs should be installed in public places



Note: All figures are in percentages. Rest of the respondents did not support the installation of cameras or did not answer. Question asked: Would you support the installation of CCTV cameras at these places?

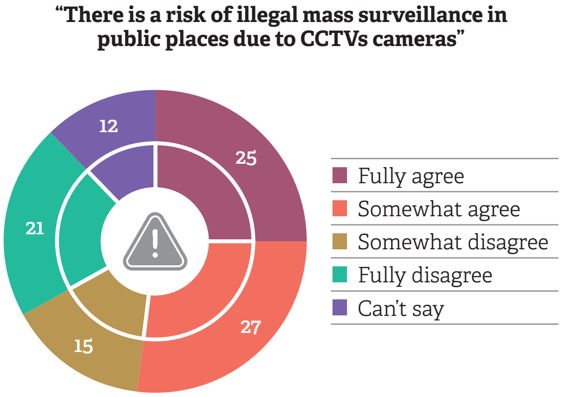
Figure 5.14: People from Kerala most supportive of CCTVs in public places



Note: All figures are in percentages. Rest of the respondents did not support the installation of cameras or did not answer.
Question asked: Would you support the installation of CCTV cameras at these places?

The study also tried to determine how the support for the installation of CCTVs in various public places varied across states. In states like Kerala, Haryana, and Assam, more than 90 percent of respondents supported the installation of CCTVs in public places. People are largely in favour of the installation of CCTVs in public places, with respondents from Gujarat exhibiting the least amount of support at 72 percent (Figure 5.14). This may be suggestive of the people associating CCTVs with a sense of safety and security in public places on the one hand, and significantly lower concerns about the breach of privacy in such shared spaces on the other.

Figure 5.15: One out of four people strongly feel that CCTVs carry a risk of illegal mass surveillance



Note: All figures are in percentages.
Question asked: Please tell me whether you agree or disagree with the statement: There is a risk of illegal mass surveillance in public places due to CCTVs cameras?

5.4. Fear of mass surveillance

Communication technology has made enormous developments in the modern world and has touched every sphere of people's lives, from security to entertainment. However, this has also come at a cost. While technology may aid the investigation of crimes, it also might lend itself to misuse, whether by individuals, private organisations or even government agencies.

In this section, we tried to analyse people's perception of CCTV cameras in public places on their sense of privacy. The study tried to examine the extent to which people agree that CCTV cameras have the potential to be used as an instrument of illegal mass surveillance. The respondents' perceptions were divided on this issue. One out of two respondents (52%) felt that there is a fear of mass surveillance with the increased presence of CCTV cameras in public places, with one-fourth (25%) fully agreeing with the statement and a little over one-fourth (27%) agreeing partially. On the other hand, two of every ten respondents did not agree with the notion that CCTV cameras in public spaces entail a risk to their privacy, while another 15 percent somewhat disagreed with the statement (Figure 5.15). While a multitude of reasons could be attributed to either the agreement or disagreement with the statement, it could also be indicative of the level of trust they place in the agencies involved in the installation of these cameras and those who have access to them.

In Tamil Nadu, a significant proportion of the respondents (73%) felt that the installation of CCTVs in public places runs the risk of illegal mass surveillance. Similar levels of concern were also observed in another southern state -- Andhra Pradesh (including Hyderabad city from Telangana state), where 60 percent of respondents were concerned about mass surveillance. On the other hand, in Assam, a larger section of people (45%) believed that the increased presence of CCTV cameras in public spaces does not pose a risk of illegal surveillance (Table 5.1).

When the data is analysed with regards to the religion of the respondents, one-fourth of Hindu and Muslim respondents (25% each) agreed that CCTVs in public places entail a risk of illegal mass surveillance. Every third Christian respondent (31%) agreed that CCTV in public places put their privacy at risk. When compared with other religious communities, Sikhs were least likely to believe that there is a risk of mass surveillance, with four of every ten (39%) fully disagreeing with the statement (Table 5.2).

We also sought to understand how educational background affected people's opinion of CCTVs and mass surveillance. It is widely believed that people having access to higher education would have a greater desire to secure their privacy. However, findings from the survey did not prove this hypothesis as there was no clear pattern of agreement or disagreement among people of different educational levels. Close to a quarter of respondents from all educational levels fully agreed that there is a risk of illegal mass surveillance due to the prevalence of cameras in public places. Conversely, a quarter of the college-educated or above respondents completely disagreed with the statement, while just 18 percent of the non-literates completely disagreed with the statement, thus indicating slightly more faith in CCTV technology among the highly educated as against the non-educated respondents (Table 5.3).

Table 5.1: Fear of CCTVs leading to mass surveillance highest in Tamil Nadu, lowest in Assam

States	Risk of illegal mass surveillance in public places due to CCTVs cameras		
	Agree	Disagree	Can't say
Tamil Nadu	73	23	4
Andhra Pradesh	61	28	11
Haryana	55	39	6
West Bengal	55	30	15
Kerala	54	33	13
Maharashtra	54	27	19
Gujarat	53	35	12
Karnataka	51	46	3
Uttar Pradesh	50	35	15
NCT Of Delhi	47	45	8
Punjab	41	44	15
Assam	33	45	22

Note: All figures are in percentages.
Question asked: Please tell me whether you agree or disagree with the statement: There is a risk of illegal mass surveillance in public places due to CCTVs cameras?

Table 5.2: Both Hindus and Muslims equally likely to believe that CCTVs can be misused for illegal mass surveillance

Religion	Risk of illegal mass surveillance in public places due to CCTVs cameras			
	Fully agree	Somewhat agree	Somewhat disagree	Fully disagree
Hindu	25	28	15	21
Muslims	25	27	17	15
Christians	31	27	15	14
Sikh	18	25	10	39
Others	28	18	11	28

Note: All figures are in percentages. Rest did not respond.
Question asked: Please tell me whether you agree or disagree with the statement: There is a risk of illegal mass surveillance in public places due to CCTVs cameras?

Table 5.3: Those with higher levels of education are less likely to believe that CCTVs can be misused for illegal mass surveillance

Level of Education	Risk of illegal mass surveillance in public places due to CCTVs cameras			
	Fully agree	Somewhat agree	Somewhat disagree	Fully disagree
Non-Literate	23	21	10	18
Upto Primary	22	28	14	15
Upto Matric	26	26	15	19
Intermediate-under graduate	24	31	15	19
College and above	25	27	16	24

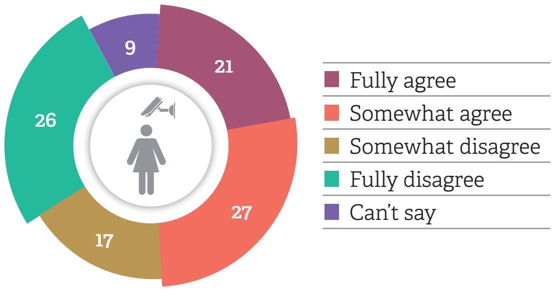
Note: All figures are in percentages. Rest did not respond.
Question asked: Please tell me whether you agree or disagree with the statement: There is a risk of illegal mass surveillance in public places due to CCTVs cameras?

5.4.1. Surveillance of women

Security and privacy have become a great concern for people from different backgrounds and identities, especially women (Bhandari, 2021). The sense of invasion of privacy due to CCTV cameras in public places and other spaces is more in women compared to men because it is linked with the perpetuation of violence against them through technological means (Mason and Magnet, 2012). This insecurity is compounded by uncertainty over who has access to the data from the cameras. Particularly in the context of rising digital voyeurism, where spy cameras are installed to snoop on people in private spaces, such technology can be especially threatening. In an age where the boundaries between private and public spaces are being constantly negotiated, incidents such as the online circulation of intimate footage captured through CCTVs raise concerns over women's right to privacy in public spaces (Barman, 2019).

Taking these issues into consideration, people were asked to what extent they think CCTV cameras in public places can be used against women to monitor them. Two of every ten respondents (21%) completely agreed that there is a possibility of cameras being used against women in public places to monitor them. On the other hand, one-fourth of respondents (26%) strongly disagree with the possibility (Figure 5.16).

Figure 5.16: One out of two people are of the opinion that CCTVs in public places can be used against women to monitor them



Note: All figures are in percentages.
Question asked: Please tell me whether you agree or disagree with the statement: CCTVs cameras in public places can be used against women to monitor them.

At the state level, people in Tamil Nadu, Gujarat, Karnataka, and Maharashtra, largely believe that CCTV cameras in public places can be used to monitor women. On the contrary, in Punjab, Kerala, and Assam most respondents disagreed with the statement, though in Assam one-fifth did not share their opinion on this question (Table 5.4). As seen earlier in Table 5.1, respondents from Tamil Nadu were most likely to fear misuse of CCTVs for illegal mass surveillance. Similarly, those from Tamil Nadu are also most likely to believe that CCTVs in public places can be used to surveil women.

Interestingly, gender does not make much of a difference in the perception of men and women on the potential misuse of CCTVs against women. The dilemma of the choice between security and violence seems to be reflected in the responses of both men and women. The survey shows that men and women think alike on the subject (Table 5.5).

5.5. Data security and privacy: who can access CCTV data?

Access to CCTV cameras is a highly sensitive matter and the prevention of its misuse depends to a great extent on the ability to secure the data collected. With rising cybercrimes coupled with notable vacuums in the law regarding data security; breach of data, including CCTV data, has become commonplace. Worldwide, cases of terrorist organisations hacking CCTV cameras have

Table 5.4: Seven in ten respondents from Tamil Nadu agree that CCTVs in public spaces can be used against women to monitor them

States	CCTVs cameras in public places can be used against women to monitor them		
	Agree	Disagree	Can't say
Tamil Nadu	67	30	3
Gujarat	57	36	7
Karnataka	54	44	2
Maharashtra	51	35	14
Haryana	51	45	4
Andhra Pradesh	49	43	8
NCT Of Delhi	47	49	4
Uttar Pradesh	47	39	14
West Bengal	43	45	12
Kerala	36	54	10
Punjab	36	53	11
Assam	34	46	20

Note: Numbers are aggregate of agree (fully & somewhat) and disagree (fully & somewhat). All figures are in percentages.
Question asked: Please tell me whether you agree or disagree with the statement: CCTVs cameras in public places can be used against women to monitor them.

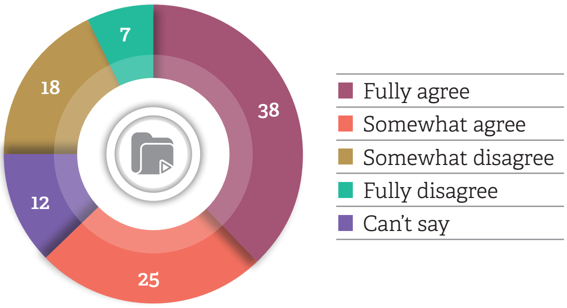
Table 5.5: No difference of opinion across genders on the issue of CCTVs being a threat to women's privacy

	CCTVs cameras in public places can be used against women to monitor them	
	Agree	Disagree
Male	47	44
Female	47	43

Note: Numbers are aggregate of agree (fully & somewhat) and disagree (fully & somewhat). All figures are in percentages. Rest did not respond.
Question asked: Please tell me whether you agree or disagree with the statement: CCTVs cameras in public places can be used against women to monitor them.

been on the rise, as have cases of private hacking of CCTVs. For instance, recently in Tehran, 5,000 surveillance cameras and 150 websites were hacked by a group (Iran International, 2022). Therefore, we sought the public's perception of how safe they think CCTV data is.

Figure 5.17: Two out of five people believe that only the person/agency who has installed CCTV cameras has access to the footage



Note: All figures are in percentages.
Question asked: Please tell me whether you agree or disagree with the statement: CCTV cameras footages can be accessed only by the person who has installed it.

Respondents were asked to what extent they believe that access to camera footage is available only to the owning individual/agency. Four of every ten (38%) fully believed that access to CCTV camera footage was only available to the person who had it installed. Another quarter of respondents (25%) agreed with the statement to some extent. There were, however, three of every ten (30%) who disagreed with the statement (Figure 5.17).

5.6. CCTV and crime control

CCTV cameras are often used by law enforcement agencies to ensure public safety, deter criminal activity, prevent crimes and aid the investigation of cases. With this rationale, many state governments in India have made it compulsory to install cameras in public places for the maintenance of law and order (Press Trust of India, 2022; Indian Express, 2022; Deccan Herald, 2018; NDTV, 2020).

In this section, we examine to what extent people in urban areas believe that CCTV

Table 5.6: Nearly three out of four people strongly believe that CCTVs help monitor and reduce crimes

	Fully agree	Somewhat agree	Somewhat disagree	Fully disagree
CCTV cameras help to monitor and reduce crimes	72	20	3	2
CCTV cameras help in crime investigation	41	22	19	13
CCTV cameras in public places make people feel safer	35	19	20	18

Note: All figures are in percentages. Rest did not respond.
Question asked: Please tell me whether you agree or disagree with the statements given in the first column of the table.

Table 5.7: Overwhelming majority across states believes CCTVs help monitor and reduce crime

States	Monitor and reduce crime	Help in crime investigation	Make people feel safe
Kerala	97	88	68
Haryana	97	67	59
Andhra Pradesh	97	63	61
NCT Of Delhi	96	72	63
Gujarat	95	68	57
Assam	91	77	71
Maharashtra	91	47	41
Punjab	91	47	47
Uttar Pradesh	90	57	51
Tamil Nadu	90	46	34
Karnataka	86	55	39
West Bengal	84	60	48

Note: Only the percentages of those who agree (fully & somewhat). have been presented here. All figures are in percentages. Rest of the respondents either disagreed (fully & somewhat) or did not answer.
Question asked: Please tell me whether you agree or disagree with the statements given in the first column of the Table 5.6.

cameras are useful in the maintenance of law and order. They were asked if CCTVs help in crime reduction, investigation and making public spaces safer. Close to three-fourths of the respondents (72%) fully agreed that it helps in the monitoring and reduction of crimes. While four in every ten (41%) believe that CCTVs are beneficial in the investigation of crimes, another one-third (35%) agreed that it gives a sense of security to people in public places (Table 5.6).

Across the states in which this study was conducted, nearly all respondents from Kerala, Haryana, and Andhra Pradesh (97% each) felt that CCTVs help in monitoring and reducing crime. Notably, in Tamil Nadu, a third of the respondents (34%) felt that CCTVs make people feel safer, yet 90 percent believe that they aid in crime reduction. Those from West Bengal were most sceptical (84%) about the importance of CCTVs in controlling crime and were least likely to

Table 5.8: People with higher levels of education are more likely to believe that CCTVs help in crime reduction, investigation and public safety

Level of Education	Monitor and reduce crime	Help in crime investigation	Make people feel safe
Non-Literate	82	51	45
Upto Primary	87	60	51
Upto Matric	92	62	52
Intermediate-under graduate	93	62	51
College and above	95	68	59

Note: Only the percentages of those who agree (fully & somewhat). have been presented here. All figures are in percentages. Rest of the respondents either disagreed (fully & somewhat) or did not answer.
Question asked: Please tell me whether you agree or disagree with the statements given in the first column of the Table 5.6.

agree that it helps monitor and reduce crime (Table 5.7).

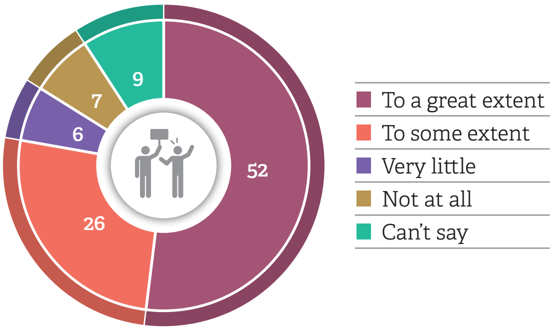
As levels of educational attainment rose, there was increasing trust in CCTVs utility in monitoring and reduction of crime. While eight of every ten (82%) among non-literates agreed with the statement, the proportion rose to nine of every ten (95%) when it came to those who had access to college education. The level of education is directly proportional to the perception of cameras in the domain of law and order. Six of every ten (68%) respondents who had access to college education reported that cameras help in assisting the process of crime investigation. In comparison to them, a little over half (51%) of the non-literate respondents endorsed this view (Table 5.8).

5.7. Curbing political movement through CCTV camera

In the past few years, there have been allegations of the police and government using data from CCTVs to target and control those who either disagree with the government's policies or minority groups. For instance, there were allegations of the police identifying those who were protesting against the Citizenship Amendment Act (Ulmer & Siddiqui, 2020), or allegations of the police selectively identifying and targeting Muslims from the 2020 Delhi riots, all using CCTV footage (Santoshini, 2022). A recently released report on the 2020 Delhi riots, "Uncertain Justice: A Citizen's Committee Report on the North East Delhi Violence", authored by several retired judges and IAS officers, also finds that in many cases where the Delhi Police submitted CCTV footage in the court as evidence, the submitted footage either exonerated the accused or failed to back the charges made by the police, thus suggesting misuse of the technology for political purposes (Lokur et.al. 2022). The founder of an Indian start-up Innefu Labs, which uses facial recognition software AI Vision, claimed that police in 10 states use their software technological products to clamp down on protests and political movements (Ulmer & Siddhiqui, 2020).

Figure 5.18: Over half of the people strongly justify the use CCTV cameras for controlling protests

"To what extent is it justified for the government to use CCTV data to control protests against government policies?"



Note: All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use CCTV cameras to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

Amid these concerns, we tried to ascertain people's opinions about the government using surveillance to curb political dissent. A majority (52%) believe it is justified for the government to use CCTV cameras to curb political movements, protests, and agitations against its policies. In comparison to this, only seven percent are against the use of cameras to control dissent (Figure 5.18).

Nearly 95 percent of the respondents in Gujarat justified the government's use of CCTV as a means to control political movements of all sorts (Table 5.9). Two-thirds of the respondents from Uttar Pradesh and Haryana (65% and 64% respectively) completely supported the use of CCTV in clamping down on protests. In these three states, there was an extremely small proportion of people who were against CCTVs being used by the state for political purposes. All three states are currently ruled by the BJP. However, respondents from West Bengal, Punjab and Karnataka were not as enthusiastic in their support. Only one-third of the respondents (29%) from Bengal completely justified the use of surveillance footage to curb dissent. The number is slightly higher in Punjab (36%) and Karnataka (37%) (Table 5.9).

Table 5.9: Those from Gujarat most likely to support government use of CCTV to control protests

States	Use CCTV cameras to curb political movement or protests against policies & laws enforced by the government				
	To a great extent	To some extent	Very little	Not at all	Can't say
Gujarat	84	10	2	1	3
Uttar Pradesh	65	19	2	2	12
Haryana	64	21	4	5	6
Andhra Pradesh	60	23	4	7	6
NCT Of Delhi	59	22	5	6	8
Maharashtra	53	22	3	9	13
Tamil Nadu	48	28	12	8	4
Kerala	46	27	7	13	7
Assam	42	33	6	7	12
Karnataka	37	46	13	3	1
Punjab	36	29	8	10	17
West Bengal	29	28	12	15	16

Note: All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use CCTV cameras to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

Across dwellings, a little less than half of the small cities (49%) strongly agreed with this practice, the proportion went up to 56 percent in capital cities. Similarly, support for this went up with an increase in the class status of the respondents (Table 5.10).

Across all age groups, there is a general consensus in favour of the use of CCTV by the

Table 5.10: People from small cities and poor backgrounds least likely to support the use of CCTVs to curb political movements or protests

States	Use CCTV cameras to curb political movement or protests against policies & laws enforced by the government				
	To a great extent	To some extent	Very little	Not at all	Can't say
Cities					
Capital Cities	56	25	5	7	7
Mid-sized Cities	52	24	7	9	8
Small Cities	49	29	7	6	9
Slums/poor	46	24	8	8	14
Type of localities					
Low-income locality	52	27	6	7	8
Middle-income locality	54	26	6	7	7
High-income locality	58	24	6	7	5

Note: All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use CCTV cameras to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

Table 5.11: Sikhs and Muslims least likely to support the use of CCTV cameras to curb political movements or protests

Religion	Use CCTV cameras to curb political movement or protests against policies & laws enforced by the government				
	To a great extent	To some extent	Very little	Not at all	Can't say
Hindus	54	25	6	7	8
Muslims	48	25	7	8	12
Christians	52	24	7	12	5
Sikhs	46	30	9	8	7
Other minority religions	49	26	5	12	8

Note: All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use CCTV cameras to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

government to control political movements and protests against it. Almost half of the respondents in all age groups fully support the government's use of technology to curb opposition. While those who are totally against this are a small number – it does not exceed one of every ten in any age group.

Support for the curbing of political dissent by means of CCTV cameras is the least among religious minorities such as Sikhs and Muslims. Forty-six percent of Sikhs and 48 percent of Muslims justify the use of CCTV for political motives. Followers of both these religions disagree with it in equal proportion (Table 5.11). This could well be linked to the perception of the government's attitude towards the protests of Muslims after the Citizenship Amendment Act was passed in 2020 and farmers' protests against the now-scrapped farm laws in which the Sikh community participated in large numbers. The current dispensation has dealt with protesters belonging to minorities and their allies- protesting for their democratic rights with a stringent crackdown (Human Rights Watch, 2021).

Conclusion

Closed-circuit technology has now become an integral part of the modern world. Without it the exercise of security is unimaginable. There are multiple intricacies around this technology and this chapter brings to light the different dynamics as well as complexities involved in the purveyance of CCTV cameras in public spaces. It examines the perspectives of people with regard to CCTV cameras and issues related to them such as illegal surveillance, surveillance against women in public places and the government's use of CCTV cameras for political motives.

Amongst the surveyed locations, half the population reported being under CCTV coverage, indicating their widespread usage, particularly in urban areas. These cameras have been installed by various agencies, including the government and the security forces or the police. There is extensive support for the use of CCTVs among the public, with eight of every ten supporting the installation of CCTV cameras in public places.

Even though the differences in responses are small, a general trend emerged that those residing in slums and poor localities are least likely to support the installation of CCTVs in either private, semi-private or public spaces and are most vary of the way in which the data is used, while those from high-income localities are most likely to support it. Yet, respondents from slums are also three times more likely to report that the government has installed CCTV cameras in their localities, while those from high-income localities are far more likely to have privately installed the cameras.

Even as empirical evidence suggests that CCTVs have little to no impact on the instances of crime in a locality (Ratcliffe and Rosenthal, 2021), the general public is largely of the opinion that they help in monitoring and reducing crimes. An unsettling popular opinion is that more than half the population justifies the government's usage of CCTV data to curb protests. Predictably, religious minorities are less likely to hold this opinion. Even amongst these groups, however, the practice's support levels are notably high.

Overall, the findings suggest that the public, to a large extent, trusts mass surveillance technologies such as CCTVs, believing that these will ensure their own safety and security. Despite its widespread usage in the surveyed localities, very little critical opinion emerged on this issue, except among minorities and under-privileged.

References

Ashby, M.P.J. (2017) The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research,* 441-459.

Barman, S.R. (2019, August 3). Delhi Metro Orders Probe as Footage Featuring Couple is Leaked. *Indian Express*. Retrieved from: https://indianexpress.com/article/cities/delhi/delhi-metro-orders-probe-as-footage-featuring-couple-is-leaked-5861920/.

Bhandari, A. (2021, March 8).Feminist Perspectives on Space, Safety and Surveillance: Improving a Woman's Right to the city. *The Wire.* Retrieved from: https://thewire.in/women/feminist-perspectives-on-space-safety-and-surveillance-improving-a-womans-right-to-the-city.Accessed on 18th October 2022.

Common Cause and Centre for Study of Developing Societies (2018). Status of Policing in India Report 2018—A Study of Perceptions and Performance. Retrieved from: https://commoncause.in/pdf/SPIR-2018-c-v.pdf.

Deccan Herald, (2018, July 29). 'CCTV cameras to be made mandatory in public places'. Retrieved from: https://www.deccanherald.com/cctv-camera-mandatory-public-684341.html. Accessed on 9th November 2022.

Dee, M. J. (2000) The use of CCTV to police public spaces: a case of big brother or big friend? *Public Space & Cities for the Well-Being of Children, Forbes India.* (2021, August 25). Delhi, Chennai among most surveilled in the world, ahead of Chinese cities. Retrieved from:https://www.forbesindia.com/article/news-by-numbers/delhi-chennai-among-most-surveilled-in-the-world-ahead-of-chinese-cities/69995/1. Accessed on 18th October 2022.

Human Rights Watch. (2021, February 19). India: Government policies, Actions Target Minorities. Retrieved from:https://www.hrw.org/news/2021/02/19/india-government-policies-actions-target-minorities.Accessed on 20th October 2022.

Indian Express. (2022, March 31). CCTVs mandatory at certain establishments, Bill passed. Retrieved from: https://indianexpress.com/article/cities/gandhinagar/cctvs-mandatory-at-certain-establishments-bill-passed-7845178/. Accessed on 9th November 2022.

Iran International. (2022, February 6). Tehran's 5,000 Surveillance Cameras, 150 Sites Hacked. Retrieved from: https://www.iranintl.com/en/202206025165.

Lokur, M.B., Shah, A.P., Sodhi, R.S., Prakash, A. (Justices) and Pillai, G.K. (2022). Uncertain Justice: A Citizen's Committee Report on the North East Delhi Violence 2020. *Constitutional Conduct Group.* Retrieved from: https://constitutionalconduct.files.wordpress.com/2022/10/uncertain-justice-citizens-committee-report-on-north-east-delhi-violence-2020.pdf.

Mason, C.,& Magnet, S. (2012). Surveillance Studies and Violence Against Women. *Surveillance and Society.* 10, 105-118.

NDTV. (2022, February 26).CCTV Cameras To Become Mandatory In Maharashtra Buildings, says Minister. Retrieved from:https://www.ndtv.com/india-news/cctv-cameras-to-become-mandatory-in-maharashtra-buildings-says-home-minister-anil-deshmukh-2186243. Accessed on 9th November 2022.

Neusteter, R. and Khogali, M. (2018). Emerging Issues in American Policing. *Vera Institute of Justice.* Retrieved from: https://www.vera.org/publications/emerging-issues-in-american-policing-digest/volume-5/digest-5.

Nwadike, C. (2020, January 16). Privacy and Welfare Surveillance Among Vulnerable Communities. *Internews.* Retrieved from: https://internews.org/commentary/privacy-and-welfare-surveillance-among-vulnerable-communities/.

O'Brien, G. (2021). Racial Profiling, Surveillance and Over-Policing: The Over-Incarceration of Young First Nations Male in Australia. *Social Sciences,* 10(2), 68.

Press Trust of India. (2022, February 23). CCTV cameras to be made mandatory for major institutions in Rajasthan. Retrieved from:https://www.business-standard.com/article/current-affairs/cctv-cameras-to-be-made-mandatory-for-major-institutions-in-rajasthan-cm-122022301323_1.html. Accessed on 9thNovember 2022.

Ratcliffe, J. & Rosenthal, J.M. (2021). Video Surveillance of Public Places, 2nd edition. Response Guide No. 4. *ASU Center for Problem-Oriented Policing.* Retrieved from: https://popcenter.asu.edu/content/video-surveillance-public-places-2nd-edition.

Santoshini, S. (2022, October 11). Indian Police Use Facial Recognition to Persecute Muslims and Other Marginalized Communities. *Codastory*. Retrieved from: https://www.codastory.com/authoritarian-tech/india-police-facial-recognition/.

Ulmer, A. & Siddiqui Z. (2020, February 17). India's use of facial recognition tech during protests causes stir. *Reuters*. Retrieved from:https://www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ. Accessed 19th October 2022.

Chapter 6:

Spying Through Your Pockets

Key findings

- Nearly one out of three government employees believe that the government can access information on people's phones without their consent or knowledge.
- Two out of five people are concerned about hackers accessing information on their phone without their consent or knowledge.
- One out of five people believe that it is right for the government to monitor people's social media posts.
- One out of three people oppose government surveillance of individuals' online and mobile activities.
- Majority of respondents feel government surveillance by CCTVs, drones, FRT, etc. to suppress protests and political movements is justified. Respondents from Punjab are least likely to support government surveillance during protests, while those from Gujarat most likely to support it.
- Nearly two out of three respondents are scared to post their political or social opinions online for fear of legal action.
- Two out of three people have not heard of the Pegasus spyware issue. More than a quarter of the respondents feel that surveillance of MPs/MLAs and other politicians using Pegasus spyware is completely justified.
- About two out of three respondents are concerned that data collected by private entities can be misused.
- Nearly one out of two people receives targeted ads based on online search history frequently.

CHAPTER 6

Spying Through Your Pockets

Today's surveillance technology has risen to a level where one rarely needs spy glasses, human detectives, or even the physical presence of a spy to keep tabs on anyone. A phone is enough to do the job effectively, even without the owner's consent or knowledge. Phone surveillance can be as simple as a parent keeping an eye on their child's activity log, or partners snooping on each other, to as complex as private companies maintaining a database of information to track and profile consumers according to their interests and relative worth. Similarly, government agencies and policing systems use predictive technology, social sorting tools, and other methods of advanced surveillance to classify people according to their likelihood of committing a crime, participating in protest movements or activities disagreeable with the government, or more simply, keeping dissent in check. But increasing demand for newer and more intrusive forms of surveillance have also given rise to a greater focus on human privacy.

This chapter discusses citizens' perceptions and experiences with government and private surveillance in light of notions of and right to privacy. The chapter is divided into the following three sections:

- **Section 1** presents the general perception of people regarding the right to and violation of privacy.
- **Section 2** focuses on government surveillance, analysing the challenges people face while expressing their opinions on a digital platform. It also reports public perceptions about the government keeping an eye on the general public and controlling the opposition using digital surveillance technology.
- **Section 3** comprehensively details surveillance by private entities. The profiling of consumers using their personal and sensitive data is becoming a common marketing technique. On that note, it evaluates specifically tailored advertisements and messages based on consumer activities.

6.1. Concerns about the intrusion of privacy

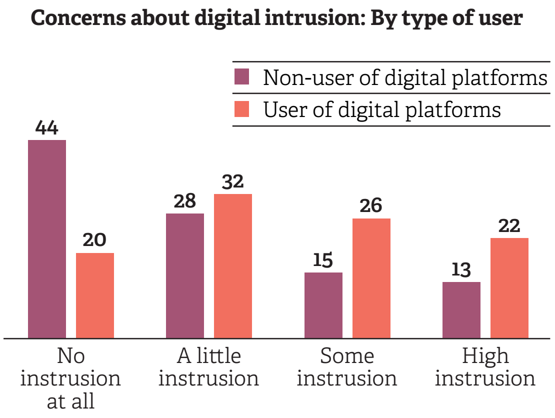
While digitisation has many advantages, there is a need to address the threats it can pose to human privacy, whether by the state or private agencies. In 1928, Louis Brandeis warned that "the progress of science in furnishing the government with the means of espionage is not likely to stop with wiretapping" (Lyon, 1994). This seems to be true in the present scenario. Earlier surveillance technologies were designed to keep an eye on specific individuals, such as politicians, likely dissenters, or the rich. However, with the introduction of mass surveillance technology and artificial intelligence-based categorisations of information, the scope of surveillance has widened manifold. Now, any and every person can come under the ambit of surveillance by both state and private agencies. It is natural that in such a context, people's concerns and anxieties would also rise with regard to their privacy and digital intrusion.

In the study, when people were asked to share their opinion on non-consensual surveillance, close to three out of four responded affirmatively to this being a possibility (74%), agreeing that personal data on phones can be subject to digital surveillance by various entities. An index was created on 'People's perception of digital intrusion through phone' to assess the overall levels of concerns regarding mobile surveillance by various agencies (See Index 2 in Appendix 5).

A significant section of the respondents was anxious about non-consensual mobile surveillance by various agencies – one in five (20%) was highly concerned and a little less than a quarter (23%) were somewhat concerned. Analysing the level of educational attainment among respondents reveals an inverse relationship with people's perception of digital intrusion. Among those who are non-literate, nearly half (46%) are of the opinion that there is no intrusion at all. Among those who are educated till college and higher levels, this percentage is nearly halved, with just 22 percent believing that there is no intrusion at all (Table 6.1).

There is also a visible division in the opinions of the users of digital platforms[4] (such as social media, internet, emails) as well as non-users, with more than four of every ten (44%) non-users of digital platforms reporting that there is no intrusion at all and only 13 percent claiming there is high intrusion. This equation reverses for the users of digital platforms. In sharp contrast, a much lower number of the users of digital platforms (20%) believed that there was no intrusion while a higher percentage (22%) agreed that there was high intrusion (Figure 6.1).

Figure 6.1: People who use digital platforms more likely to be concerned about digital intrusion



Note: All figures are in percentages.

Table 6.1. Concerns about digital intrusion through phones increase with an increase in the level of education

Level of education	People's perception on digital intrusion through phone			
	No intrusion at all	A little Intrusion	Some Intrusion	High Intrusion
All	**26**	**31**	**23**	**20**
Non-Literate	46	25	14	15
Upto Primary	39	31	16	14
Upto Matric	26	34	23	17
Intermediate-under graduate	24	31	25	20
College and above	22	31	26	21

Note: All figures are in percentages. Details about the index are mentioned in Appendix 5 – Index 2.

[4] An index 'Users of digital platforms' was created and details about the index are mentioned in Appendix 5 – Index 1.

In the following sub-sections, people's opinions and concerns about non-consensual mobile surveillance by various state and non-state agencies are discussed in detail.

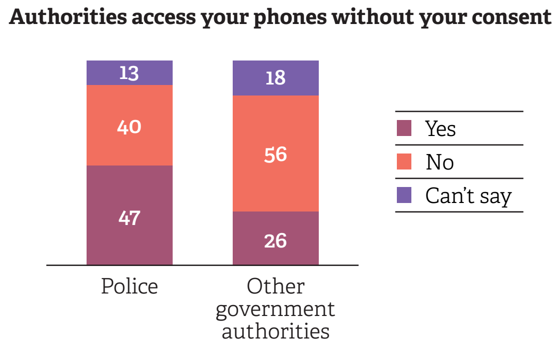
6.1.1. State surveillance: Police & government

Some level of state surveillance is considered vital for public safety and national security. This makes it important to strike a careful balance between citizens' privacy and state's legitimate concerns around safety and security. However, a problem arises when the language of the law concerning such surveillance and data protection is so ambiguous that it leaves significant scope for misuse and misinterpretation, thus broadening the surveillance powers of state agencies to unjustifiable levels. Intrusion of privacy poses an immediate threat to human dignity, that further highlights the need for proportionality and legality vis-à-vis the legitimate concerns of the state.

To better understand people's opinions about the legality of state surveillance, respondents were asked about the extent to which they believed that police or the government can, without their knowledge or consent, access personal data on their mobile phones.

Close to half (47%) of the respondents believe that the police can access their phone without their consent. On the contrary, close to one in four respondents believed that other government authorities can view the content on their phones without their consent or knowledge (Figure 6.2).

Figure 6.2: Nearly one out of two people believe that police can access information on people's phones without their consent or knowledge



Note: All figures are in percentages.
Question asked: Can the following authorities access your phones without your consent?" a. Police & b. Other government authorities

Notably, across occupations, government employees were most likely to believe that personal information on phones can be accessed by authorities without their knowledge or consent. This was followed by professionals, who were most likely to believe so. Close to three in ten respondents from those fields were suspicious about the government authorities spying on their phones (Table 6.2).

Table 6.2: Nearly one out of three government employees believe that the government can access information on people's phones without their consent or knowledge

Occupation	Government authorities can access phone with consent
Government Employees	32
Professionals	30
Students	28
Business	25
Labourer	21
Farmers	21
Housewife/ stay at home	21
Other occupations	26

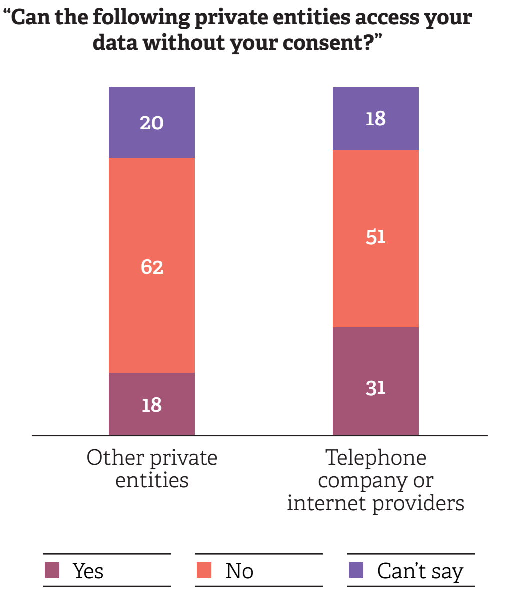
Note: All figures are in percentages.
Question asked: Can the following authorities access your phones without your consent?" a. Police & b. Other government authorities

6.1.2. Non-state surveillance: Private companies

Private companies often use searchable databases to process personal data for various commercial purposes. It creates a richer source of information for them about people's behaviour and choices. This is considered to be a great resource and even a catalyst for current marketing practices.

Survey findings show that overall, close to one in five (18%) respondents believed that their data could be viewed without their consent by private companies/advertisers. On the other hand, one in three (31%) respondents believed that the personal information on their phones could be viewed by telephone companies or internet providers without their consent or knowledge (Figure 6.3).

Figure 6.3: Nearly one out of three people believe that telecom companies and internet service providers can access people's data without their consent or knowledge



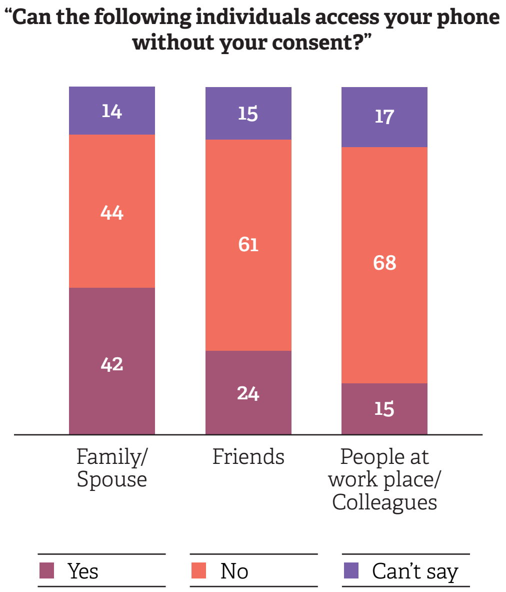
Note: All figures are in percentages.
Question asked: Can the following authorities access your phones without your consent? Telephone companies or internet providers; & Other private companies.

6.1.3. Social surveillance: Family, friends & colleague

Smartphones have made snooping on a family member or partner easier and more intrusive than ever. Such sentiments were also reflected in the survey findings, with 42 percent respondents expressing their concern that their family member might view personal content in their phones without their consent or knowledge. Further, one out of four people believed that their friends could view personal data on their phones without their consent or knowledge, although a significant proportion (61%) believed their friends could not do so.

In the drive towards increasing productivity and competition, workplace surveillance is emerging as a contentious issue. However, the survey findings suggest that people are not very concerned about their colleagues or employers accessing their personal information on the phone, with more than two out of three (68%) denying its possibility (Figure 6.4).

Figure 6.4: Forty-two percent people believe that family/spouse can access information on their phone without their consent or knowledge

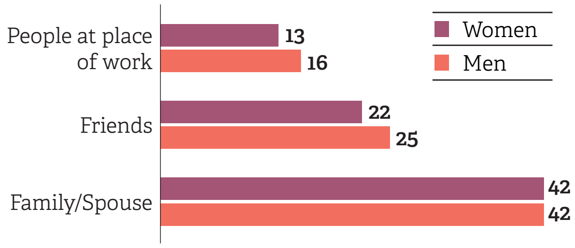


Note: All figures are in percentages.
Question asked: Can the following authorities access your phones without your consent?" – Family/spouse; Friends; People in offices or places of work

Examining the responses based on the gender of the respondents, men were more likely to believe that their phone data could be accessed without their consent by their colleagues as well as by their friends than women. On the other hand, both men and women were equally likely to believe that their family members/ spouses could snoop on their phone data (Figure 6.5).

Figure 6.5: Men more likely to believe their phones are being accessed non-consensually at work or by friend

“Can the following individuals access your phone without your consent?”



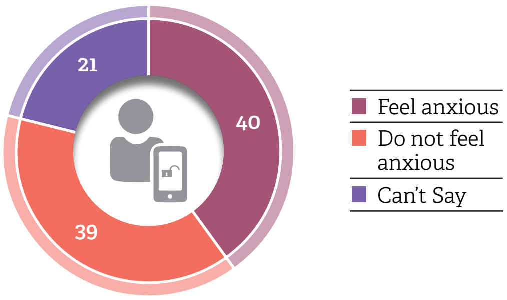
Note: All figures are in percentages.
Question asked: Can the following authorities access your phones without your consent?” – Family/spouse; Friends; People in offices or place of work.

6.1.4. Unauthorised surveillance/hacking

By 2023, about six of every ten (64%) of the Indian population (907.4 million) will have access to the internet, according to a Cisco report (Cisco Annual Internet Report, 2022). With the rising number of internet users in the country, there has also been a steep increase in cyber crimes. Over 18 million cases of cyber-attacks and threats were recorded within the first three months of 2022 in India, with an average of nearly 2,00,000 threats every day, according to the cyber security firm Norton (Bordoloi, 2022). With a rapid increase in cyber crime cases in India, the levels of anxiety against such unauthorised surveillance would also likely go up.

Figure 6.6: Two out of five people are concerned about hackers accessing information on their phone without their consent or knowledge

Concerns about hackers accessing information on the phone



Note: All figures are in percentages.
Question asked: Can the following authorities access your phones without your consent?”Hackers?

When the general public was asked whether they think that hackers can view photos, messages, videos, or search history from their devices without their consent or not, two out of five people (40%) responded in the affirmative (Figure 6.6).

6.2. People’s perceptions of government surveillance

In this section, the study assesses the general public’s levels of comfort in sharing their opinions about a political or social issue on a digital platform. In addition, the study tries to analyse the general consensus with regard to government activity in the name of national interest– balancing the extent of intrusion with the protection of citizens’ privacy. Finally, it will briefly discuss awareness and opinions about the Pegasus scandal, one of the most alarming instances of government surveillance that emerged in the recent past.

6.2.1. Monitoring and restriction

The survey enquired into people’s opinions on the government surveilling their digital activities, such as what they post on social media or the internet, call history, location tracking, tracking what they downloaded or read online, or collecting their socio-economic information. People were most likely to support total government surveillance for monitoring social media or online posts, with 21 percent saying that it is always right and another 30 percent saying that it is right in some cases. On the other hand, more than one out of two people felt that it was wrong for the government to track people’s online activities, profile individuals based on their online activities and access people’s call histories. Twenty-eight percent of people felt that it was right in some cases for the government to impose restrictions on the content posted on social media and track people’s locations, but even in these categories more than 45 percent were of the opinion that it is wrong (Table 6.3).

Table: 6.3: One out of five people believe that it is right for the government to monitor people's social media posts

	Government's action is....?			
	Right	Right, but in some cases	Wrong	Can't say
Monitoring what is posted on social media or the internet	21	30	36	13
Tracking online/phone activities and accessing contents	12	24	50	14
Imposing restriction on social media contents	12	28	45	15
Location tracking	12	28	47	13
Creating social and financial profile by collecting information from different sources	11	20	52	17
Tracking call histories	10	24	56	10

Note: All figures in percentages.
Question asked: Do you think it would be right or wrong for the government to do these things? List of questions are mentioned in the first column of this table.

For a nuanced understanding of the responses, an index on the level of support for government surveillance of people's digital activities was created using all the listed items in Table 6.3 (see index 3 in Appendix 5 for details). A little over one in six (17%) of the respondents strongly supported the idea of the government surveilling individuals' online activities, while one in three people (34%) did not support such surveillance. A greater proportion (41%) showed conditional support (in some cases) for the government's surveillance of people's online activities.

Across states, Punjab was the least supportive of such surveillance by the government – close to three out of five (57%) were against it. Other than Punjab, low levels of support were observed in Delhi, Kerala, and Haryana; whereas, in contrast, Karnataka and Tamil Nadu reported higher levels of support for such surveillance (Table 6.4).

Table: 6.4: One out of three people oppose government surveillance of individuals' online and mobile activities, Punjab most likely to oppose

	Support for targeted digital surveillance by the government			
	Least support	Somewhat support	Strong support	No opinion
All	**34**	**41**	**17**	**8**
Punjab	57	27	7	9
NCT Of Delhi	51	33	10	6
Kerala	46	44	7	3
Haryana	40	40	16	4
Andhra Pradesh	33	38	22	7
West Bengal	33	41	13	13

Uttar Pradesh	30	43	17	10
Maharashtra	30	40	23	7
Tamil Nadu	28	41	28	3
Gujarat	23	51	20	6
Assam	21	45	10	24
Karnataka	14	49	35	2

Note: All figures are in percentages. Details about the index is mentioned in Index 3 in Appendix 5.

6.2.2. Support for mass surveillance

When people were asked about the use of mass surveillance technology by the government for suppressing protests and political movements, a significant proportion (45%) of the respondents strongly supported the idea of such mass surveillance[5]. On the other hand, one in five were opposed to this.

On being asked about the level of support for the use of technologies such as CCTVs, facial recognition, mobile surveillance, etc. to curb protests and movements, the people reported the highest levels of support for the use of CCTV cameras, with one out of two respondents strongly supporting its use. A little over a quarter strongly supported the use of mobile surveillance such as phone tapping or hacking, facial recognition and voice recognition technology to curb protests, while three in 10 strongly supported the use of drones by the government (Table 6.5).

Across states, those from Gujarat and UP were most likely to fully support government surveillance for curbing protests, political movements, etc. (Table 6.6). On the other hand, Punjab, which witnessed large-scale protests against new farm laws in 2021, was least likely to support the use of such mass surveillance technologies by the government to curb protests and political movements. Tamil Nadu, where dominant Dravidian politics has traditionally been adversarial to that of the Centre, also showed a lower level of support for mass surveillance.

Table 6.5: Majority of respondents feel government surveillance by CCTVs, drones, FRT, etc. to suppress protests and political movements is justified

Use of mass surveillance technology by the government to curb protests and political movements					
	To a great extent	To some extent	Very little	Not at all	Can't say
CCTV camera	52	25	6	7	10
Drones	30	29	13	12	16
Mobile Surveillance	27	30	15	14	14
FRT	25	26	14	13	22
Voice recognition technique	24	26	16	15	19

Note: All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use the following technologies to curb political movement or protests against policies & laws enforced by the government – to a great extent, to some extent, very little or not at all?

[5] See Index 4 "Support for mass surveillance by the government to curb protests and political movements through various technologies" in Appendix 5.

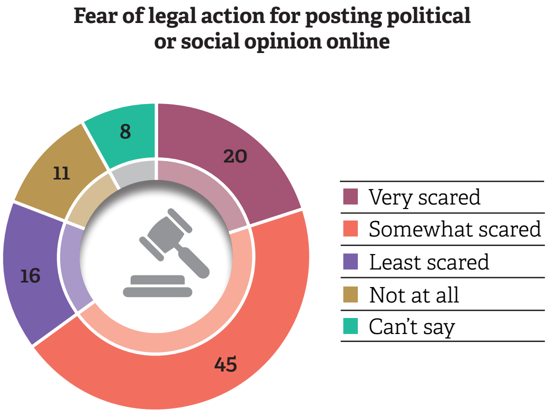
Table 6.6: Punjab least likely to support government surveillance during protests, Gujarat most likely to support it

States	Full support to mass surveillance by government to curb protests
Gujarat	52
Uttar Pradesh	47
Haryana	36
Andhra Pradesh	31
Maharashtra	30
NCT Of Delhi	27
Assam	24
West Bengal	18
Kerala	16
Karnataka	15
Tamil Nadu	13
Punjab	13

Note: All figures are in percentages. Only the full support option was analysed from the index. Details about the index are mentioned in Index 4 in Appendix 5.

According to statistics from the US-based think tank Freedom House, India ranked 51 out of 100 in terms of availability of internet freedom in its Freedom on the Net report 2022 (Shahbaz, 2022). The lack of such freedom is apparent in the survey findings about people's ability to express their opinions online. Even as the respondents supported the government's surveillance of mobile phones to curb political protests, they were simultaneously apprehensive over their ability to post their social or political opinions online freely, for fear of legal action. When respondents were asked whether they feel scared of legal action against them if any of their posts or opinions about a political or social issue on social media hurts the sentiments of certain groups, 65 percent of respondents said they were scared to varying extents (Figure 6.7).

Figure 6.7: Nearly two out of three respondents scared to post their political or social opinions online for fear of legal action



Note: All figures are in percentages.
Question asked: How scared do you feel that if you post your opinions about a political or social issue on social media,and if it hurts the sentiments of certain groups, there might be legal action against you – very scared, somewhat scared, least scared or not at all scared?

When seen across states, those in Haryana (41%), Gujarat (33%), and Delhi (32%) were very scared of provoking legal action by expressing their political opinions online whereas in Karnataka, Maharashtra and Kerala not many people exhibit their fear of legal action for posting political or social opinion. Nearly a quarter of the citizens in Kerala (23%) said they were not scared at all (Table 6.7).

Table 6.7: Those in Haryana, Gujarat, and Delhi, most scared of sharing their opinions online

	Fear of legal action for posting political or social opinion online			
	Very scared	Somewhat scared	Least scared	Not at all
Haryana	41	35	7	11
Gujarat	33	46	9	8
NCT Of Delhi	32	39	11	13
West Bengal	25	43	14	9
Tamil Nadu	19	56	14	5
Uttar Pradesh	18	43	20	9
Andhra Pradesh	18	46	12	10
Punjab	13	46	20	12
Assam	12	55	12	12
Kerala	11	32	20	23
Maharashtra	10	49	14	14
Karnataka	4	52	36	5

Note: All figures are in percentages. Rest did not respond.
Question asked: How scared do you feel that if you post your opinions about a political or social issue on social media,and if it hurts the sentiments of certain groups, there might be legal action against you – very scared, somewhat scared,least scared or not at all scared?

Individual vs. mass surveillance

An interesting pattern emerges when one looks at people's support for government surveillance, based on the type of surveillance technology. It was found that people were less likely to support targeted surveillance of people's individual activities and monitoring of online activities, such as what they post on social media or the internet, with whom they talk on the phone, location tracking, etc. However, when it comes to mass surveillance technologies, they overwhelmingly supported the government (Table 6.8).

6.2.3. Pegasus: Awareness and opinions

In July 2021, the International Consortium of Investigative Journalism (Pegasus project) revealed that about 50,000 phone numbers and linked devices across the globe were infected by the Pegasus spyware. The investigation reported that targets were concentrated in countries where unlawful surveillance and

Table 6.8: People are much more likely to support mass digital surveillance by the government than targeted digital surveillance

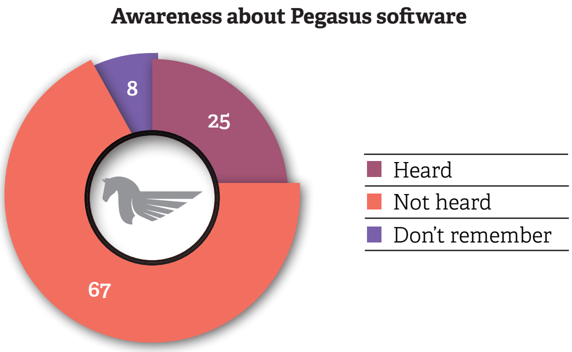
	Support for targeted digital surveillance of individuals by the government	Support for digital mass surveillance by the government
Least support	34	18
Somewhat support	41	30
Strong support	17	45
No opinion	8	7

Note: All figures are in percentages. Details about the Index 3 for Support for targeted digital surveillance of individuals by the government and Index 4 for Support for digital mass surveillance by the government in Appendix 5.

poor legislative protections were prevalent. Within the target list, around 300 phone numbers that were surveilled belonged to serving ministers, journalists, opposition leaders and judges, business persons, and activists from India (Shekar & Mehta, 2022). It was alleged that the governments of various countries, including India, purchased the spyware from an Israeli company, the NSO Group, as part of their defence deals.

In this context, people were asked if they had ever heard of the Pegasus spyware. Two out of three people (67%) responded in the negative, while just a quarter of the respondents (25%) said that they had heard of Pegasus spyware (Figure 6.8).

Figure 6.8: Two out of three people have not heard of the Pegasus spyware issue



Note: All figures are in percentages.
Question asked: Have you heard of the Pegasus software which was used by governments of various countries, including India,to listen to the calls and read the messages of some people, including politicians, journalists and judges?

To further probe people's opinions on the issue, the respondents were asked whether the government should use such spyware on different categories of people. Out of all categories of people listed in the table below, respondents were most likely to strongly support such targeted surveillance of suspected criminals (43%). On the other hand, a little over a quarter (27%) said that it should be used against politicians. Troublingly, about 20 percent were also strongly supportive of the targeted surveillance of bureaucrats, journalists, and lawyers. On the other hand, 51 percent of the respondents strongly opposed the targeted surveillance of ordinary citizens. (Table 6.9).

Table 6.9: More than a quarter of the respondents feel that surveillance of MPs/MLAs and other politicians using Pegasus is completely justified

Support for targeted surveillance of the following groups using spywares such as Pegasus				
People	Fully support	Support in some cases	Oppose	Don't know
Suspected Criminal	43	21	15	21
MP/MLA	27	24	26	23
Other Politician	27	25	25	23
Bureaucrat	20	24	32	24
Journalist	19	22	35	24
Lawyer	18	23	36	23
Judge	16	24	37	23
NGO	16	24	35	25
Businessmen	15	24	36	25
Ordinary citizen	9	17	51	23

Note: All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use the following technologies to curb political movement or protests against policies & laws enforced by the government – to a great extent, to some extent, very little or not at all?

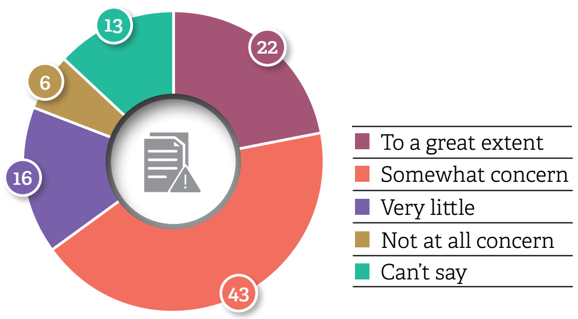
6.3. People's perception of surveillance by private entities

The rise of digitisation has led to an increase in technology access and usage. Digital inclusion, it is argued by many, would bring economic advancement and is sustainable for the ever-increasing population. Simultaneously, however, there is also an increasing focus on 'dataveillance' (surveillance by databases). A sustained and systematic analysis of consumers' perceptions not only helps in improving services but verifies identities, assesses the relative worth of the consumers and classifies individuals according to their value to the markets. Such unchecked surveillance by private companies can pose a major threat to people's right to privacy.

Data transparency thus becomes an important concern, and it contributes significantly to consumer trust. When we asked people to share their opinions about the level of trust they have with regard to data collection by private entities, close to two-thirds (65%) felt that such data can be misused (Figure 6.9). Responses indicated that people feel anxious while sharing their data with private entities.

Figure 6.9: About two out of three respondents concerned that data collected by private entities can be misused

Degree of fear of misuse of data by private entities



Note: All figures are in percentages.
Question asked: Private companies, in general, collect data in the name of improving their services to deliver products that are more relevant to the consumers. How concerned do you feel that this information can be misused - to a great extent, somewhat, very little or not at all?

6.3.1. Perception of targeted advertisements

Codes, usually processed by computers, are known to sort out interactions, perceptions, and attitudes. They are invisible doors that permit access to participation in a multitude of events, experiences, and processes (Lyon, 2003). Advertisements shown according to the general activity and worth of an individual are a reflection of the increasing use of databases. Inevitably, surveillance by private entities is a serious threat to one's privacy.

However, according to the survey findings, the general public is not very concerned about the potential breach of privacy and view targeted advertisements positively. Overall, 59 percent felt that targeted advertisements based on such data surveillance by private companies were helpful.

Comparing perceptions across types of cities, nearly one out of three people residing in capital cities found such advertisements shown according to their interests most helpful (32%). One in every three people who have attained graduation and above degrees found advertisements shown based on their interests very helpful. On the other hand, two out of three non-literate people (62%) did not respond to this issue. This could be due to the lesser usage of smartphones and social media amongst these groups. Further, one in every three respondents from the 18-25 age group found advertisements based on their interests very helpful,while among the older cohorts (56 years and above), just 16 percent found them to be very helpful (Table 6.10). As in the case of educational levels, this variation could be because of lower access to smartphones and internet usage amongst the elder respondents.

Table 6.10: Young, highly educated and those in capital cities are most likely to have a positive perception of targeted advertisements based on data surveillance

	Opinions regarding targeted ads				
Category	**Very helpful**	**Somewhat helpful**	**Not very helpful**	**Not at all helpful**	**Can't say**
Overall	**28**	**31**	**12**	**12**	**17**
Capital cities	32	31	9	12	16
Medium cities	25	31	13	14	17
Small cities	26	32	14	9	19
Non-literate	11	14	5	8	62
Upto Primary	18	21	7	10	44
Upto Matric	25	29	9	11	26
Intermediate/ under graduate	28	36	12	12	12
Colleges and above	33	35	14	13	5
18 to 25 years old	33	35	13	10	9
26 to 35 years old	31	34	13	12	10
36 to 45 years old	28	33	12	11	16
46 to 55 years old	25	28	11	12	24
56 years and above	16	19	9	16	40

Note: All figures are in percentages.
Question asked: According to you, how helpful are the data collected by private companies from customers like you for these things– very helpful, somewhat helpful, not very helpful or not at all helpful? - Ads are shown to you according to your interests

Based on what people search online

The rise of the internet and the World Wide Web has opened a myriad of opportunities and provided a significant platform for advertisers to target billions of people instantly, and almost effortlessly. With the increasing sophistication of ad personalisation, advertisers can easily direct material to the right user at the right time. It is important to note that the personalisation of advertisements has been very profitable for private entities. Advertisements received based on what one searches online depend on a number of factors, such as the page they are visiting, their browsing history, their IP address, operating system, the plug-ins installed and other information related to their web browser.

When people were asked how frequently they receive targeted advertisements or messages based on what they searched online, more than 46 percent reported receiving such messages frequently (Table 6.11). The frequency of receiving such targeted advertisements is higher amongst the younger and more educated respondents.

Based on likes on social media

Social media advertising is a medium to serve users on digital media platforms. Searchable databases reflecting what we like, comment on, and share online, are categorised through our cookie settings, search history, and the frequency of page views etc., which show products according to our individualised interests, likes and dislikes. Also, a quarter of social media users say they tend to buy brands they see advertised on such platforms (Gorman, 2022), thus pointing to the profitability of such targeted ads.

Table 6.11: Nearly one out of two people receives targeted ads based on online search history frequently

Frequency of receiving advertisements or targeted messages based on these activities	Frequently	Sometimes	Never	No response
What people search online	46	26	10	18
Likes on social media	36	31	13	20
Conversations on phone	15	22	43	20
Conversations on messaging apps such as WhatsApp, Facebook messenger, etc.	18	26	35	21
Face-to-face conversations with someone	12	19	47	22

Note: All figures are in percentages.
Question asked: How frequently do you receive advertisements or targeted messages based on these activities – Frequently, sometimes or never?

According to the survey findings, a little over two-thirds (67%) of the respondents reported receiving targeted messages and advertisements based on what they liked on social media. Of these, more than one-third (36%) received frequent ads and three of every ten (31%) received them occasionally.

Based on phone conversations

Phones have in-built microphones through which they can hear conversations. Claims suggest that marketers have repeatedly been accused of listening in on phone conversations in order to personalise our online advertising experiences. A recent survey conducted by social media platform LocalCircles found that one in two Indian citizens get advertisements based on their conversations on private phone calls, microphone access, and contact list access (LocalCircles, 2022). Users are put at adverse risk due to a lack of awareness regarding the organised leakage of personal data, whether through first-party and third-party tracking apps or microphone surveillance.

The survey found that overall, more than two out of every five (43%) respondents stated that they had never received targeted advertising or messages based on phone conversations. Close to one in six (15%) reported frequently receiving such advertisements based on phone conversations and close to one in five (22%) said they sometimes received messages or advertisements based on phone conversations.

Based on conversations on messaging applications - WhatsApp and Facebook Messenger

Around 84 percent of smartphone users in India have granted contact list access to WhatsApp; 51 percent have granted access to Facebook, Instagram, or both; and 41 percent have granted access to apps like TrueCaller (LocalCircles, 2022). A majority of Indians have enabled microphone access on their mobile phones for audio/video calls, social media networking, and audio-video recording apps. While this simplifies the device's operation, it severely limits customers' right to privacy and subsequently their freedom of expression/choice.

When people were asked whether they receive targeted adverts and messages based on their conversations on social media platforms, more than two-fifths (44%) responded affirmatively. Of these, more than one-fourth (26%) respondents received targeted advertisements sometimes while 18 percent reported frequently receiving such advertisements (Table 6.11). On the other end of the spectrum, more than one-third of respondents reported never receiving targeted ads based on messaging app interactions.

Based on face-to-face conversations with someone

The introduction of virtual assistant technologies like Alexa and Siri has instilled anxiety in people concerning surveillance over face-to-face conversations, even if they are in their personal space or a closed room. The moment you utter 'Ok Google' or 'Hi Alexa' these devices start recording whatever you say. This suggests that even while they pay attention to everything you say during the day, their response mechanism only engages when you call them out.

According to the survey findings, while nearly a majority (47%) of the general public believed that they never got targeted messages based on face-to-face conversations, a significant proportion believed otherwise. Nearly one-third of respondents, or 31 percent, reported receiving targeted advertisements and messages based on face-to-face conversations they had around these devices either frequently or sometimes.

6.3.2. Opinion on digital transactions and financial data

Saving credit and debit card details for speedy payment has become the new normal. Nowadays, people often save their card details on shopping sites and web pages to save time, though it imposes a significant risk of the credentials being leaked if that company is breached or if the account is hijacked. According to Cisco Data Transparency Report, 43 percent say that they do not feel they can adequately protect their transactional data online. Of those that responded this way, the vast majority (76%) say that they are unhappy with company data transparency policies and practices; they simply don't know what is being done with their data behind the scenes (Ikeda, 2022).

In this survey, when respondents were asked whether they think that it is helpful that one need not enter card/ payment details every time while doing online shopping, more than half (51%) of them responded affirmatively. Of those, a little less than 20 percent felt that it was very helpful, while close to one out of three (32%) found this facility to be somewhat helpful. It is notably higher in the younger generation, with nearly a quarter of the respondents in the 18-25 age group (23%) of the opinion that it is very helpful. Among the older cohorts, however, more than two-fifths of respondents (43%) did not express any opinion, and just 12 percent said that it was very helpful (Table 6.12).

6.3.3. Calls and messages regarding products and services one might be interested in

During the course of the day, one often receives spam calls and messages from unknown numbers regarding products and services. While this in itself may not be a big cause for worry, what can be inferred from it is the fact that often personal data such as mobile

Table 6.12: Older respondents more worried about sharing financial/card details for online purchases

Age groups	Shared data is helpful for making online purchase without entering card/payment details				
	Very	Somewhat	Not very	Not at all	Can't say
All	**19**	**32**	**15**	**14**	**20**
18 to 25 years old	23	37	16	12	12
26 to 35 years old	21	36	15	14	14
36 to 45 years old	18	32	17	13	20
46 to 55 years old	17	28	14	14	27
56 years and above	12	19	11	16	42

Note: All figures are in percentages.
Question asked: According to you, how helpful are the data collected by private companies from customers like you that you don't have to enter your card/ payment details every time when you make a purchase – very helpful, somewhat helpful, not very helpful or not at all helpful?

numbers, linked to a person's identity details (name, location, etc.), is being leaked to third parties without the consumers' knowledge or consent. This has great potential for further misuse and breach of privacy.

However, the survey found that people were more or less neutral about such targeted advertisements, with a slightly higher percentage claiming that these are in fact helpful. Nineteen percent said that it was very helpful and another 30 percent felt that it was somewhat helpful. In contrast, 32 percent opined that it was not helpful (Figure 6.10).

6.3.4. News or other information as per one's interest

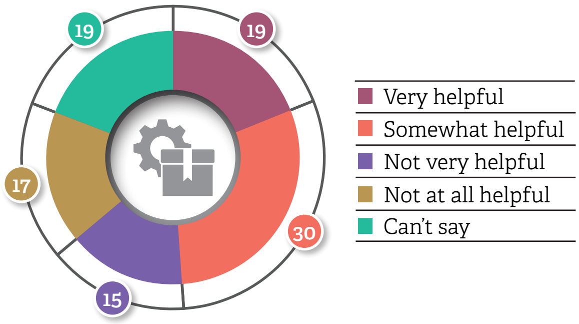
Private companies maintain large databases of their clients to serve them and attract their interest in every way possible. With personalisation and tailored news recommendations, customers feel better equipped and comfortable with the respective webpage or digital platform. It increases activity status and interaction with that specific platform, garnering immense profit for the entity. As a result, news suggestions based on personal interests are more valuable for social media marketers and private corporations than for one's comfort.

Other than a marketing tool, selective dissemination of news and information can also have much more significant political and social impact in a country. In what is often termed a "post-truth era", public sentiments and opinions tend to blur the "factual" documentation of any issue or event and there is disputed claim over such public truths (Hyvonen, 2018). This results in larger distrust of mainstream media and information portals, with people likely to disbelieve any information that doesn't fit into their specific worldview.

In such an age, targeted news and information can indeed spur polarisation by constantly feeding contradictory information to various groups of people, based on their social and political leanings, and leaving a limited platform for shared knowledge. This can have huge impacts on the political and social trajectories of nations.

Figure 6.10: Nearly half of the respondents believe that shared data is helpful for receiving calls and messages regarding interesting products and services

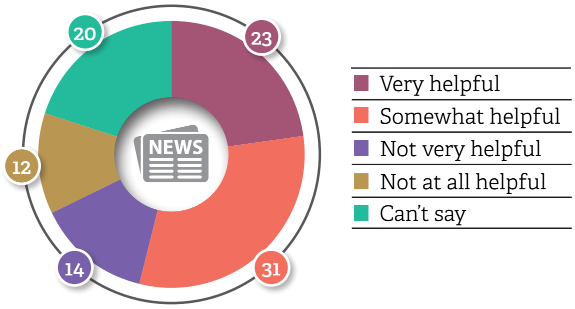
Shared data is helpful for receiving calls and messages regarding products and services you might be interested in



Note: All figures are in percentages.
Question asked: According to you, how helpful are the data collected by private companies from customers like you for these things – very helpful, somewhat helpful, not very helpful or not at all helpful? – You get calls and messages regarding products and services you might be interested in

Figure 6.11: One out of four people feel that sharing data with private companies to get targeted news is very helpful

Data collected by private companies used to provide targeted news or other information as per interest



Note: All figures are in percentages.
Question asked: According to you, how helpful are the data collected by private companies from customers like you that you get news or other information as per interest – very helpful, somewhat helpful, not very helpful or not at all helpful?

However, amongst the larger public, there is in fact great support for such targeted news and information, as found in the survey. Close to 55 percent of the respondents said that the data collected by the private companies was helpful in getting news and information as per their interest, thus lending their support to such targeted dissemination of news (Figure 6.11). Only 12 percent were of the opinion that it is not at all helpful.

Conclusion

Findings from the survey suggest that the larger public, to a great extent, is not very concerned about either mass surveillance by the government or surveillance by private companies. In general, people do not tend to view the issue of digital surveillance, undertaken in different forms, through a critical lens. Just as social media has become as common a daily activity like commuting to work or doing domestic chores, surveillance is also being accepted as part of daily life. Hardly any day passes without the media highlighting the use of CCTV cameras in the context of solving crimes or making our cities 'smarter'. The findings of this chapter also show that people have also accepted surveillance by advertisers and private companies as a way of life. In fact, the use of social media by common people and their dependence on mobile and Wi-Fi networks, coupled with the omnipresence of CCTV cameras and smartphones, may have normalised surveillance as an everyday activity.

However, when it comes to targeted surveillance of individuals' online and phone-based activities, there is a certain level of anxiety regarding the safety of their personal data. While there is a high level of support for mass government surveillance, a significant proportion opposed targeted surveillance of individuals by the government based on their online activities. People expressed strong dissent against tracking phone activity, location-tracking and creating a social/financial profile database of citizens.

However, troublingly, people expressed their support for mass surveillance by the government for curbing political movements or protests, thus devaluing the right to freedom of expression and freedom of dissent. The concerns for right to privacy are much more pronounced when it comes to personal and financial data, but when it comes to the questions of mass surveillance or even targeted surveillance against specific groups, very little critical opinion emerged. The chapter discusses the low levels of awareness among the general public about the Pegasus issue that was brought to light in 2021, as well as the public's support for such non-consensual surveillance by the government, even if it used against bureaucrats and journalists. All of these findings, put together, suggest little concern amongst the larger public for democratic values such as freedom of expression and the right to privacy.

The findings also suggest that the level of trust with regard to data collection by private entities is very low. The majority of people feel very anxious while sharing their data, fearing privacy breaches and misuse. However, with regard to receiving targeted advertisements on the basis of their online activity, there was a relatively positive response, thus indicating that people tend to see these as tailored services catering to their specific needs, rather than as a breach of privacy.

References

Bordoloi, P. (2022, September 24). Does India Need a Cybersecurity Ministry? *Analytics India Magazine.* Retrieved from: https://analyticsindiamag.com/does-india-need-a-cybersecurity-ministry/. Accessed on: October 19th, 2022.

Cisco. (2022, August 18). Cisco Annual Internet Report. Retrieved from: https://www.cisco.com/c/dam/m/en_us/solutions/executive-perspectives/vni-forecast-highlights/mobile/pdf/India_Internet_Users.pdf. Accessed on 12th December 2022.

Gorman, D. (2022, February 8). How effective are ads on social media? *GWI.* Retrieved from: https://blog.gwi.com/trends/ads-on-social-media/. Accessed on: October 12th, 2022.

Hyvonen, Ari-Elmeri. (2018, October 22). Defining Post-Truth, Structures, Agents and Styles. *E-International Relations.* Retrieved from: https://www.e-ir.info/2018/10/22/defining-post-truth-structures-agents-and-styles/

Ikeda, S. (2022, October 17). Cisco Data Transparency Report: Consumer Trust Increasingly Hinges on How Personal Data is Treated. *CPO Magazine*. Retrieved from: https://www.cpomagazine.com/data-privacy/cisco-data-transparency-report-consumer-trust-increasingly-hinges-on-how-personal-data-is-treated/. Accessed on: October 19th, 2022.

LocalCircles. (2022, May 26). 1 in 2 citizens surveyed acknowledge seeing ads based on their private voice conversations; microphone and contact list access to certain apps is leading to privacy breaches. Retrieved from: https://www.localcircles.com/a/press/page/personal-data-privacy-survey. Accessed on: October 13th, 2022.

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society.* Minneapolis: University of Minnesota Press.

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk and Discrimination.* Routledge.

Shahbaz, M., Funk, A., & Vesteinsson, K. (2022). Freedom on the Net 2022. *Freedom House.* Retrieved from: https://freedomhouse.org/country/india/freedom-net/2022.

Shekar, K., & Mehta, S. (2022, February 17). The state of surveillance in India: National security at the cost of privacy? *Observer Research Foundation.* Retrieved from: https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/. Accessed on: October 25th, 2022.

Chapter 7:

People's Perceptions of the Use of Advanced Surveillance Technologies

Key findings

- Four out of five people support linking of Aadhaar card with other services. The rich are the most supportive of linking Aadhaar with welfare schemes, while the poor are least supportive.
- One out of five people are not at all comfortable sharing their Aadhaar details with private agencies.
- About half the respondents supported the collection of biometric details of suspects, including undertrials. While Adivasis and Muslims were most critical of the police collecting biometric details of all suspects, upper caste Hindus were the most supportive.
- More than one out of two people strongly support the use of drones by the armed forces, government, and the police. There is a high level of support for use of drones by government agencies, but low support for use by private agencies.
- Across occupational categories, farmers are most likely to oppose drone usage by government agencies.
- The poor are least likely to support regular drone surveillance of the public by the police/ government.
- Nearly one out of three people strongly support drone usage by the government to curb political protests.
- More than 60 percent support the use of FRT to identify protestors, two out of five say it should be used to identify common citizens.
- Sikhs least likely to support the use of FRT by government during protests, communal riots and to identify common citizens.

CHAPTER 7

People's Perceptions of the Use of Advanced Surveillance Technologies

Surveillance technologies include any digital medium - software, devices or systems, that have the potential to gather and track an individual's communications and activities. With technology upgrading at unprecedented rates, newer audio and video surveillance methods are becoming commonplace. They analyse minute details about an individual's actions with extreme precision and accuracy. With the easy availability of many such technologies, it is increasingly being used by individuals, companies and governments to various ends.

When such surveillance technology is employed by the government, several issues of public concern emerge. At one end of the surveillance continuum lies the legitimate purpose of safeguarding national security,at the other end are concerns regarding the people's right to privacy. The relationship between them is often fraught with challenges aggravated by a lack of legislation. Added to this, newer technology like biometrics, drones and facial recognition techniques have transformed the surveillance architecture, making intrusion of privacy easier than ever before. This has the potential to damage the democratic ethos of a nation.

While the precision of such technology is improving, they are not infallible, adding another layer of concern. For instance, facial recognition technology, which is now commonly employed by various state and private entities worldwide, has been found to be inaccurate in various studies. While most FRT technologies today claim 90 percent accuracy, the level of accuracy goes down significantly across races and genders (Najibi, 2020). Particularly in the context of police usage of FRT for criminal investigations, such mis-identifications can prove to be hugely detrimental to people's right to a fair trial and proper delivery of justice.

However, the moot question is – Are the citizens aware of their regular surveillance through technologies virtually invisible to them? If yes, how do they perceive it? Do they see it as necessary, inevitable or as an intrusion? We try to find out all this and more in this chapter which is divided into the following sections:

- **Section 1** focuses on the Aadhaar landscape and the right to privacy. It investigates the opinions on the Aadhaar card regime and its linkage to state and non–state-mandated services.
- **Section 2** explores people's perceptions of biometrics and its usage for criminal investigation.
- **Section 3** explores the citizen's perception of drone usage by state agencies and private entities.
- **Section 4** assesses the general public perception regarding the usage of facial recognition techniques (FRT).

7.1. Aadhaar and linkage of services

In India's Aadhaar scheme, a uniform biometric-oriented identity card was created by the government to ensure, "...efficient, transparent and targeted delivery of subsidies, benefits and services" [The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, p.1] for the citizens. Its aim was to "empower marginalised sections of society in the broader quest for good governance" (Ibid). The scheme was initiated to provide a unique identification number (UID) to every citizen.

However, the initiative has spurred concerns over privacy including those related to informed consent, dignity and the question of data security. It was argued that the Aadhaar architecture was "capable of tracing and profiling citizens" (Sethi, 2017). Moreover, UIDAI, the parent organisation of Aadhaar, has the power to cancel Aadhaar numbers. There was no redressal mechanism; hence, citizens could potentially be deprived of access to essential services. Another concern raised was that Aadhaar could be weaponised against India's constitutional ethos and its abiding morality. Within its foundation were the remnants of surveillance that can transform the intrusive state into a full-fledged surveillance state, based on data gathered from individuals (Kaur, 2018; Bakshi et al., 2018). All of these issues, along with the threat of a lapse in security that could lead to data breaches and leakages, as happened in a number of incidents in the country (Singh, 2022; Nitin, 2018; Singh, 2017), led to scepticism about the Aadhaar infrastructure amongst a section of the population.

In the digital economy, such concerns arise amidst a colossal digital footprint left behind by citizens or consumers. The state possesses a database where one's whole identity including name, gender, date of birth and residential address is collected in one place. Clustered together with digital transactions, it creates a semantic web, that allows data to be captured by intelligent machines and produce algorithms that provide a definite picture of an individual's preferences, value systems and personality traits. It further creates a behavioural prediction model tailored specifically to monitor individuals' actions and predict their next move (Zuboff, 2020).

In order to reclaim the fundamental right to privacy, Justice K. S. Puttaswamy, a retired judge of Karnataka High Court, challenged the government when it was making the Aadhaar card mandatory. He argued that it was a clear violation of privacy and since the Parliamentary Standing Committee on Finance rejected it, there was no reason why the Government of India should still go ahead with it. It was deemed a "dangerous" project. The PIL for scrapping Aadhaar was filed in 2012, and on August 24, 2017, a nine-judge bench of the Supreme Court of India, in a landmark judgement, declared the right to privacy as a fundamental right. The court held that the citizens' right to privacy was integral to freedoms guaranteed via fundamental rights under Articles 14, 19 and 21 of the Constitution and was an intrinsic aspect of dignity, autonomy, and liberty. Later, on September 26, 2018, a five-judge bench struck down many of the existing provisions of Aadhaar. The latter decision proclaimed that non-state actors cannot make it mandatory for consumers to provide their Aadhaar details for authentication purposes.

Post the 2018 Supreme Court verdict, provisions for linking of Aadhaar card with various public and private services have been relaxed. It is not mandatory for all services, but there are exceptions.

In this survey, respondents were asked whether they would support the linkage of Aadhaar with various services. The highest proportion, four out of five respondents (80%) supported Aadhaar's linkage with a bank account or PAN card and a similar level of support was observed for linking other services too, such as mobile numbers (78%), voter ID cards (77%), welfare schemes (78%) and access to health services (77%) (Table 7.1).

Table 7.1: Four out of five people support linking of Aadhaar card with other services

Linking Aadhaar with...	Support linking Aadhaar	Oppose linking Aadhaar
Bank/Pan	80	13
Mobile Number	78	15
Voter ID	77	15
Welfare scheme	78	13
Access to health services	77	13

Note: All figures are in percentages. Rest did not respond.
Question asked: Do you support or oppose the linkage of Aadhaar with the following items? (List mentioned in the left column of the table)

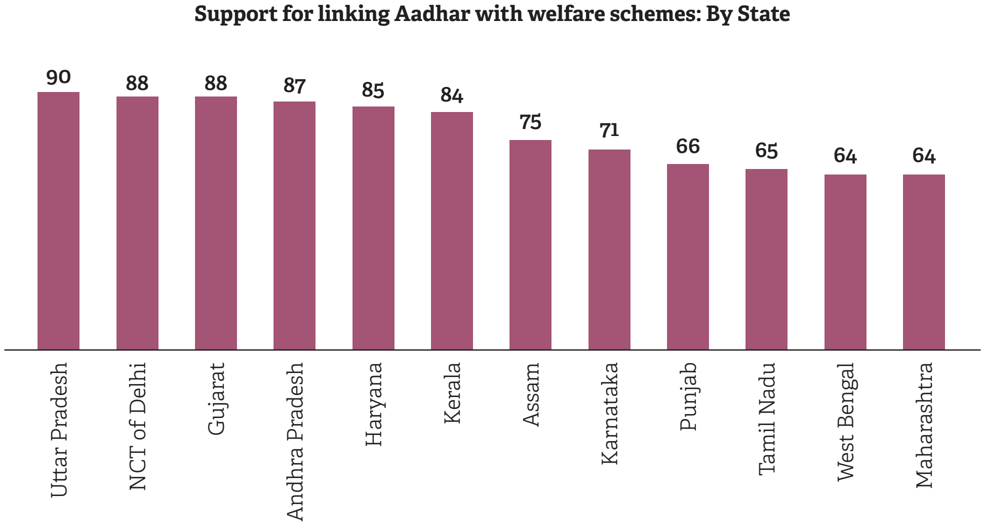
7.1.1. Welfare services like PDS or LPG

The primary function of Aadhaar, as stated, was the empowerment of the marginalised by streamlining the delivery of welfare services and subsidies in an effective and targeted way. Therefore, in the survey, we enquired about the public's opinions about the linking of Aadhaar with welfare schemes such as ration, LPG, pension schemes etc.

Nearly four out of five respondents (78%) supported its linkage with welfare schemes such as LPG, ration and the like. Across states, it was found that the support came in large measure from Uttar Pradesh (90%), NCT of Delhi (88%), and Gujarat (88%), whilst comparatively low support was observed from Tamil Nadu (65%), West Bengal (64%), and Maharashtra (64%) (Figure 7.1).

Interestingly, even though this move is aimed at easing the delivery of welfare schemes, for which a majority of the beneficiaries are from the poorest sections of society, rich people (81%) find it more beneficial to link Aadhaar card than the poor (73%) (Table 7.2). This may suggest that higher levels of positive perceptions around the issue of linking Aadhaar with welfare services may be more opinion-based than experience-based.

Figure 7.1: People from UP most supportive of linking Aadhaar with other welfare schemes, those from Maharashtra least supportive



Note: All figures are in percentages. Rest either did not respond or don't have an Aadhaar Card.
Question asked: Do you support or oppose the linkage of Aadhaar with welfare schemes such as pension scheme, ration, LPG cylinder etc.?

Table 7.2: Rich most supportive of linking Aadhaar with welfare schemes, poor least supportive

Class	Linking Aadhaar with welfare schemes such as LPG, ration etc.		
	Support	Oppose	Can't say
Poor	73	11	16
Lower	78	13	9
Middle	78	13	9
Rich	81	13	6

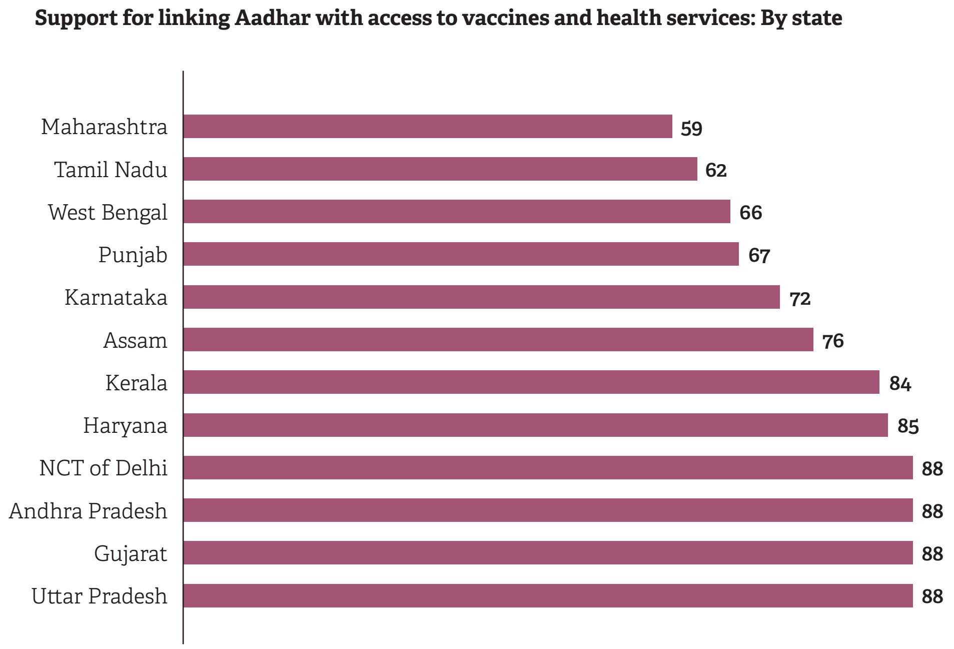
Note: All figures are in percentages.
Question asked: Do you support or oppose the linkage of Aadhaar with the Welfare schemes such as pension scheme, ration, LPG cylinder etc.?

7.1.2. Linking Aadhaar with access to vaccines and health services

In the broader quest for good governance and providing welfare services and the maintenance of records, the Aadhaar card became a means for accessing the public healthcare system. Access to healthcare services and vaccines became a priority, especially after the Covid-19 pandemic.

When respondents were asked whether they support or oppose the linkage of Aadhaar with access to vaccines and health services, three out of four (77%) supported it (Figure 7.2). Across states, Uttar Pradesh, Gujarat, Andhra Pradesh and NCT of Delhi emerged as the top supporters (88%). In contrast, relatively lower support came from Maharashtra (59%), Tamil Nadu (62%), West Bengal (66%) and Punjab (67%).

Figure 7.2: UP most supportive of linking Aadhaar with health services, Maharashtra least supportive



Note: All figures are in percentages. Rest either opposed or did not respond.
Question asked: Do you support or oppose the linkage of Aadhaar with the access to vaccines and other health services?

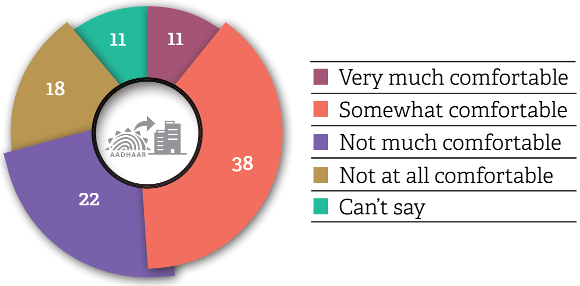
7.1.3. Linkage with other services

Post the nine-judge-bench verdict on Aadhaar, commercial banks, payment banks and even telecom service providers cannot seek Aadhaar details[6] from their customers. Earlier, they often insisted on linking their customers' Aadhaar cards with respective services threatening to block their access in the case of failure to meet this requirement (Sengupta, 2017). This cautionary intimidation by private companies has been struck down after the *Puttaswamy vs Union of India* case. The Apex Court removed Section 57 of the Aadhaar Act and declared it "unconstitutional", thus ensuring that no company or private entity has the authority to coerce an individual to disclose their 12-digit Aadhaar number.

However, when people were asked whether they felt comfortable sharing their Aadhaar number with different agencies such as telephone companies or internet service providers and banks, one in ten (11%) said that they feel very much comfortable sharing their Aadhaar number whereas nearly 40 percent felt somewhat comfortable. On the other end, close to one in five (18%) were not at all comfortable (Figure 7.3).

Figure 7.3: One out of five people not at all comfortable sharing their Aadhaar details with private agencies

Level of comfort in sharing Aadhaar data with private companies



Note: All figures are in percentages.
Question asked: How comfortable do you feel sharing your Aadhaar number with private companies such as telephone companies or internet service providers and banks, etc. – very much, somewhat, very less or not at all comfortable?

In states such as Kerala (36%), Andhra Pradesh (29%) and Delhi NCT (26%) a proportionally higher number of people said that they were not at all comfortable sharing their Aadhaar numbers (Table 7.3). Notably, more than a third of the respondents from Kerala felt very uncomfortable sharing their Aadhaar details with such entities, and a majority of the respondents from the state, 57 percent, felt uncomfortable (very and somewhat combined).

Table 7.3: Respondents from Kerala, Andhra, Delhi, and Haryana least comfortable sharing Aadhaar details with private companies

States	How comfortable are you sharing Aadhaar number with telephone/internet service providers across states			
	Very much	Somewhat	Not much	Not at all
NCT of Delhi	11	37	17	26
Uttar Pradesh	9	41	20	11
Assam	10	50	10	11
Kerala	11	24	21	36
Tamil Nadu	9	46	24	11
Maharashtra	7	44	19	17
Gujarat	20	37	24	11
Karnataka	10	30	50	8

[6] As per the Prevention of Money-laundering (Maintenance of Records) Third Amendment Rules, 2019, if anyone wishes to receive any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016), it is mandatory to submit Aadhaar number to the banking service provider. For other banking services, Aadhaar is a preferred KYC document. One may use any other officially valid documents as prescribed by Reserve Bank of India

Punjab	6	48	20	11
Haryana	14	37	20	23
Andhra Pradesh	12	31	23	29
West Bengal	7	35	24	18

Note: All figures are in percentages. Rest either did not have Aadhaar card or did not respond.
Question asked: How comfortable do you feel in sharing your Aadhaar number with private companies such as telephone companies or internet service providers and banks, etc. – very much, somewhat, very less or not at all comfortable?

7.2. Biometric landscape and criminal investigation

The Criminal Procedure (Identification) Act 2022, a law allowing the collection of biometrics of convicts, under-trials and arrested persons, came into effect on August 4, 2022. As per this legislation, police now have the authority to collect palm prints, fingerprints and footprints, DNA, retina and iris biometrics and several other behavioural and physical features including the handwriting and signature, of any person who has been apprehended, whether as an accused, convict or otherwise, for the purposes of a criminal investigation. The legislation has come under severe criticism from opposition parties and other non-state actors such as rights activists due to its alleged violation of individuals' liberties, freedom, and privacy (Bhardwaj, 2022).

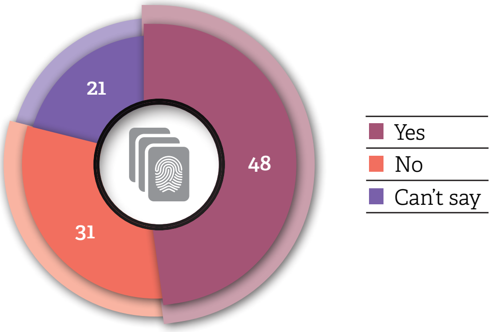
The law was aimed at empowering state agencies to keep a detailed record of all under-trials or suspects, as well as convicts, with an understanding that they might, in the future, be possibly involved in an illegal act. It further authorises the National Crime Records Bureau (NCRB) to store, preserve, and share the biometric data, which if required, can be shared or destroyed depending upon its intended use by law enforcement agencies. The data can be stored for up to 75 years.

In an attempt to create a robust infrastructure for crime prevention, the legislation, in fact, gave unbridled powers to the state and executive machinery. Some politicians have voiced their concerns that the law is "intrusive and violative of the Supreme Court verdict on privacy" (The Times of India, 2022). It can also be used against those who are detained for being involved in political protests and becoming a 'threat' to the state. However, the Home Minister has reassured that these people will be kept out of the law's purview (Ibid). Yet, on the other hand, the new law also expands its scope with a wider 'ambit of persons' that is bound to help investigation agencies gather data against the accused, and based upon legally admissible evidence, establish them as criminal.

Given this, we tried to gauge the citizens' perspective on this issue. The respondents were asked whether they think the police should be able to collect the biometric details (such as fingerprint, footprint, iris, retina scan, facial recognition, etc.) of all suspects, including those who haven't been declared guilty by the court. Close to half (48%) agreed that police should be allowed to collect such details; three in every ten (31%) said that they should not be able to whereas one in five (21%) did not share their perspective on this issue (Figure 7.4).

Figure: 7.4: About half supported the collection of biometric details of suspects, including under trials

"Should the police be allowed to collect biometric data of suspects, including those who haven't been declared guilty?"



Note: All figures are in percentages.
Question asked: Do you think the police should be able to collect the biometric details (such as fingerprint, footprint, iris, retina scan, facial recognition, etc.) of all suspects, including those who haven't been declared guilty by the court?

Table 7.4: Haryana most supportive of the police collecting biometric data of suspects, Tamil Nadu least supportive

States	"Police should be able to collect the biometric details of suspects"	
	Support	Against
Haryana	74	16
Gujarat	69	22
NCT of Delhi	65	24
Kerala	58	24
Uttar Pradesh	57	17
Andhra Pradesh	48	22
Karnataka	38	54
Assam	35	32
Maharashtra	34	38
West Bengal	34	37
Punjab	32	36
Tamil Nadu	25	56

Note: All figures are in percentages. Rest did not respond.
Question asked: Do you think police should be able to collect the biometric details (such as fingerprint, footprint, iris, retina scan, facial recognition, etc.) of all suspects, including those who haven't been declared guilty by the court?

A large proportion of the respondents from Haryana (74%), Gujarat (69%) and Delhi - NCT (65%) were of the opinion that police should have this power. Conversely, a significant proportion of respondents from Tamil Nadu (56%) and Karnataka (54%) (Table 7.4) were of the opinion that police should not be allowed to possess such powers.

Those belonging to the Adivasi community (44%) were significantly more likely to oppose giving the power to the police to collect biometric data, as compared to the general caste group (28%) (Table 7.5). Tribal lands are often encroached upon by the state in the name of 'development'. With the help of existing laws, the state builds dams and displaces communities leaving those inhabiting these localities vulnerable (Mohanty, 2020) and thus their livelihoods and lives get affected. If, however, they protest against the government, it is found that at times they get imprisoned or blacklisted for 'fabricated' charges (adaniwatch.org, 2022). Under such conditions, their biometric data allows the government to keep a constant vigil on them. This may be a probable cause for their reservation against the collection of biometric details by the police. In SPIR 2018, it was found that more than a quarter of the respondents (28%) were of the opinion that STs are falsely implicated by the police under Maoism-related charges. Similar findings also emerged in SPIR 2020-21, Volume I, when people from only conflict-affected areas were surveyed. In such a context, distrust of the police's intention may be a major factor for the Adivasis being critical of the provisions of the new CrPC (Identification) Act.

Across religious groups, Muslims were the least supportive of giving the power to the police to collect the biometric data; 39 percent of the Muslims were in support, 32 percent were against giving power to the police to collect biometric details whereas the greatest chunk i.e., 29 percent of Muslims did not share their opinion on this (Table 7.5).

Table 7.5: Adivasis and Muslims most critical of the police collecting biometric details of all suspects

Caste Group	Police should be able to collect the biometric details	
	Support	Against
Dalits	42	34
Adivasis	39	44
Other Backward castes	50	31
General	50	28
Hindu	50	30
Muslims	39	32
Christians	44	36
Sikhs	43	34
Other religious minorities	47	32

Note: All figures are in percentages. Rest did not respond.
Question asked: Do you think police should be able to collect the biometric details (such as fingerprint, footprint, iris, retina scan, facial recognition, etc.) of all suspects, including those who haven't been declared guilty by the court?

Some parallels can also be drawn between the rate of imprisonment of people from specific communities and their reluctance in supporting the collection of biometric data by the police. According to the prison statistics compiled by the NCRB until December 31, 2019, two out of three inmates (66%), hail from the SC, ST and OBC categories. Out of this 34.01 percent are OBCs, 20.74 are SCs and 11.14 percent are STs. Across states, the rate of incarceration of SCs, STs, OBCs and Muslims is disproportionately higher than their overall population. Hence, as reported in the current study, STs (44%), SCs (34%) and OBCs (31 %) are more reluctant towards biometric data collection, compared to those from the general category (Table 7.5).

7.3. Drones

Drones or unmanned aerial vehicles represent a landmark development in technology (Holden, 2020). For the purposes of regulation, jurisdictions categorise them by weight, size, speed and other attributes. The term 'remote pilot' implies that despite being unmanned, there is always a pilot who remotely controls its operation.

Recently, drones and their multitude of use have become more visible, ranging from public services such as helping in disaster-prone areas (Das, 2022), to the detection of crimes, detection of LPG leaks (Delft University of Technology, 2021), etc. Their application can also be helpful in law-and-order enforcement and in border patrolling. However, in the absence of adequate safeguards and regulation, several issues pertaining to government overreach, data aggregation, and the invasion of privacy are emerging (Nishith Desai Associates, 2018). Under these conditions, it becomes necessary to understand how the citizens of India perceive the use of drones by state or non-state actors.

7.3.1. State agencies vs non-state actors

One of the points of query in this survey was to understand how the mechanism of possible drone surveillance impacts citizens and how likely they are to support it if it is done by state and non-state actors. Several questions to this end were asked in the survey, such as on the use of drones by various state actors such as the government, armed forces, or the police, as well as private entities, including individuals and private companies.

Table 7.6: More than one out of two people strongly support the use of drones by the armed forces, government, and the police

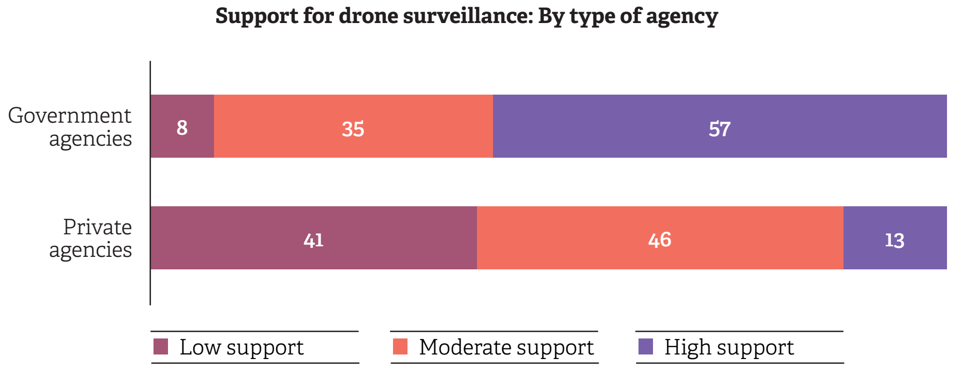
State and non-state agencies	Level of support for drone usage				
	Full Support	Somewhat support	Somewhat opposition	Fully opposition	Not aware of drones
Government	55	23	4	4	10
Armed forces	58	20	4	3	10
Police	51	26	5	3	10
Individuals	10	18	17	32	12
Private companies	12	22	17	27	11

Note: All figures are in percentages. Rest did not respond.
Question asked: To what extent do you support or oppose the use of drones by the following agencies? (List of agencies mentioned in the left column of the table)

As one can observe in Table 7.6, a large segment of the population (55%) supports the use of drones by state agencies. On the other hand, there is a trust deficit when it comes to usage by individuals and by private companies (11%). More than half the respondents fully supported the use of drones by the government (55%), the armed forces, (58%) and the police (51%). In contrast, when it comes to the usage of drones by private entities such as individuals and private companies, nearly 30 percent are completely opposed to it. Since this is a fairly new and evolving technology which hasn't yet penetrated many parts of the country, one-tenth of the respondents did not know about drones and their usage.

The study clubbed all the responses of government agencies including the government, armed forces, and the police on one side and created an index of support for drone usage by government agencies (refer Index 5 in Appendix 5 for details about the index formation), while the individuals and private companies were clubbed and another index of support for drone usage by private agencies was created (Index 6 in Appendix 5). Upon analysis, it was found that the support for drone usage by government agencies significantly outnumbered the support for its use by private agencies (Figure 7.5). People were more than four times more likely to strongly support the use of drones by government agencies, compared to its use by private entities.

Figure 7.5: High levels of support for use of drones by government agencies, low support for use by private agencies



Note: All figures are in percentages. Appendix 5 Index 5 (by government agencies) & Index 6 (by Private agencies).

The lack of trust for its use by private entities is striking in the context of the loosening of laws and regulations around owning and flying drones by individuals, particularly in the absence of any data protection law or a proper grievance redressal mechanism. According to the Drone (Amendment) Rules 2022 issued by the Ministry of Civil Aviation on February 11, 2022, the requirement of a certificate or license for flying small to medium-sized drones (up to 2 kgs) for non-commercial purposes has been done away with (News18, 2022).

Regarding the use of drones by state agencies, while examining the state-wise opinions, it was found that respondents from Gujarat (81%) and Uttar Pradesh (72%) showed substantially high levels of support. Respondents from Karnataka (60%) also indicated moderate support, relatively higher opposition to this was seen in states such as Punjab (17%) and West Bengal (17%) (Table 7.7).

Across the occupation category, the lowest levels of support were observed amongst farmers (14%). The relatively lower levels of support for drone usage by government agencies amongst farmers is a noteworthy finding, especially in view of the fact that the Centre has been pushing for incentivising the use of drones for farming. In a two-day drone festival organised in May 2022, Prime Minister Narendra Modi said that one of his dreams was to see a drone on every farm.

Conversely, respondents from Kerala (69%) and NCT of Delhi (57%) showed relatively low support, followed by Assam (72%) and Karnataka (70%). More than one-tenth of the respondents from Andhra (18%) and Uttar Pradesh (17%) displayed a higher degree of support (Figure 7.6).

Table 7.7: Those from Gujarat most supportive of the use of drones by government agencies, those from Karnataka least supportive

States	Degree of support for usage of drones by government agencies (Index)		
	Low	Moderate	High
Gujarat	3	16	81
Uttar Pradesh	2	26	72
Andhra Pradesh	3	29	68
Haryana	5	28	67
NCT of Delhi	5	30	65
Maharashtra	8	36	56
Assam	5	39	56
Kerala	6	38	56
Tamil Nadu	13	41	46
Punjab	17	38	45
West Bengal	17	40	43
Karnataka	10	60	30

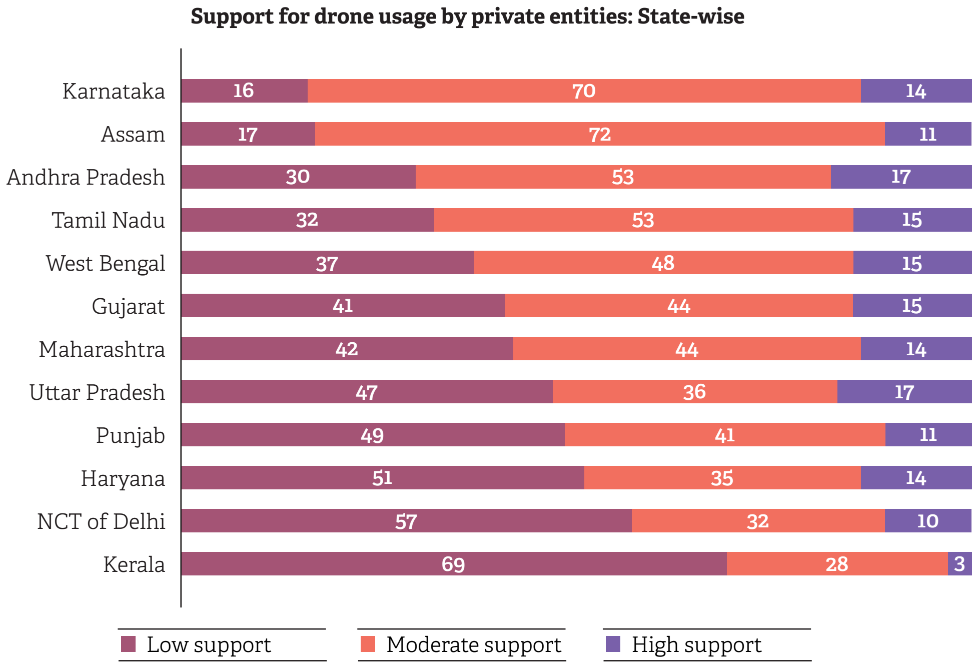
Note: All figures are in percentages. Details about the index are mentioned in Appendix 5 Index 5.

Table 7.8: Farmers most likely to oppose drone usage by government agencies

Religion	Degree of support for usage of drones by government agencies (Index)		
	Low Support	Low	High
Professionals	7	33	60
Government Employee	6	36	58
Business	7	38	55
Labourer	9	38	53
Farming	14	36	50
Student	6	35	59
Housewife-stay at home	8	34	58
Other occupation	6	35	59

Note: All figures in percentages. Extreme polarities were taken into consideration rather than moderate categories on either side, while doing the analysis in order to give a clear distinction of choices. Details about the index are mentioned in Appendix 5 – Index 5.

Figure 7.6: Karnataka most supportive of drone usage by private entities (Index), Kerala least supportive

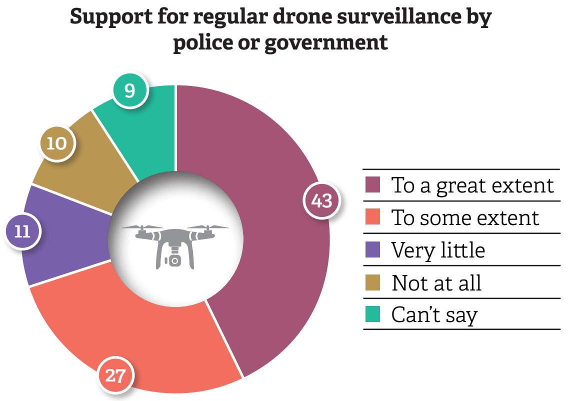


Note: All figures in percentages. Details about the index are mentioned in Appendix 5 – Index 6.

7.3.2. Drones and their usage by state and non-state actors

The use of drones for mass surveillance is well known. Drones, by the virtue of their elusive size and design, have the potential for secret surveillance. They can be operated without detection while traversing the public/private divide in people's lives with ceaseless monitoring through ultra-high-resolution cameras that can track people from as high as 20,000 feet (Lynch, 2012). Such unwarranted surveillance has the potential to jeopardise citizens' civil liberties, privacy, and fundamental rights.

Figure 7.7: Forty-three percent people highly supportive of regular drone surveillance of the public by the government or the police



Note: All figures are in percentages.
Question asked: In your opinion, to what extent is the use of drones justified for regular surveillance of the public by the government or police?

In order to understand how routine surveillance through drones impacts people, they were asked whether state surveillance (by the police or government) through drones is justified and a majority agreed. Four of every ten (43%) respondents said that it is justified 'to a great extent', followed by one-fourth (27%) saying that it is okay to 'some extent'. Only one of every ten (10%) of the respondents was against state surveillance through drones (Figure 7.7).

Across, locations, significant support came from states such as Gujarat (63%), UP (57%) and Delhi (56%). In contrast, the opposing states were Kerala (30%) and Punjab (14%) (Table 7.9).

Interestingly, the degree of support increased as we moved across income levels, with one out of two rich respondents strongly justifying drone surveillance by the state, as against 39 percent among the poor who justify it (Table 7.10). It was also found that people belonging to the poor and lower economic classes were less aware of drone technology, and therefore the proportion of no responses was higher amongst these sections.

Table 7.9: Gujarat most supportive of regular drone surveillance by police/ government, Karnataka least supportive

States	How justified is the usage of drones for regular surveillance by police and government	
	Fully justified	Not at all justified
Gujarat	63	3
Uttar Pradesh	57	5
NCT of Delhi	56	8
Andhra Pradesh	50	8
Haryana	48	11
Assam	46	5
West Bengal	44	10
Maharashtra	38	6
Punjab	33	14
Kerala	32	30
Tamil Nadu	24	11
Karnataka	22	4

Note: All figures are in percentages. Extreme polarities were taken into consideration rather than moderate categories on either side, while doing the analysis in order to give a clear distinction of choices.
Question asked: In your opinion, to what extent is the use of drones justified for regular surveillance of the public by the government or police?

Table 7.10: Poor least likely to support regular drone surveillance of the public by the police/government

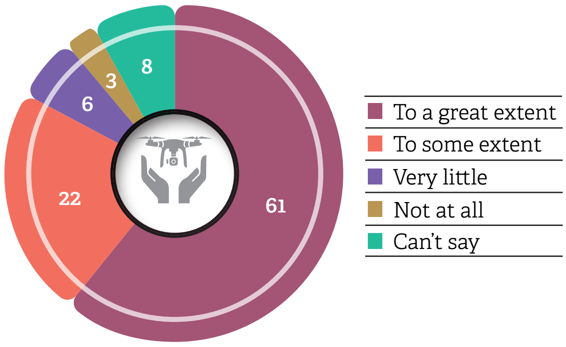
Class	How justified is the usage of drones for regular surveillance by police and government?	
	Fully justified	Not at all justified
Poor	39	11
Lower	40	9
Middle	44	9
Rich	50	11

Note: All figures are in percentages. Extreme polarities were taken into consideration rather than moderate categories on either side, while doing the analysis in order to give a clear distinction of choices.
Question asked: In your opinion, to what extent is the use of drones justified for regular surveillance of the public by the government or police?

Such perceptions justifying mass surveillance by the state can be problematised in the absence of adequate legislation to prevent unauthorised state surveillance and misuse of such technology or the data gathered through them. Such unchecked powers have the potential of serious abuse. Unfettered use of surveillance technology by the police can have major negative consequences, particularly in the absence of structural reforms in the day-to-day working of the police, which suffer from widespread biases and prejudices (SPIR, 2018 and 2019), along with several other infrastructural and procedural deficiencies.

Figure 7.8: Sixty-one percent strongly support the use of drones by the police for enforcement of rules

Support for drone usage by police for rules' enforcement

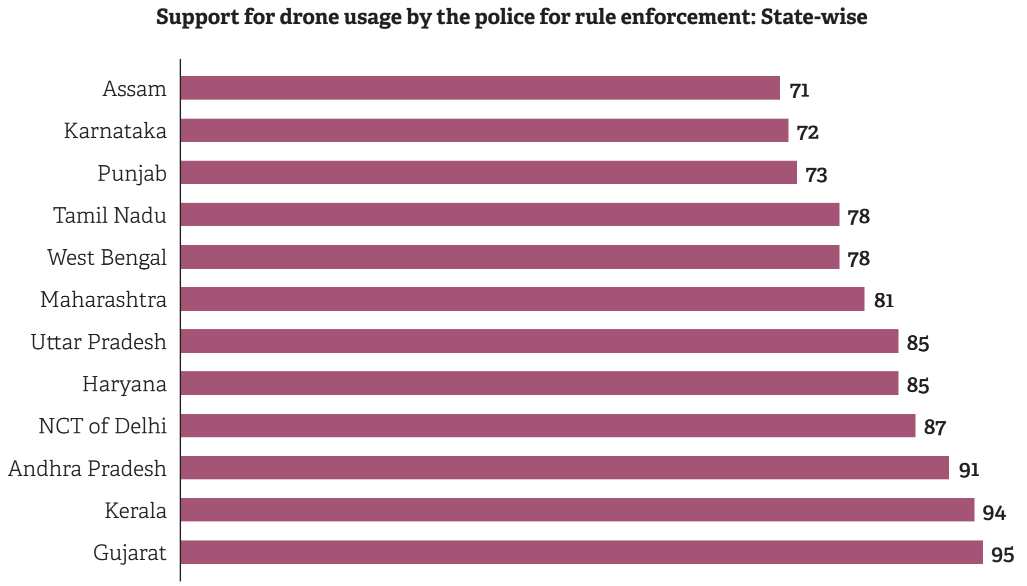


Note: All figures are in percentages.
Question asked: In your opinion, to what extent is the use of drones justified in the enforcement of rules and regulations by the police – such as enforcing a lockdown during the pandemic?

When the respondents were asked whether drone usage by police for rule enforcement is justified or not, three out of five felt it is fully justified and another one of five said that it is justified to some extent (Figure 7.8). Merely three percent were completely against the usage of drones for enforcing the rules and regulations by the police, while six percent were slightly concerned. This further consolidates the argument that the use of such technologies by state actors, even in the absence of safeguards against undue surveillance, is seen to be in the public interest.

Across states, similar patterns were observed, with the highest proportion of respondents from Gujarat supporting the usage of drones by the police for law enforcement (95%), followed by Kerala, (94%) and Andhra Pradesh (91%); while Assam, Karnataka, and Punjab stood at the opposite end of the spectrum.

Figure 7.9: Those from Assam least likely to support police usage of drone for rule enforcement, those from Gujarat most likely to support



Note: Responses such as 'to a great extent and to some extent' have been merged and presented in the graph. All figures are in percentages.
Question asked: In your opinion, to what extent is the use of drones justified in the enforcement of rules and regulations by the police – such as enforcing a lockdown during the pandemic?

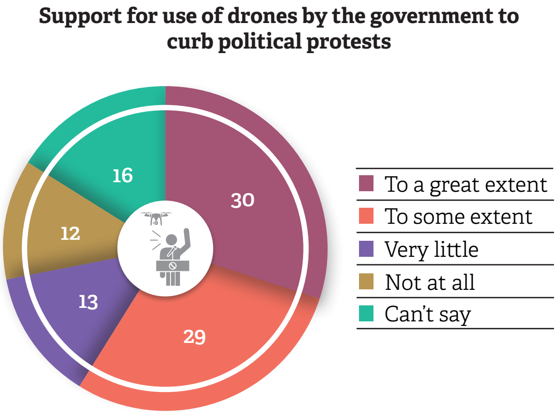
7.3.3. Use of drones for crackdown on protest

Police drones usually come with cameras and built-in speakers and have a variety of surveillance equipment and communication interception tools such as 'IMSI' (International Mobile Subscribers Identity) catchers. They have the potential to track people's movement or monitor their calls and messages. FRT (facial recognition technique) is also employed to do the same. There have been reports that the government has used drones to crack down on dissent during Citizenship Amendment Act (CAA)–National Register of Citizens (NRC) protests of 2020. Protestors were often surprised when they saw the drones flying over their heads and while spotting them some did cover their heads (Ganai, 2019).

In order to assess how the citizens perceive this crackdown on protests, they were asked whether they think drone usage by the government to curb protests is justified or not. Close to 60 percent (including 30% who said it is justified to great extent and 29% who said that it justified to some extent) supported it. However, a quarter felt that it is not justified (Figure 7.10).

While doing a state-wise comparative analysis, we found that in BJP-ruled states such as Gujarat (85%), Haryana (67%), and Uttar Pradesh (65%), the support for using drones for curbing political protest was highest. On

Figure 7.10: Nearly one out of three people strongly support drone usage by the government to curb political protests



Note: All figures in percentages.
Question asked: To what extent do you think it's justified for the government to use drones to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

Table 7.11: Over four of five people in Gujarat support drone usage by government to quell dissent

States	Support for drone usage by the government to curb protests	Against drone usage by the government to curb protests
Gujarat	85	7
Haryana	67	17
Uttar Pradesh	65	12
Andhra Pradesh	65	22
Maharashtra	61	20
NCT of Delhi	57	35
Assam	57	20
Tamil Nadu	57	22
Karnataka	57	42
Kerala	56	32
West Bengal	45	30
Punjab	34	37

Note: Responses such as 'to a great extent and to some extent' were merged into one category of support and 'very little and not at all' were merged into another category 'against' to give a binary and comparison. Rest did not respond. All figures are in percentages.
Question asked: To what extent do you think it's justified for the government to use through drones to curb political movement or protests against policies & laws enforced by the government – to a great extent, to some extent, very little or not at all?

the other hand, 42% of respondents from Karnataka, 32% from Kerala, 30 percent from West Bengal, and 37 percent Punjab respectively were against it. (Table 7.11).

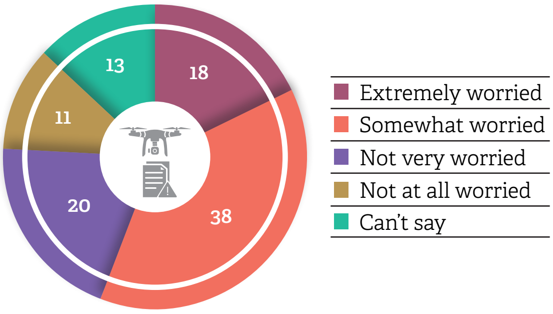
7.3.4. Concerns about breach of privacy

Unlike CCTV cameras which are conventional stationary monitoring devices, drones are portable and equipped with high-powered cameras with night vision that can surveil large areas without anyone seeing them. This becomes a concern for every citizen as their privacy can be easily breached and photos or videos of them can be collected without their consent or even their knowledge.

In order to understand how concerned the public is about such possible intrusions, the respondents were asked how worried they feel about the fact that drones can be misused to collect their photos or videos. More than half (56%) of the respondents said that they were worried that drones can be misused, with 18 percent being 'extremely worried' and 38 percent 'somewhat worried'. On the other hand, a little over 30 percent were not worried about this (Figure 7.11).

Across states, respondents from Haryana (71%) and Andhra Pradesh (71%) were the most worried about the misuse of drone footage, followed by those in Gujarat (68%) (Table 7.12).

Figure 7.11: More than one out of two people worried that drones could be misused to collect their personal data



Note: All figures in percentages.
Question asked: How worried do you feel that drones could be misused to collect data/photos of people like you

Table 7.12: Haryana most worried about misuse of drones, Karnataka least worried

States	Worried that drones can misused to collect their data/photos	Not worried that drones can misused to collect their data/photos
Haryana	71	22
Andhra Pradesh	71	17
Gujarat	68	27
NCT of Delhi	67	21
Assam	61	15
Tamil Nadu	58	32
Maharashtra	54	25
Punjab	53	30
Kerala	52	40
Uttar Pradesh	48	32
West Bengal	45	40
Karnataka	30	67

Note: Responses such as 'A lot and somewhat' were merged into one category of 'worried' and 'least and not at all' were merged into another category 'not worried' to give a binary. Rest did not respond. All figures in percentages.
Question asked: How worried do you feel that drones could be misused to collect data/photos of people like you?

7.3.5. Drone usage for public good

Drones, besides being used for state or commercial surveillance, also have a lot more potential to provide deliveries and support services during emergencies. Several pieces of research have indicated that they have helped in nuclear accidents, preventing the release of dangerous material, in floods, forest fires and earthquakes. They can be used for rapid damage assessment and thus help in de-escalating the disaster through aerial reconnaissance. Rescue teams often use them for locating victims (Restas, 2015). Moreover, they can also be used to supply goods during calamities.

When people were asked whether it is justified to use drones for providing services and essential goods to the public during crises, 62 percent strongly supported their usage. On the contrary, when asked about the usage of drones by private companies to deliver goods, the proportion of those who strongly supported it went down to 41 percent (Table 7.13).

7.4. Facial Recognition Technique (FRT)

In modern 'surveillance societies' (Wood, 2009) individuals are monitored increasingly by an entangled assemblage of government and private entities. These actors use human faces to discover an individual's identity. The human face becomes symbolic of a person's identity and the face becomes an 'exclusive' terrain for the formation of a facial recognition system. FRT and its application stand next to finger-based biometric systems and are in huge demand. The system plays an important role in crime detection, information security, forensic investigations, and border surveillance and has several other applications (Rusia & Singh, 2022). The recognition system uses spatial geometry for distinguishing between individuals and uses particular facial features to identify and authenticate the person in the source image (Chawla & Trivedi, 2017).

Table 7.13: People more likely to support drone use by the government for goods/service delivery than its use by private companies

How justified is the usage of drones	By the government to deliver essential goods during difficult time	By the private companies to deliver goods
To great extent	62	41
To some extent	19	26
Not much	7	12
Not at all	3	9

Note: All figures are in percentages. Rest did not respond.
Question asked: In your opinion, to what extent is the use of drones justified for providing services and essential goods to the public during difficult times such as droughts, famines, natural calamities, etc. - to a great extent, to some extent, very little or not at all? In your opinion, to what extent is the use of drones justified to provide services and essential goods to the public by private companies - to a great extent, to some extent, very little or not at all?

Even though FRT can be a beneficial tool in the identification of an individual, its potential form is use is far more concerning. Its actual use or misuse depends upon who operates it, for what purposes and in what configuration. This can also be compounded by the absence of a requisite legal and regulatory infrastructure governing its usage. In India, there is currently no legislative sanction against the use of FRTs either by the state or by private agencies or through personal usage. Recently, the Internet Freedom Foundation issued a legal notice to NCRB and Ministry of Home Affairs in relation to a Request for Proposal (RFP)[7] issued by them in July 2019. The legal show cause notice intended to shed light on the absence of statutory sanction for the creation of such relevant systems. The NCRB replied with a 2009 Cabinet note which provided authority to six agencies (Internet Freedom Foundation, 2019), including NCRB, to use such technology. As per NCRB, FRT had the approval of the Cabinet and need not have any legislative or executive order for the establishment of AFRS (automated facial recognition system). However, the cabinet approval in itself is not a statutory enactment and cannot confer upon anyone the legislative authority to use the technology of facial recognition. Moreover, as noted in *Puttaswamy vs Union of India*, "an executive notification does not satisfy the requirement of a valid law *Puttaswamy*. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental rights cannot be sustained by an executive notification". Thus, the system of FRT lacks both, adequate legislation, and the principle of legitimate state aim and proportionality. The use of FRT in both the public and private sectors needs legislative oversight using an impact assessment for data protection to ensure privacy before deployment.

However, even in the absence of such an assessment or legal provisions governing its usage, FRT is being employed not only by the NCRB but also by several other state agencies (see Chapter 2 for more details). In December 2022, the Ministry of Civil Aviation launched the DigiYatra, a facial recognition application, at several domestic airports. Under this system, users can upload their photos to a government-owned app and post-Aadhar verification, their travel documents will be scanned and verified using facial recognition while travelling (MoneyControl, December 2022). Unfortunately, the nuances of surveillance architecture have not yet

[7] Request for Proposal to procure National Automated Facial Recognition System' available at http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

Table 7.14: One out of two people fully support the use of FRT by the government, police

Agencies	Level of support usage of FRT			
	Fully support	Somewhat support	Somewhat oppose	Fully oppose
Government	50	20	4	4
Police	46	23	5	4
Traffic signal	44	21	6	4
Private companies	11	19	15	25
Individuals	9	16	15	30

Note: All figures are in percentages. Rest did not respond.
Question asked: To what extent do you support or oppose the use of facial recognition technology (FRT) by following agencies? (List of the agencies mentioned in the left column of the table)

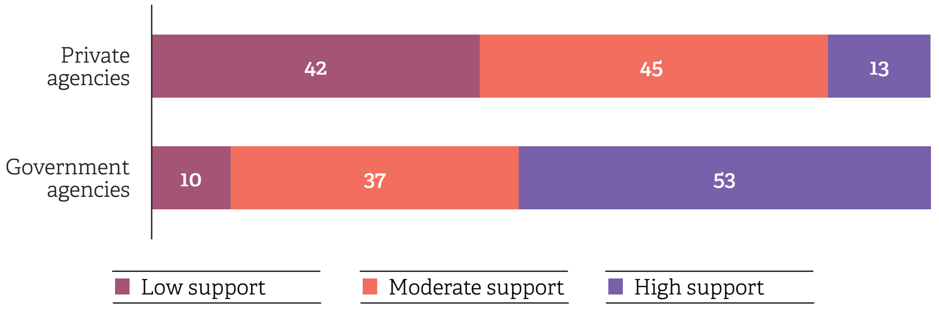
become topics of larger public debates and dialogues. Little information is also available in the media about the dangers and pitfalls of such technologies (See Chapter 4 for a detailed media analysis of surveillance-related issues), and what is often emphasised in the public domain is only the effectiveness of such technology in crime prevention and/or detection. This context helps us understand the response of the public to this issue.

7.4.1. State and private entities

Despite the lack of a robust regulatory legal infrastructure for FRT, the study wanted to understand how citizens perceive its usage by state and private entities. In an attempt to understand this multi-layered complexity, several questions were asked, on the extent of support for the use of facial recognition technology (FRT), whether by the government, police and traffic signal (the state actors) or by private companies and individuals (private entities).

Notably, we found that a little over one in five people were not aware of FRT. Among the rest, a majority of the respondents showed sweeping support in favour of the usage of FRT by state agencies, including the government (50%), police (46%), and at traffic signals (44%), while significantly lower proportions of respondents supported its use by private entities. In the case of private companies, a quarter of the respondents were completely opposed (25%) to the use of FRT, whereas for individual usage, 30 percent completely opposed it (Table 7.14).

Figure 7.12: People are four times more likely to strongly support the use of FRT by government agencies, compared to its use by private entities (Index)



Note: All figures are in percentages. Details about the indices are mentioned in Appendix 5 – Index 7 (by government agencies) & Index 16 (by Private agencies).

This data further endorses the argument that support for government entities and their use of surveillance technology is wide-spread, as opposed to the use of same technologies by private companies or individuals. Two consolidated indices were made to measure the level of support for using FRT by government agencies and another for private agencies, and the findings reiterate the above point (Figure 7.12).

In the case of state agencies, respondents from Gujarat showed extensive support for FRT usage by government agencies (71%), followed by UP (70%), and Andhra Pradesh (65%), whereas lower levels of support were shown by respondents from Punjab (21%), followed by West Bengal (19%) and Tamil Nadu (15%) (Table 7.15).

Some of these trends also resonate with the findings of drone surveillance by government actors (refer to Section 7.3.1.) that shows extensive support for state agencies. Further, in the case of private entities, Kerala had the highest level of opposition to their use of FRT (74%) followed by Delhi (60%) and Haryana (52%). Some states, like Assam (72%) and Karnataka (70%), displayed moderate support. On the other end, respondents from UP exhibited the strongest support (21%) followed by Andhra (16%) (Table 7.15) for use of FRT by private entities.

7.4.2. FRT and criminal investigation

FRT, in its essence, has two main functions – verification and identification. Verification is completed by matching a live photograph of a person by comparing it to one existing in a database. In contrast, the authentication of an individual's identity is done by matching the face of an individual from a photograph/video and comparing it with the best match from the entire database. The latter is usually done for the purposes of security and surveillance (Jain, 2021). The system may be used to identify criminals from a pool of suspects. FRT creates a probability match score between the suspect that is to be identified

Table 7.15: Those from Andhra most likely to support use of FRT by government agencies, those from Punjab most likely to oppose it.

States	Use of FRT by the government agencies		Use of FRT by the private agencies	
	Oppose	Support	Oppose	Support
Andhra Pradesh	3	65	31	16
Assam	8	59	17	10
Gujarat	2	71	46	15
Haryana	7	61	52	13
Karnataka	13	20	16	14
Kerala	7	63	74	4
Maharashtra	9	57	42	14
NCT of Delhi	9	48	60	12
Punjab	21	41	51	8
Tamil Nadu	15	44	34	15
Uttar Pradesh	5	70	47	21
West Bengal	19	36	43	15

Note: All figures are in percentages. Rest did not respond. The response categories of "fully support" and "somewhat support" were clubbed together as "Support" and "Somewhat oppose" and "fully oppose" were clubbed together as "Oppose". Details about the indices are mentioned in Appendix 5 – Index 7 (by government agencies) & Index 8 (by Private agencies).

Table 7.16: People more likely to support FRT use by government for convicted criminals than for under trials

Use of FRT in criminal cases	Support	Against	Can't say	Fully oppose
Those convicted of minor offences	80	8	12	4
Those convicted of serious offences like rape, sexual assault	78	9	13	4
Those charged but not convicted	60	25	15	4

Note: The category "to a great extent" and "to some extent" were clubbed together to make 'support' and 'very little and not at all' were clubbed to make 'against' for a better contrast. All figures are in percentages.
Question asked: To what extent is the use of Facial Recognition Technology (FRT) by the police or the government justified in the following circumstances – to a great extent, to some extent, very less or not at all? (List mentioned in the left column of the table)

and a database of identified criminals or suspects. Various matches are generated with varying likelihoods of them being the correct matches, which are then finalised by a human analyst to reduce misidentification (Goldberg, 2021). As a result, the police or the government possess large databases of the facial identity of citizens, purportedly for public safety.

The increased use of FRT by government agencies has led to the emergence of concerns with respect to privacy, accountability and transparency, as there is a lack of regulatory infrastructure (Bacchini & Lorusso, 2019). In such conditions, possessing a database of people's facial identification gives the government enormous and unchecked power over citizens. Compounded with incessant monitoring, it has the potential to transform an intrusive state into a surveillance state. Therefore, with the aim of understanding how the general public perceives these issues, several questions were asked in the survey.

Table 7.17: Kerala, Gujarat and Andhra most likely to support FRT use for convicted criminals/accused, Punjab least likely

STATES	Support for database of FRT for minor offenses	Support for database of FRT for serious offenses	Support for database of FRT for those charged but not convicted
Kerala	92	93	64
Gujarat	91	89	75
Andhra Pradesh	87	85	73
Haryana	84	85	68
Tamil Nadu	80	77	67
Karnataka	79	71	64
West Bengal	79	75	43
NCT of Delhi	77	80	56
Maharashtra	75	74	57
Uttar Pradesh	71	77	62
Assam	68	65	54
Punjab	64	58	39

Note: The categories of support "to a great extent" and "to some extent" were clubbed together to form the support category. All figures are in percentages. Rest were against or did not respond.
Question asked: To what extent is the use of Facial Recognition Technology (FRT) by the police or the government justified in the following circumstances - to a great extent, to some extent, very less or not at all?

The respondents were asked their opinion on the use of FRT by the police or the government to keep a database of people. Nearly eighty percent supported its use by the government to keep a database of people who have been convicted of minor or serious offences (78%), but the degree of support went down to 60 percent for those who have been charged with a crime but have not been convicted (Table 7.16).

States such as Kerala, Gujarat, and Andhra Pradesh were the most supportive of maintaining an FRT database of people who were convicted for minor and major offences and, in fact, the same set of states also favoured that an FRT database should be kept for persons who were charged but not convicted. On the other hand, people from Punjab and Assam did not show high levels of support for the idea of storing a database of such persons (Table 7.17).

Christians were the biggest supporters (90%) of using FRT for keeping records of a person convicted for minor offences. In fact, Christians, along with Hindus, were also largely in favour of keeping FRT records of those who were charged but not convicted. On the contrary, the support among the other religious minorities such as Muslims and Sikhs was not as strong (Table 7.18).

7.4.3. FRT and political dissent

FRT can also be used for the purposes of identifying people who participate in political protests, communal riots, and even common citizens. For such identification, one's face is matched with many others in the database. In simpler words, a facial map is obtained from a photograph or video and matched against the entire database of people to identify the likely person in the photograph/video. Post the Criminal Procedure (Identification) Act 2022, which replaced Sections 3 and 4 of the Identification of Prisoners Act, 1920, the police can now collect wider categories of data pertaining to 'convicts and other people' for the purposes of investigation in criminal matters.

In this context, respondents were asked whether they support or oppose the use of FRT by the police or government on those protesting against government laws/ policies. Six out of every 10 respondents (61%) supported such use, with those Gujarat (84%) most in support, followed by Andhra Pradesh (73%) and Tamil Nadu (69%). The states where low support was found were Punjab, Kerala, and West Bengal (Table 7.19).

When the respondents were asked whether the use of FRT by the police to identify those engaging in communal riots was

Table 7.18: Muslims and Sikhs least likely to support government use of FRT for convicted criminals or under trials

	Support for database of FRT for minor offenses	Support for database of FRT for those charged but not convicted
Hindu	80	62
Muslims	75	54
Christians	90	63
Sikhs	77	55
Other religious minorities	76	56

Note: The categories of support "to a great extent" and "to some extent" were clubbed together to form the support category. All figures are in percentages. Rest were against or did not respond.
Question asked: To what extent is the use of Facial Recognition Technology (FRT) by the police or the government justified in the following circumstances - to a great extent, to some extent, very less or not at all?

Table 7.19: More than 60 percent support the use of FRT to identify protestors, two out of five say drones should be used to identify common citizens

Degree of support for identification through FRT	Support	Against	Can't say
To identify those participating in protest against government or laws	61	24	15
To identify those participating in communal riots or disturb law and order	75	11	14
To identify common citizens, regardless of crime	39	44	17

Note: The category "to a great extent" and "to some extent" were clubbed together to make 'support' and 'very little and not at all' were clubbed to make 'against' for a better contrast. All figures are in percentages.
Question asked: To what extent is the use of Facial Recognition Technology (FRT)by the police or the government justified in the following circumstances - to a great extent, to some extent, very less or not at all? (List of circumstances mentioned in the left column of the table).

justified or not, a staggering three-fourths (75%) found it justified, as opposed to a mere four percent who did not (Table 7.19). Across states, Kerala emerged as the biggest supporter (91%), followed by Gujarat (87%). In comparison, respondents from Punjab were least supportive of the use of FRT, followed by those in Assam (Table 7.20).

On being asked whether they think regular surveillance of common citizens by FRT is justified or not, respondents were more likely to say that it was justified (39%),compared to those who were against it (31%) (Table 7.19). Notably, however, the level of support for government use of FRT for regular surveillance is significantly lower, compared

Table 7.20: Gujarat most likely to support use of FRT to identify protestors, Kerala most likely to support its use during communal riots and Karnataka most likely to support its use to identify common citizens

States	Support for identification through FRT ...		
	To identify those protesting against government	Of those who are causing communal riots and disturbing law and order	Of common citizens regardless of them having committed a crime
Gujarat	84	87	41
Andhra Pradesh	73	84	50
Tamil Nadu	69	73	55
Karnataka	68	68	57
Uttar Pradesh	67	73	33
Maharashtra	64	72	48
Haryana	63	79	35
Assam	58	65	42
NCT of Delhi	58	74	31
Kerala	56	91	27
West Bengal	41	73	29
Punjab	27	56	24

Note: The categories of support "to a great extent" and "to some extent" were clubbed together to form the support category. All figures are in percentages. Rest were against or did not respond.
Question asked: To what extent is the use of Facial Recognition Technology (FRT) by the police or the government justified in the following circumstances - to a great extent, to some extent, very less or not at all?

Table 7.21: Sikhs least likely to support the use of FRT by government during protests, communal riots and to identify common citizens

Religion	Support for identification through FRT ...		
	To identify those protesting against government	Of those who are causing communal riots and disturbing law and order	Of common citizens regardless of them having committed a crime
Hindu	62	76	40
Muslims	56	69	35
Christians	61	86	36
Sikhs	39	65	33
Other religious minorities	54	73	37

Note: The categories of support “to a great extent” and “to some extent” were clubbed together to form the support category. All figures are in percentages. Rest were against or did not respond.
Question asked: To what extent is the use of Facial Recognition Technology (FRT) by the police or the government justified in the following circumstances - to a great extent, to some extent, very less or not at all? (List of circumstances mentioned in the left column of the table).

to the levels of support for specific purposes, such as creating a database of convicts or identifying protestors or rioters. When responses across states were compared, major support for this came from Karnataka (57%), followed by Tamil Nadu (55%), and Andhra Pradesh (50%). In contrast, the least support came from the states of Kerala, Punjab, and West Bengal (Table 7.21).

Overall, Hindu and Christian respondents supported the usage of FRT for identifying people whether they were engaged in any political protest, or communal riots or using FRT for the identification of common citizens. On the other hand, the least support was noticed among the respondents belonging to the Sikh religion (39%). The context of this low support could be their participation in the recent farmer movement against farm laws, during which there were reports of the government deploying such technology to identify protestors (Financial Times, 2021). Other than Sikhs, Muslims and other religious minorities were also less likely to support the use of FRT for identifying people (Table 7.21).

Conclusion

In people’s perception, the distinction between ‘private’ and ‘government’ is layered with different connotations. Very often, while private entities are viewed with suspicion, similar surveillance activities by the government is frequently overlooked and often even encouraged, as is evident from the findings.

As observed in both cases of surveillance involving drones and FRT, state agencies, including the police, enjoyed the overwhelming support of the common citizenry in India. State agencies are seen as acting in the best interest of citizens even while conducting widespread surveillance. Such support is especially noteworthy in the case of crackdown on dissent and routine surveillance of public spaces.

The highest levels of support for surveillance by government agencies come from states such as Gujarat, Uttar Pradesh, and Haryana ruled by the same party which is in power at the Centre. In contrast, the opposition-ruled states such as Kerala, West Bengal and Punjab are more likely to oppose the use of such technologies, across several of the survey questions. For Punjab, in particular, such distrust in government use of surveillance technology could stem from their historical adversarial stance against the Centre as well as their recent experience of large-scale protests against the enactment of the controversial farm laws which were later withdrawn. During these protests, the government reportedly used several of these technologies to identify and target protestors.

References

Adani Watch (2022, April 11). Indian tribal protesters jailed under 'fabricated' charges as railway for Adani's Carmichael coal goes full steam ahead. Retrieved from: https://www.adaniwatch.org/tribal_protesters_jailed_under_fabricated_charges_as_railway_for_adani_coal_goes_full_steam_ahead. Accessed on: 21st October 2022

Bacchini, F. and Lorusso, L. (2019), Race, again: how face recognition technology reinforces racial discrimination", Journal of Information, Communication and Ethics in Society, Vol. 17 No. 3, pp. 321-335. https://doi.org/10.1108/JICES-05-2018-0050

Bakshi, G. K., Arya, P., & Reddy, K. (2018, May 31). Aadhaar Day 2- *senior advocate Shyam Divan: "how can the state compel me to part with personal information to a private entity?"*. The Leaflet. Retrieved from: https://theleaflet.in/aadhaar-day-2-senior-advocate-shyam-divan-how-can-the-state-compel-me-to-part-with-personal-information-to-a-private-entity/. Accessed on: 22nd October 2022.

Bhardwaj, A. (2022, March 28). New bill in Parliament allows biometric data collection on arrest or detention, OPPN up in Arms. *The Print*. Retrieved from: https://theprint.in/politics/new-bill-in-parliament-allows-biometric-data-collection-on-arrest-or-detention-oppn-up-in-arms/892149/. Accessed on: 21st October 2022.

Common Cause and Centre for Study of Developing Societies. (2018). Status of Policing in India Report 2018: A Study of Performance and Perceptions. Retrieved from: https://commoncause.in/pdf/SPIR-2018-c-v.pdf.

Common Cause and Centre for Study of Developing Societies. (2019). Status of Policing in India Report 2019: Police Adequacy and Working Conditions. Retrieved from: https://www.commoncause.in/uploadimage/page/Status_of_Policing_in_India_Report_2019_by_Common_Cause_and_CSDS.pdf.

Common Cause and Centre for Study of Developing Societies. (2021). Status of Policing in India Report 2020-21, Volume I: Policing in Conflict-Affected Regions. Retrieved from: https://www.commoncause.in/uploadimage/page/SPIR-2020-2021-Vol%20I.pdf.

Chawla, D., & Trivedi, M. C. (2017). A comparative study on Face Detection Techniques for security surveillance. *Advances in Computer and Computational Sciences,* 531–541.

Das, K. (2022, April 28). Uttarakhand: Drones could soon help tackle natural disasters. *The Times of India.* Retrieved from: https://timesofindia.indiatimes.com/city/dehradun/ukhand-drone-agency-developing-first-of-its-kind-system-to-help-in-disasters/articleshow/91133621.cms. Accessed on: 21stOctober 2022.

Delft University of Technology. (2021, July 14). Swarm of autonomous tiny drones can localize gas leaks. *ScienceDaily*. Retrieved from www.sciencedaily.com/releases/2021/07/210714110540.htm. Accessed on: 18th October 2022

Ganai, N. (2019, October 22). Police use drones to shadow and identify protesters in Kashmir. *Outlook India.* Retrieved from: https://www.outlookindia.com/website/story/india-news-police-use-drones-to-shadow-and-identify-protesters-in-kashmir/340897. Accessed on 18th October 2022.

Goldberg, R. D. (2021, April 12). You can see my face, why can't I? facial recognition and Brady. *Columbia Human Rights Law Review*. Retrieved from: https://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-. Accessed on: 17th October 2022.

Holden, P. (2016). Flying Robots and Privacy in Canada. 14.1 CJLT 65., Retrieved from https://ssrn.com/abstract=2571490. Accessed on 20th October 2022.

Internet Freedom Foundation (08th November 2019). NCRB Finally Responds to Legal Notice on Facial Recognition, We Promptly Send a Rejoinder. Retrieved from: https://internetfreedom.in/the-ncrb-responds/.

Jain, A. (2021, July 2). From investigation to conviction: How does the police use FRT?. *Internet Freedom Foundation.* Retrieved from: https://internetfreedom.in/from-investigation-to-conviction-how-does-the-police-use-frt/. Accessed on: 18th October 2022.

Kaur, N. (2018, June 11). "Making the Aadhaar compulsory through executive instructions is completely illegal and contrary to the directions of the Supreme Court", says senior advocate Arvind Datar. *The Leaflet.* Retrieved from: https://theleaflet.in/specialissues/making-the-aadhaar-compulsory-through-executive-instructions-is-completely-illegal-and-contrary-to-the-directions-of-the-supreme-court-says-senior-advocate-arvind-datar/. Accessed on: 20th October 2022.

Lynch, J. (2012, January 10). Are drones watching you? *Electronic Frontier Foundation.* Retrieved from: https://www.eff.org/deeplinks/2012/01/drones-are-watching-you. Accessed on: 21st October 2022.

Ministry of Civil Aviation. (2022, February 11). Drone (Amendment) Rules, 2022. Retrieved from: https://egazette.nic.in/WriteReadData/2022/233331.pdf.

Mohanty, A. (2020, September 8). Pro-poor schemes in plenty, but no end to tribal community struggles. *Down to Earth.* Retrieved from: https://www.downtoearth.org.in/blog/governance/pro-poor-schemes-in-plenty-but-no-end-to-tribal-community-struggles-73273. Accessed on: 21st October 21 2022.

MoneyControl News. (2022, December 1). Govt rolls out facial recognition system DigiYatra at Delhi, Bengaluru and Varanasi airports. Retrieved from: https://www.moneycontrol.com/news/business/govt-rolls-out-facial-recognition-system-at-delhi-bengaluru-and-varanasi-airports-9634731.html. Accessed on 11th December 2022.

Najibi, A. (2020, October 24). Racial Discrimination in Face Recognition Technology. *Harvard University: Graduate School of Arts and Sciences.* Retrieved from: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

Nishith Desai Associates (2018). Unravelling the Future Game of Drones: Can they be legitimized? Retrieved from:http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research20Papers/Unravelling_The_Future_Game_of_Drones.pdf. Accessed on: 18th October 2022.

Nitin, B. (2018 April 25). 1.3 Lakh Aadhaar Numbers Leaked from Andhra Government Website, Linked to Personal Details. *The News Minute.* Retrieved from: https://www.thenewsminute.com/article/13-lakh-aadhaar-numbers-leaked-andhra-govt-website-linked-personal-details-80178.

Restas, A. (2015). Drone Applications for Supporting Disaster Management. *World Journal of Engineering and Technology,* 316-321.

Rusia, M. K., & Singh, D. K. (2022). A comprehensive survey on techniques to handle face identity threats: Challenges and opportunities. *Multimedia Tools and Applications.*

Sengupta, R. (2017, October 6). Link Aadhaar to bank account: Is it really mandatory to link Aadhaar with Bank Account and Mobile? *The Times of India*. Retrieved from: https://timesofindia.indiatimes.com/business/india-business/is-it-really-mandatory-to-link-aadhaar-with-bank-account-and-mobile/articleshow/60780393.cms. Accessed on: October 21, 2022.

Sethi, A. (2017, August 25). Right to privacy: Data shows states using Aadhaar to build profiles of Citizens. *Hindustan Times.* Retrieved from: https://www.hindustantimes.com/india-news/despite-govt-denials-states-building-databases-for-360-degree-profiles-of-citizens/story-qnSLHGyZIXiZiO4ce84UuO.html. Accessed on: 2nd November 2022.

Singh, H. (2017, August 8). 20,000 Aadhaar numbers leaked on Punjab government website. *Hindustan Times.* Retrieved from: https://www.hindustantimes.com/punjab/20k-aadhaar-numbers-leaked-on-govt-website-in-ludhiana/story-SUNfHvrLvwLR2IqOmtzwPP.html.

Singh, S. (2022, June 14). New Aadhaar Data Leak Exposes 11 Crore Indian Farmers' Sensitive Info. *Zee News.* Retrieved from: https://zeenews.india.com/personal-finance/aadhaar-data-breach-over-110-crore-indian-farmers-aadhaar-card-data-compromised-2473666.html.

Times of India. (2022, August 23). Explained: The New Criminal Procedure (Identification) act and why it has raised some concerns. Retrieved from: https://timesofindia.indiatimes.com/india/explained-the-new-criminal-procedure-identification-act-and-why-it-has-raised-some-concerns/articleshow/93343873.cms. Accessed on: 16th October 2022.

Zuboff, S. (2020). The age of surveillance capitalism: The fight for a human future at the New Frontier of Power. *Public Affairs.*

Chapter 8:

Digital Financial Security and Cybercrimes

Key findings

- Three out of four people are anxious about an unknown person/company accessing their email accounts.
- Nearly one out of two persons reported frequently receiving targeted ads based on internet search history.
- Forty percent people are very anxious that information provided by them online can be misused.
- Four out of ten people are very anxious that their digital identity can be stolen by a person or company.
- Seven percent people report having their personal photos or videos being shared online without their permission.
- Upper caste, upper class, educated respondents most likely to use digital financial modes such as digital wallets, net banking, UPI, etc., while SC, illiterate and poor respondents least likely to use these.
- Forty-four percent people very anxious about unknown persons/companies tracking their bank account transactions. Nearly three out of four people worried that their personal data such as Aadhar number or PAN can be leaked online.
- Twelve percent survey respondents have been victims of online financial frauds.

CHAPTER 8

Digital Financial Security and Cybercrimes

The digital world is expanding by the day. The ubiquity of the discourse around digitisation and technology – from payments to the use of social media, and multiple forms of online communication– further encourage its uses and advantages. The whole process, however, is rarely viewed from a critical lens. The rise of social media and digital platforms have impacted the country's entire social fabric. Instagram, Facebook, and Twitter accounts have become common and routine. Access to one's social media handles reveals crucial information about the person in question. Mobile phones are transforming the world of finance and thus creating opportunities for widespread inclusion among underserved groups and regions (Traynor, 2018). Digital credit allows individuals and businesses to access a more networked space in real time. However, even with the ease that comes with digitisation of all aspects of life, it is also fraught with huge challenges that people face regularly, with no clear solutions in sight.

The pervasiveness of social media platforms has, in many ways, expanded and democratised the global space. It is no more a luxury but a necessity to own a smartphone. Yet, equally critical are the issues of access and denial of digital technology or the Internet– particularly in terms of resources, capacities, and skills. A 2022 report by Lokniti- CSDS, 'Media in India: Access, Practices, Concerns and Effects', shows that between 2004 and 2014, the proportion of households owning at least one mobile phone increased nearly eight-fold, from 11 percent to 84 percent. Other studies show that nearly six of every ten (58%)Indians use social media sites in the year 2022 (Narayan, 2022). The Hindu reports that by 2025, one-fourth of all social media users globally will be from India (Ibid).

Concerns around digitisation are primarily related to access or security of one's data and information. No wonder then, that an increase in digitisation has also led to a proportionate rise in cybercrimes. According to data released by the National Crime Records Bureau (NCRB), India reported 52,974 cases of cybercrimes in the year 2021. This figure has increased by five percent from 2020 and 15 percent from 2019. Assuming that a significant proportion of the cases of cybercrimes go unreported or unregistered, the actual numbers of such cases are likely to be much higher. According to a report released by the US Federal Bureau of Investigation (FBI), India had the fourth-highest number of victims of cybercrimes (The Mint, 2022). In March 2022, the government stated in the Parliament that the estimated financial loss due to cybercrimes in the Financial Year 2020-21 was to the tune of Rs. 63 crores (Times of India, 2022).

This chapter is divided into four sections and focuses on multiple aspects of digital privacy, financial security, and the corresponding measures.

- **Section 1** deals with issues concerning digital privacy, access to one's data and security, where we tap into the public's opinions surrounding digital and online data accessibility to an unknown person or company.

- **Section 2** focuses on threats to digital privacy, that is, identity theft and related cybercrimes.
- **Section 3** focuses on digital financial data and the potential risks surrounding it.
- **Section 4** discusses the feasibility, success and failures of measures such as verification and alerts that are being adopted by organisations involved in the finance sector.

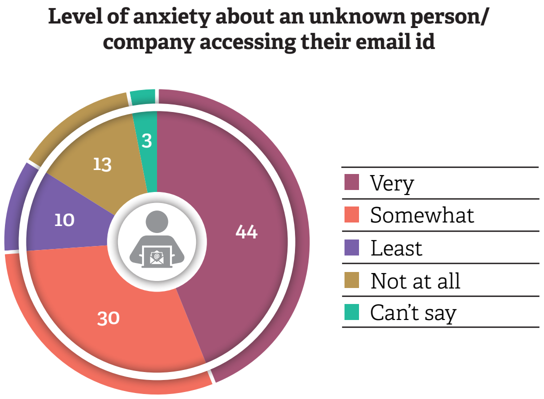
8.1. Concerns around digital privacy: Data access and security

Data accessibility has grown incrementally in digitally networked societies. While this empowers citizens in multiple ways, it also poses a serious threat to individual privacy. Globally, privacy is fast emerging as an important fundamental human right encompassing personal data, its processing, personal communications, as well as the processing of personal profiles on social media. However, with the rise of a global database of information and communication, the understanding of privacy has changed (Romansky, 2014). For instance, in Europe, as proposed by the European Commission, the traditional understanding of privacy as "the right to be alone" has transformed with a newer vision of "the right to be forgotten." (Ibid)

Further, smartphones and social media handles have made one's personal identity very visible, public, and easily accessible. One can find out almost everything by gaining access to someone's smartphone or social media handles. This, at times, creates overarching anxiety about divulging personal information on public platforms. On the other hand, large databases available on the internet, whether belonging to the government or private entities, contain several layers of personal information of even those who may never have had access to the internet themselves. Any leakage of such databases can threaten the right to privacy of even those who never actively disclosed their personal details online.

The availability, development and utilisation of advanced computing and information technology over recent years have resulted in enormous growth in the volumes of data being generated, processed, and also shared (Mauthner & Parry, 2013). This mass collection of data is becoming increasingly significant for governments all across the world in having a pertinent database about their citizens. Often undisclosed, the collected data is at times shared with third-party individuals and organisations without the knowledge or consent of the persons concerned. Additionally, there are numerous risks associated with third-party data sharing. For instance, a poorly constructed website or web service from a security perspective could allow an individual access to the database containing employees' personal identifiable information or PII. This risk of unauthorised access or unauthorised disclosure of data and potential misuse is one of the many significant risks in digital data management (Geer, 2007). A typical example would be emails. They have now become one of

Figure 8.1: Three out of four people are anxious about an unknown person/company accessing their email accounts



Note: All figures are in percentages. Rest did not respond. Question asked: How anxious are you that this might happen to you (very anxious, somewhat anxious, least anxious or not at all anxious) - An unknown person or company can access your email account.

the most frequently used professional channel of communication.

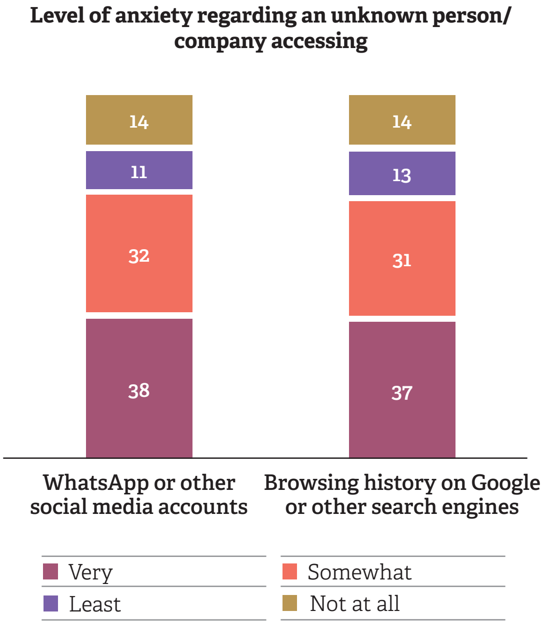
Despite their wide usage, there is some level of anxiety among users regarding the extent of privacy. In our survey, we asked the respondents how anxious they feel about the idea that an unknown person or company can access their email accounts. About three out of four (74%) respondents felt some level of anxiety about this possibility. This anxiety was equally prevalent across all age brackets (Figure 8.1).

Social media's significance as one of the most crucial influencers in global geopolitics has been ever-increasing. The level of penetration of such platforms in people's lives is unprecedented today and is continually increasing. Since 2019, there has been a 45 percent growth in active internet users in rural India (Nielsen, 2022). Social media sites are also becoming battlegrounds for the validation of personal and political identities and opinions. This has created marketing opportunities for global powers like never before. This is primarily because knowing an individual's needs and anxieties by snooping on their social media activity makes micro-targeting of advertisements possible. The more you know, the better you reach your target audience. This directly establishes linkages between data and profits leading to intense competition for the gathering of people's personal data on social media.

Despite all this, the laws have failed to catch up with the ground reality in order to ensure the digital security of social media users. This compromised privacy has led to a state of anxiety among users regarding their social media information.

To understand this, we asked our respondents how anxious they felt that an unknown person or company could access their WhatsApp or other social media accounts. The results reveal that nearly seven of every ten (70%) of the respondents were anxious to some degree and of them, close to four in ten were highly anxious about it (Figure 8.2).

Figure 8.2: Nearly four out of ten are very anxious about an unknown person/company accessing their WhatsApp or other social media accounts and search history



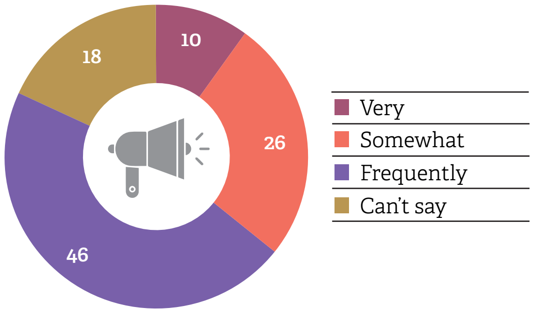
Note: All figures are in percentages. Rest did not respond. Question asked: How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) An unknown person or company or company can access your WhatsApp or other social media accounts. (ii) An unknown person or company can know what you search on google or other search engines.

Data mining practices are not only restricted to private companies for advertisement purposes but are also being actively undertaken by political parties for influencing and shaping electoral outcomes. Users' social media activities can reveal patterns that point to their specific political leanings. This information can be used by political parties to take their campaigns to the appropriate audiences.

Information about content consumption can also be obtained by looking at a person's search history. For this reason, the information about what people search on Google and other search engines is of utmost importance. When it comes to accessing browsing data on search engines such as Google, Internet Service Providers (ISPs) hold some level of power to track online activity, how much time

Figure 8.3: Nearly one out of two persons reported frequently receiving targeted ads based on internet search history

Frequency of receiving targeted ads based on your online search



Note: All figures are in percentages.
Question asked: How frequently do you receive targeted messages or advertisements- frequently, sometimes or never. (i) Based on what you search online.

a user has spent on a particular website and the kind of content one watches, along with their geographic location through IP addresses. Further, there are other freely available tools that allow unauthorised parties to retrieve deleted data as well.

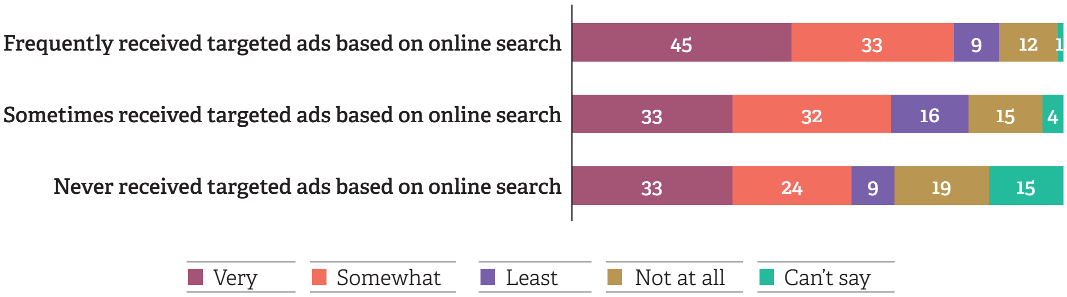
In this backdrop, we attempted to gauge the levels of concerns among Indian users. We asked the respondents if they were anxious that an unknown person or company can access their search history, and more than two out of three respondents (68%) expressed some level of anxiety (Figure 8.2). Respondents were also asked if they receive targeted messages and advertisements based on what they searched on Google or other search engines. Not surprisingly, nearly three out of four respondents (72%) reported receiving targeted messages and advertisements based on what they searched online– of them close to half (46%) reported receiving such targeted messages/advertisements frequently.

It was also found that those who frequently received targeted messages based on their online search, were also highly anxious that an unknown person or company might access their browsing history (Figure 8.4).

The anxiety among respondents was further indicative of the fact that although there have been multiple technological advances that bring the world together with a single touch, there is also a substantial rise in the concern and risk factors surrounding personal data and privacy. The revelation of the Pegasus spyware (2020) scandal sparked an intense debate on the issue of digital privacy and security. The Pegasus spyware was developed by the Israeli defence group NSO and sold only to governments and was used for surveillance mainly of government critics, activists, journalists, human rights defenders, and opposition leaders. The trojan horse virus was covertly installed on mobile phones of

Figure 8.4: Those who reported frequently receiving targeted ads also more likely to be very anxious about an unknown entity accessing their online activity

Level of anxiety regarding an unknown person/company accessing search history by frequency of receiving targeted ads based on your online search

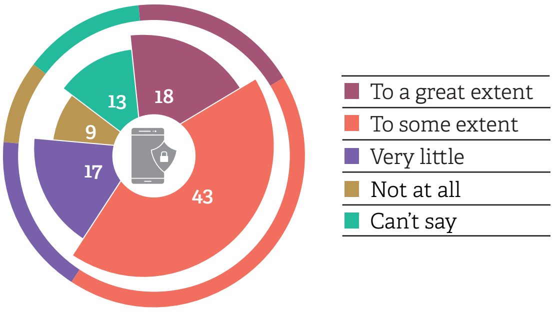


Note: All figures are in percentages.
Question asked: How frequently do you receive targeted messages or advertisements - frequently, sometimes or never? Based on what you search online.

unsuspecting users to access their data, text, chats, microphone, camera, and all apps. It came to light through investigative journalism of over a dozen media organisations worldwide (The Wire, 2021). Although mobile phone companies claim that their phones are secure and the user's privacy is not compromised because of it, the reality seems to be different.

Figure 8.5: Above 60 percent of people believe that their phone has fool-proof privacy and nobody else can access its contents

Perceptions about the level of privacy of contents on the phone



Note: All figures are in percentages.
Question asked: To what extent do you think your phone has fool-proof privacy, i.e., nobody else can access to its contents like photos, messages, videos or surfing history without your permission- to a great extent, to some extent, very little or not at all?

Thus, respondents were asked to what extent they think their phone has fool-proof privacy i.e., nobody else can access its content, such as photos, messages, videos, or surfing history, without their permission. Over six of every ten (61%) respondents believe that their phone has fool-proof privacy to varying extents. On the other hand, around a quarter of the respondents said that their phone either has very little or no fool-proof privacy (Figure 8.5).

Across people's educational levels, notably, the highest percentage of respondents who did not answer this question were non-literates. The non-literates or those with lower levels of education were most likely to be unsure of the level of privacy on their phones, while those with higher levels of education were most likely to believe that their phone has complete privacy (Table 8.1).

This may point to the digital divide prevalent in the country. At a time when the government is focusing on promoting Digital India[8], it also has to be taken into account that there is a large chunk of the population that cannot access these services.

Table 8.1: One out of two non-literate people unsure of the level of privacy of their phones.

Level of education	Degree of phone having fool-proof privacy, i.e. nobody else can access its contents like photos, messages, videos or surfing history without your permission				
	To a great extent	To some extent	Very little	Not at all	Can't Say
Non Literate	9	20	11	10	50
Upto Primary	14	29	15	8	34
Upto Matric	18	39	16	9	18
Intermediate-under graduate	18	47	18	9	8
College and above	21	48	18	8	5

Note: All the figures are in percentages.
Question asked: To what extent do you think your phone has fool-proof privacy, i.e., nobody else can access to its contents like photos, messages, videos or surfing history without your permission- to a great extent, to some extent, very little or not at all?

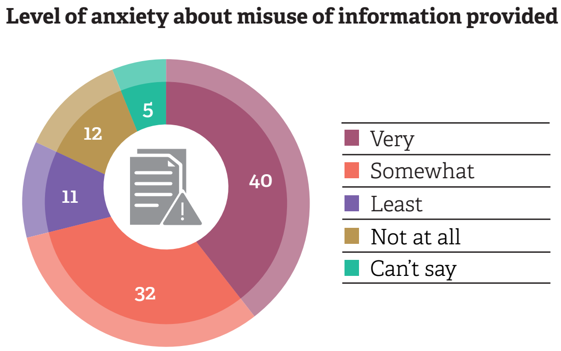
[8] Digital India is a campaign launched by the Government of India in order to ensure that the Government's services are made available to citizens electronically by improved online infrastructure and by increasing Internet connectivity or making the country digitally empowered in the field of technology.

8.2. Identity theft

The idea of digital identity, its importance, and its security becomes a particularly significant concern with growing digitisation. Although there is no concrete definition of identity theft, it is broadly understood as the theft of personal information/ data to carry out financial, social, or political frauds or a variety of cybercrimes. According to the NCRB's 'Crime in India' report (2021), Bengaluru accounts for nearly three-fourths (72%) of all registered identity theft cases across 19 metropolitan cities in India.

With personal identity information becoming a necessary prerequisite for accessing various services, whether public or private, there are rising concerns related to fraudulent activities which may threaten such information. Respondents were asked how anxious they felt about the misuse of information provided by them online. Close to three out of four (72%) expressed some level of anxiety and two-fifths were highly anxious about it (Figure 8.6).

Figure 8.6: Forty percent people very anxious that information provided by them online can be misused



Note: All figures are in percentages.
Question asked: How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) Information you provide for one purpose online can be used for another purpose.

State-wise analysis indicated that 60 percent of the respondents from Delhi (the highest among the 12 states that were surveyed), were very anxious that the information provided by them online can be used for another purpose. On the other hand, the proportion was lowest

Table 8.2: Despite higher reported cybercrime rates in Bengaluru, respondents from Karnataka least anxious about the misuse of information posted online

States	Level of anxiety anxious about misuse of information provided online			
	Very	Somewhat	Least	Not at all
NCT of Delhi	60	19	5	9
Andhra Pradesh	57	27	8	3
Gujarat	52	32	8	5
Haryana	52	24	7	11
Kerala	50	24	10	13
Uttar Pradesh	41	25	8	16
Maharashtra	35	39	8	8
Assam	33	41	4	9
West Bengal	30	41	12	9
Tamil Nadu	27	39	15	17
Punjab	20	39	12	20
Karnataka	12	33	29	23

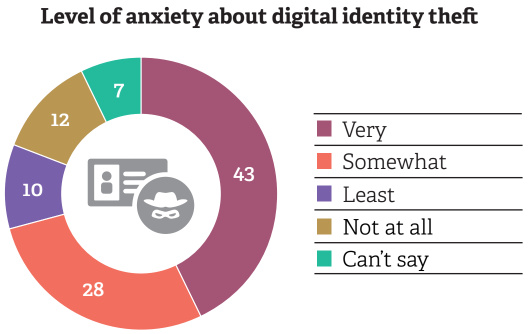
Note: All figures are in percentages. Rest did not respond.
Question asked: How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) Information you provide for one purpose online can be used for another purpose.

in Karnataka, where one of every ten felt that way (Table 8.2). This is despite the fact that the state capital, Bengaluru, which is also the IT capital of the country, has the maximum reported number of cybercrimes in India (NCRB, 2021). Although cybercrimes are highest in Bengaluru, they have declined between 2018 and 2021. The Karnataka Cyber Security Policy, which was massively publicised by the state government, and passed in May 2022, seems to have provided a sense of security to the residents of the state (Chetan, 2022).

Cases of cybercrimes and identity theft are gaining ground across the world and India is no exception to this. Several studies point to the widespread prevalence of identity theft in India. The 2021 report of the cyber security major NortonLifeHack states that two in every five Indian consumers have experienced identity theft (Dogra, 2021).

To understand the situation better, the survey respondents were asked how anxious they are that an unknown person or company can steal their digital identity. As anticipated, seven in ten respondents (71%) expressed some level of anxiety that their digital identity can be stolen (Figure 8.7). According to NCRB, India reported 4,071 cases of identity theft in 2021. At a time when the system is getting digitised and all of our digital identities are getting intermingled, this number in itself raises multiple questions on our digital policy frameworks.

Figure 8.7: Four out of ten people very anxious that their digital identity can be stolen by a person or company

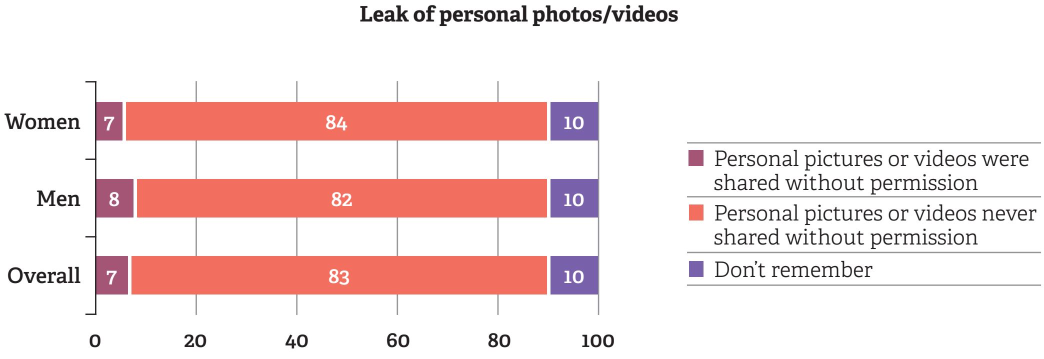


Note: All figures are in percentages.
Question asked- How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) An unknown person or company can steal your digital identity.

8.2.1 Information privacy and public defamation

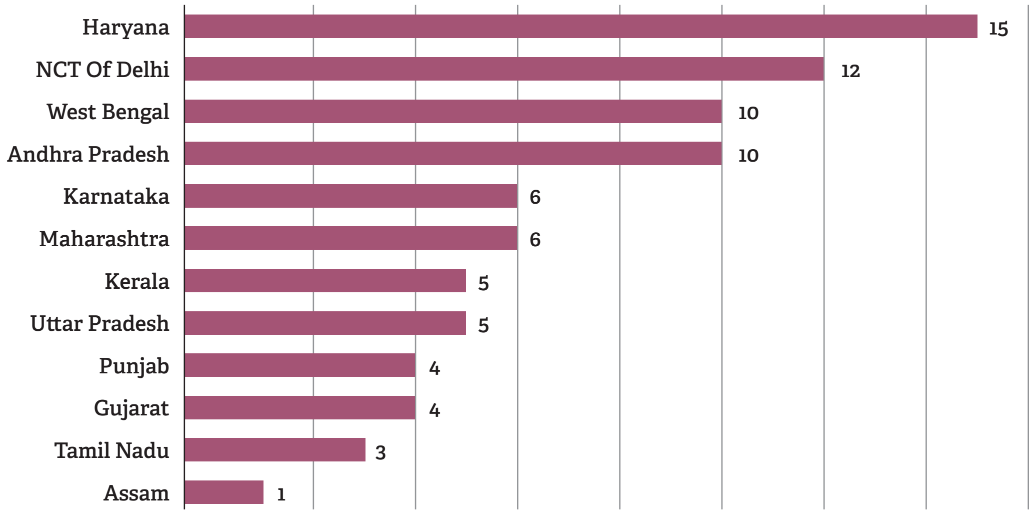
The internet makes a large universe of information available to users. While this available information provides unprecedented opportunities, it also exacerbates concerns about reputation and privacy. The study tried to assess whether the respondents have faced non-consensual sharing of their pictures or videos online. While more than 80 percent said that their pictures and videos have not ever been shared without their permission, a small fraction, seven percent, said they had faced such situations (Figure 8.8). Even as this proportion may appear insignificant, it can

Figure 8.8: Seven percent people report having their personal photos or videos being shared online without their permission



Note: All figures are in percentages.
Question asked: Has it ever happened to you or someone close to you that someone else shared your personal photos and videos without your permission?

Figure 8.9: Fifteen percent people from Haryana reported leaking of their personal photos or videos



Note: All figures are in percentages.
Question asked: Has it ever happened to you or someone close to you that someone else shared your personal photos and videos without your permission?

lead to serious crimes such as cyberstalking, sexual violence or blackmailing, and is thus noteworthy. Notably, though, comparatively more men than women said that personal pictures or videos of theirs or someone close to them were leaked.

Among those who have had their pictures or videos shared online without their permission, nearly 15 percent of victims belong to Haryana; followed by 12 percent from Delhi (Figure 8.9).

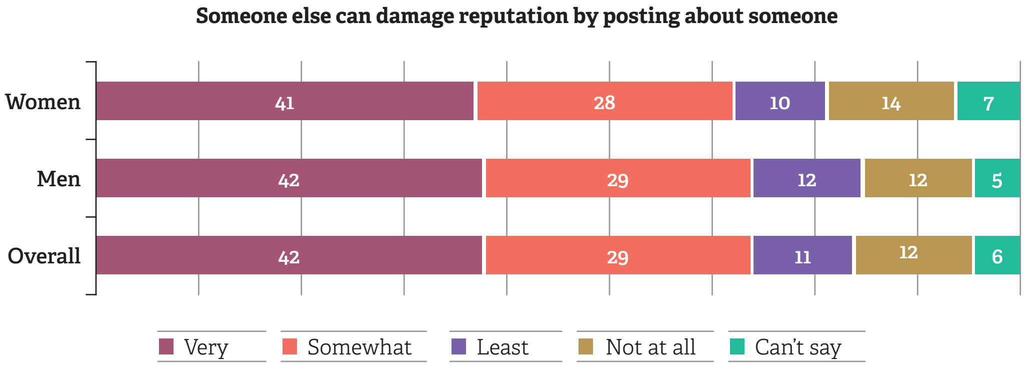
In 2015, news of organised phishing[9] and cyber scam rings from Jamtara, Jharkhand, came to light in the media (Edmond, 2015), and was later adapted into an OTT series by Netflix (Cornelius, 2020). However, over time, such rackets have mushroomed in various other parts of the country. According to interviews with senior police officers in the cybercrime department, the Mewat region, bordering Haryana and Rajasthan, is fast emerging as one of the new hubs of cyber fraud (See Chapter 3 for details of interview). Several extortion rings have emerged in the region, and they blackmail victims by threatening to leak their intimate videos online (Menon, 2022). This may be one of the reasons why, in the survey, those from Haryana were twice as likely to report such incidents, compared to the overall sample.

When respondents were asked how anxious they were that someone else can damage their reputation by posting about them online, nearly seven of every ten (71%) expressed some level of anxiety (Figure 8.10). This trend can also be seen in the data released by NCRB. The latest report of NCRB points out that out of the total 52,974 cybercrime cases reported in the year 2021, a total of 1,715 cases had the sole motive of causing disrepute (NCRB, 2022).

Cyberbullying has become a common experience for many internet users in India and is closely related to cyber defamation. According to a 2018 report published by British cybersecurity firm Comparitech, Indian children are the most cyber-bullied in the world (The Wire, 2018). An oft-used method of cyber-bullying is what is referred to as "doxxing", defined by the Merriam-Webster dictionary as the process of "publicly identifying or publishing private information about (someone) especially as a form of punishment or revenge".

[9] Phishing is the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Figure 8.10: More than two out of five people highly anxious about their reputation being damaged online by someone else

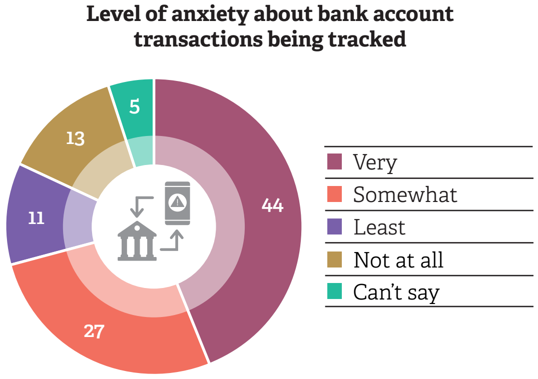


Note: All figures are in percentages.
Question asked: How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) Someone else can damage your reputation by posting about you online?

In many cases, these are targeted at vulnerable categories, such as children, women, and those from marginalised sections of society. For instance, in the 'Sulli Deals' incident of 2021, pictures of several Muslim women were posted online without their consent, to be "auctioned off" (Jha & Upreti, 2021). The legal vacuum or the lack of laws to tackle these specific crimes also becomes apparent with their rising instances (Mukherjee, 2020).

Thus, the high proportions of people who, in the survey, expressed their anxiety regarding such instances attest to the need for better safeguards, legal mechanisms and quick redressal of such forms of cybercrimes in the age of the internet.

Figure 8.11: Forty-four percent people very anxious about unknown persons/companies tracking their bank account transactions



Note: All figures are in percentages.
Question asked: How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) Your bank account transactions can be tracked by an unknown person or company.

8.3. Financial data and security

Rising digitisation has transformed the nature of service delivery across the globe, most effectively, perhaps, financial services. While the digitisation of financial technologies has created multiple opportunities for e-commerce feasibility, it has also increased risks pertaining to digital financial security. Society is thus faced with the dual nature of digital financial technologies (or Fintech), which are not only the basis of development for innovations in the financial sector but also a structural and economic risk for people (Reshetnikova et.al, 2021).

Digital financial transactions have created multiple platforms that allow customers to access basic banking facilities easily. In order to understand the penetration of digital financial services and understand people's anxiety towards operating it, we asked respondents how anxious they were that their bank account transactions can be tracked by an unknown person or company. Nearly seven of every 10 (71%) respondents expressed some level of anxiety, with 44 percent being highly anxious (Figure 8.11).

One cannot overlook the fact that there is a big chunk of the population who are cyber-illiterate and are slowly trying to become familiar with these digital payment methods. Today bank account numbers, PAN numbers and Aadhar numbers are interlinked. There are benefits of these linkages as they facilitate good governance by reaching the beneficiaries directly and bypassing a chain of middlemen. On the other hand, this linkage can also lead to the compromised financial security of the citizens. In some ways, this awareness amongst the people is apparent in the levels of their anxiousness regarding an unknown person or company tracking their bank accounts.

While more than six respondents out of 10 felt very anxious in Gujarat, close to 60 percent of the respondents from each, NCT of Delhi, Andhra Pradesh, and Haryana were also very anxious about the fact that their bank account transactions can be tracked by an unknown person or company (Table 8.3). Among these states, Gujarat has seen a spike in cases of cyber fraud in the past three years. Between the fiscal years 2019-20 and 2020-21, the cases of cyber fraud rose by a staggering 67 percent in Gujarat. The state holds a place in the top-five states with respect to cyber frauds (Raghavan, 2021). There is also a visible rise in cyber fraud cases in the NCT of Delhi and Andhra Pradesh. As per the NCRB report, the NCT of Delhi has witnessed a 110 percent rise in cybercrimes between fiscal 2019-20 and 2020-2021 (Niraj, 2022). Andhra Pradesh registered 1899 cases and out of them, fraud was the motive behind 40 percent of the cases (Babu, 2021). While answering a Lok Sabha question on a rise in cyber frauds across the states, the Ministry of Home Affairs provided data which shows that from 2020-21 to 2021-22, cases of cyber fraud have gone up in NCT of Delhi by 33 percent, in Gujarat by 51 percent, in Haryana by 79.6 percent and in Andhra Pradesh by 240 percent. (Ministry of Home Affairs, 2022).

8.3.1. Financial services and personal documents

An increasing number of digital services with greater reach, improved efficiency and minimal operating costs are being offered to individuals

Table 8.3: Respondents from Gujarat most anxious about their bank account transactions being tracked, those from Karnataka least anxious

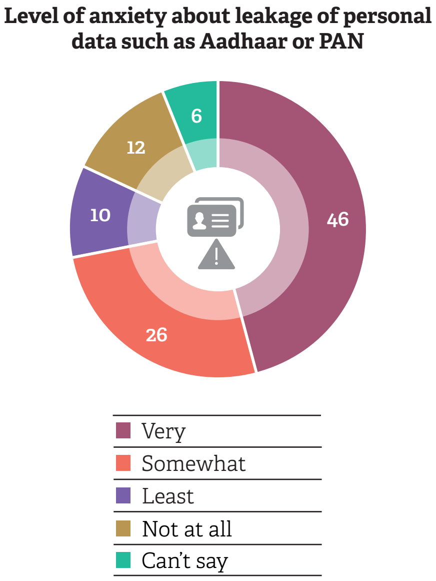
States	Level of anxiety about bank account transactions being tracked by an unknown person/company			
	Very	Somewhat	Least	Not at all
Gujarat	64	20	9	6
NCT of Delhi	59	17	5	12
Andhra Pradesh	59	21	9	6
Haryana	58	19	7	12
Kerala	54	21	10	12
Uttar Pradesh	41	24	5	20
Assam	41	33	4	12
Maharashtra	39	33	9	7
West Bengal	36	37	12	9
Tamil Nadu	34	32	12	19
Punjab	23	39	11	19
Karnataka	13	28	34	23

Note: All figures are in percentages. Rest did not respond.
Question asked: How anxious are you that this might happen to you - very anxious, somewhat anxious, least anxious or not at all anxious? (i) Your bank account transactions can be tracked by an unknown person or company.

which, aside from making life easier, also expose them to financial and other forms of crimes. The interconnectedness of systems with the involvement of a number of parties in the ecosystem extends security boundaries beyond the digital financial service, to network providers, mobile phone manufacturers, and other third-party providers in the ecosystem (Digital Financial Services Security Assurance Framework, 2021).

With the adoption of multiple forms of identification, there has been an attempt to link a number of documents with one's bank accounts. Aadhar card and PAN Card or any form of address proof has to be linked mandatorily to a bank account. However, the sharing of this data also increases the risk of it being leaked or accessed by third parties. We asked respondents how anxious they are that their personal data such as Aadhar or PAN can be leaked online. Close to three-fourths (72%) of the respondents expressed some level of anxiety (Figure 8.12).

Figure 8.12: Nearly three out of four people worried that their personal data such as Aadhar number or PAN can be leaked online



Note: All figures are in percentages.
Question asked: How anxious are you that this might happen to you- very anxious, somewhat anxious, least anxious or not at all anxious? (i) Your personal data such as Aadhar number, PAN number, etc. can be leaked online.

8.3.2. Transformation of the digital financial landscape

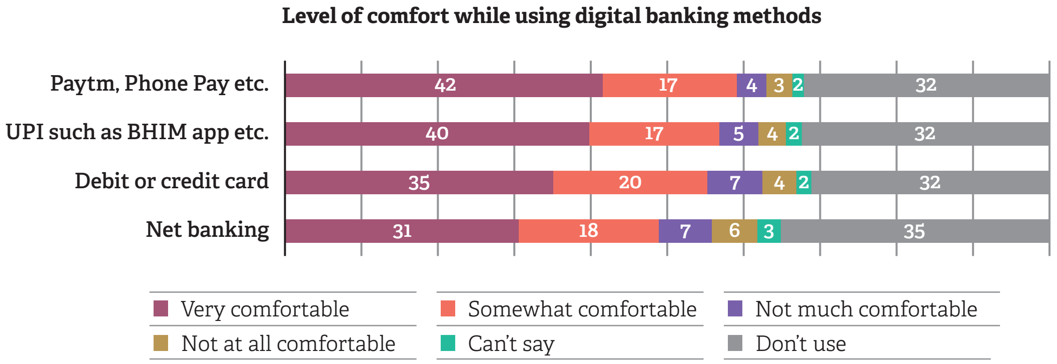
Financial literacy remains one of the essential prerequisites for effective financial planning. For financial inclusion, it is vital to have proper financial literacy, as it further affects an individual's financial decisions such as savings and investments. The Organization for Economic Co-Operation and Development (OECD) defines Financial Literacy as, "a combination of awareness, knowledge, skill, attitude, and behaviour necessary to make sound financial decisions and ultimately achieve individual financial wellbeing." (Hussain & Sajjad, 2016).

The banking landscape is changing globally. Digital stakeholders in other companies are further pushing banking industries to improve their interface and performance. With this, there has also been the gradual development of the mobile banking industry, which provides a one-stop solution for financial needs and activities.

In the larger context of the threat to data privacy, particularly financial data, the survey included questions to assess people's comfort levels while using mobile banking apps. While the questions were included with an intention of gauging how wary or not people are of such mobile applications vis-à-vis the safety of their financial data, the starkest trends emerging from the findings actually point to the socio-economic inequalities in terms of access to financial and digital literacy and the consequent variations across socio-demographic groups in terms of usage of such apps.

On average, one in every three respondents does not use these mobile banking apps. On the other hand, 40 percent were very comfortable while using Paytm, Phone Pay, UPI, BHIM, Google pay and other wallets. Our survey shows that respondents were most comfortable while using UPI and digital wallets, as compared to debit or credit card online transactions and net banking (Figure 8.13).

Figure 8.13: Nearly one out of three people do not use any form of digital banking methods



Note: All figures are in percentages.
Question asked: How comfortable do you feel while making digital or online transactions using the following modes- very, somewhat, not much or not at all comfortable? List of items are given in the graphs.

Among respondents who do not have these accounts, the highest proportion was from UP. This could be due to lower financial literacy in the state. The National Financial Literacy and Inclusion Survey, 2019, revealed that the overall financial literacy in India stands at 27 percent. It also concluded that higher the level of educational attainment and income, higher the prevalence of financial literacy among respondents. The 2015 edition of the report also revealed that UP had a financial literacy of around 10 percent, and a general literacy level of 57 percent, which indicated that the financial literacy level is even less than one-fifth of the general literacy level in the state.

In our survey, respondents were asked how comfortable they felt while making online transactions through net banking. Close to half (49%) expressed some level of comfort. The highest number of very comfortable respondents were from Andhra Pradesh (43%). This finding is in line with data provided by the Union Ministry of Electronics and Information Technology. According to the government, Andhra Pradesh ranks second in terms of per capita digital transaction, next only to Chandigarh.

Predictably, the usage of such apps is higher among younger age groups and the level of comfort decreases with an increase in the age of the respondent. More than two out of three respondents in the age bracket of 56 years and above did not use digital payment wallets, and just 17 percent were very comfortable using

Table 8.4: Older respondents least likely to use digital payment wallets or be comfortable with such apps

Age groups	How comfortable people are while using Paytm, Phone Pay and other wallets					
	Very	Somewhat	Least	Not at all	Can't say	Non-users
18-25 yrs.	55	21	4	3	1	16
26-35 yrs.	51	21	4	3	2	19
36-45 yrs.	38	19	5	4	2	32
46-55 yrs.	32	14	5	4	2	43
56 yrs. and Above	17	7	3	3	2	68

Note: All figures are in percentages.
Question asked: How comfortable do you feel while making digital or online transactions using the following modes- very, somewhat, not much or not at all comfortable? Paytm, Phone Pay, and other wallets?

Table 8.5: Nine in ten non-literates don't use Paytm, Phone Pay and other digital wallets

Level of education	How comfortable people are while using Paytm, Phone Pay and other wallets					
	Very	Somewhat	Least	Not at all	Can't say	Non-users
Non-Literate	7	2	1	1	1	88
Upto Primary	10	5	3	3	2	77
Upto Matric	25	12	3	4	2	54
Intermediate-undergraduate	45	19	4	4	2	26
College and above	57	23	5	3	1	11

Note: All figures are in percentages.
Question asked: How comfortable do you feel while making digital or online transactions using the following modes- very, somewhat, not much or not at all comfortable? Paytm, Phone Pay, and other wallets?

them, against 55 percent of those on the age group of 18-25 years (Table 8.4).

It is not just the digital banking applications, but overall, the usage of smartphones and the internet differs according to age in India. A report released by the Pew Research Centre shows that in India 57 percent of the population falling in the age group of 18-29 years use the internet or smartphones which falls to just 18 percent for Indians above the age of 50. This data is in tune with our survey results, where, as the age group increases, the level of comfort and the likelihood of using digital payment methods decreases.

A similar trend was visible across educational divisions among the respondents, with non-literate respondents occupying the lowest percentile of those who were comfortable using the applications (7%), thereby indicating a clear technological divide in the population. Further, among the respondents who were non-literate, a very significant proportion (88%), had no accounts (Table 8.5). The interface of the digital payment methods is primarily in English and text-based (instead of icon-based). This could be one of the difficulties faced by the non-literate population in using these apps. Another factor could be that non-literates are less likely to own a smartphone, as was suggested by a 2018 study conducted by CyberMedia Research, which showed that Indian states with higher literacy rates are more likely to have higher sales of smartphones, compared to feature phones (Dutta, 2018).

There was also a difference when it comes to gender divisions among the respondents who were very comfortable. While four of every ten (39%) men were very comfortable making online transactions using debit or credit cards, the proportion of women was just three of every ten (30%). This could be because of the stark digital gender divide present in India (Iqbal, 2022). The Mobile Gender Gap Report 2022 released by GSMA, points out that in India, smartphone ownership of men increased from 36 percent in 2019 to 41 percent in 2020 and 49 percent in 2021. Whereas, for women, this number is 14 percent, 25 percent and 26 percent for the years 2019, 2020 and 2021 respectively (GSMA, 2022).

There is also a stark educational divide among those who felt very comfortable while using credit or debit cards for online transactions. While only five percent of those who were illiterate expressed this comfort, over half (52%) of those who had access to education till the college levels expressed the same comfort.

A community division reveals that while more than one out of three (35%) general category respondents were very comfortable using net

Table 8.6: SCs least likely to have a net banking account, general caste most likely

Social Groups	How comfortable people are while using Net Banking					
	Very	Somewhat	Not much	Not at all	Can't say	No Account
Scheduled Caste	21	16	8	7	3	45
Scheduled Tribe	28	27	6	4	1	34
OBC	31	17	7	7	4	34
General	35	19	6	5	3	32

Note: All figures are in percentages.
Question asked: How comfortable do you feel while making digital or online transactions using the Net banking- very, somewhat, not much or not at all comfortable?

banking, just about 21 percent respondents belonging to the Scheduled Caste were very comfortable using this medium (Table 8.6). Further, SCs are also least likely to have net banking accounts at all, 45 percent, compared to 32 percent amongst the general category.

A major reason for this could be the caste-based digital divide prevalent in India. While there is little research on the subject, a study by scholars from BITS Pilani (Hyderabad) found that only 14 percent of the ST population in India has access to the internet, whereas this number is 41 percent for the Others group. Similarly, if we talk about computer literacy rates, we find that 11.2 percent of STs, 13.5 percent of SCs and 18.9 percent of OBCs know how to use computers. The same statistics for Others is 31.2 percent (Rajam et al., 2021).

With the advancements in fin-tech, there is also the entry of applications based on Unified Payment Interface (UPI) technologies such as BHIM app, Google Pay etc. that allow for quicker and easier money transfers. The study tried to gauge the opinions of respondents as to how comfortable they feel while using these apps. Nearly six of every ten (57%) were comfortable using UPI-based apps to make transactions. However, there was a clear class divide here as well. The poor were least likely to be comfortable using these apps and also the least likely to have accounts of such apps, while the rich were most likely (Table 8.7).

It is evident from the survey responses that the level of education, age, gender, class and caste is directly proportional to comfort in using digital payment methods or the likelihood of using these methods at all. The survey findings reveal that even as digital financial transactions have come a long way in India in the recent past, their usage is not uniform across socio-economic categories.

Table 8.7: Upper class four times more likely to have a UPI account, compared to the poor; more than twice as likely to be very comfortable using it

Class	Level of comfort while using UPI					
	Very	Somewhat	Not much	Not at all	Can't say	No Account
Poor	21	9	4	3	2	61
Lower	38	19	6	4	3	30
Middle	47	20	6	4	2	21
Upper	56	19	5	3	2	15

Note: All figures are in percentages.
Question asked: How comfortable do you feel while making digital or online transactions using UPI- very, somewhat, not much or not at all comfortable?

8.4. Financial security and preventive measures

E-banking has given customers a lot of ease and better service quality and many competitive advantages to the banks over the other players in the sector. But their challenges have gone up considerably due to the increasing number of digital financial crimes (Ali et.al., 2019). E-banking, which utilises ICT-based facilities for banking transactions, is also increasingly associated with various challenges which are not just limited to bank management, but also to both international and national supervisory and regulatory authorities.

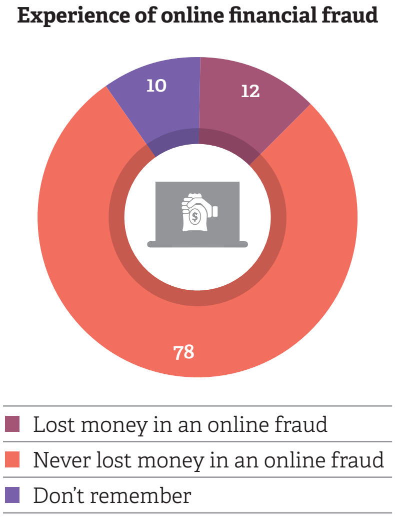
Respondents were asked if they or someone close to them had ever lost money from their bank account due to online fraud. While 12 percent reported being victims of such online frauds, over three out of four (78%) reported experiencing no such incident (Figure 8.14).

A state-wise analysis reveals that the largest share of the respondents who lost money due to an online fraud are from Haryana (30%).

With the number of online financial transactions being conducted on a daily basis globally increasing exponentially, bank frauds and cyber-crimes are also on the rise as skilled hackers keep manipulating online banking and information systems to hack into accounts. Thereby, a system of checks and measures becomes essential to not just ensure the confidentiality of customers and their data but also to ensure that they are protected against potential and harmful risks (Ali et.al., 2019).

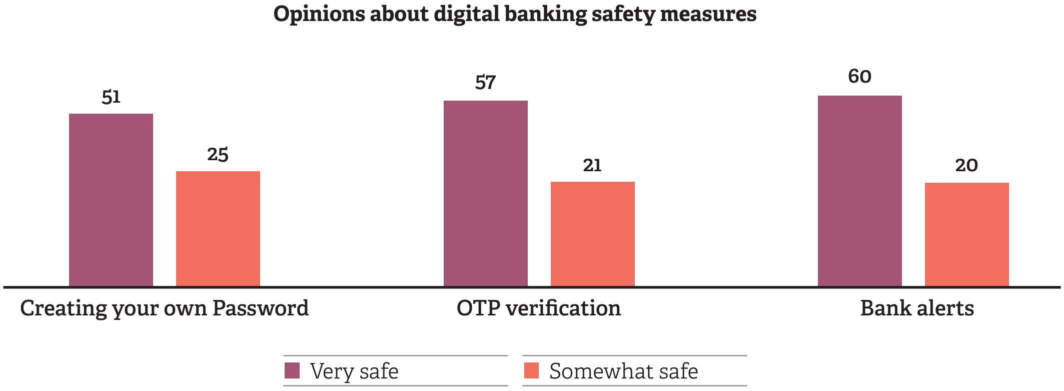
A list of measures has been adopted by digital financial applications in order to ensure customer privacy and security. The Reserve

Figure 8.14: Twelve percent respondents have been victims of online financial frauds



Note: All figures are in percentages.
Question asked: Have you or someone close to you, ever lost money from your bank account due to an online fraud?

Figure 8.15: More than half of the respondents believe that online financial safety measures such as passwords, OTPs and bank alerts are very safe



Note: All figures are in percentages.
Question asked: How safe do you think these security measures are- very, somewhat, very little or not at all safe?
a. Creating your own password according to the instructions
b. OTP verification by bank on your registered mobile/email prior to payment
c. Bank alerts for every transaction made after payments

Bank of India, as part of the public awareness initiative by the Consumer Education and Protection Department, released a booklet compiling and explaining various incidents of fraud and reporting based on the complaints received at the offices of RBI Ombudsmen to provide maximum practical information of value, especially to those who are not so experienced in digital and online financial transactions. It also emphasises the basic needs of personal information, particularly financial information confidential at all times and also warns against potential fraudulent messages, emails, and calls.

In order to assess people's opinions on safety measures adopted for digital and online financial activities, the survey asked the people how safe they thought the existing safety measures were, such as creating one's own password, OTP verification, and bank alerts. More than half the respondents were of the opinion that all the mentioned safety measures are very safe (Figure 8.15).

With one-time passwords becoming an essential element of online transactions, this common two-factor authentication is generally considered an effective deterrent against criminals and fraudsters. However, recent and increasing cases of cybercrimes have raised concerns over the effectiveness of the existing mechanism. A large number of cases have revealed multiple ways through which criminals were able to sweep through the systematic gaps and make their way to access bank details.

Conclusion

In today's world, our digital identity is becoming just as significant as our physical identity. That is why the discussions on online surveillance, intrusion, and data safety are becoming more salient. Survey data indicates several socially relevant insights into people's online behaviour and opinions about data safety.

The anxiety and concerns regarding digital and financial security span across religion, caste, age and gender boundaries. The extent differs, but there are relevant and visible concerns among the masses about their data. While in Chapter 6 we noted that people are largely supportive of surveillance by the government, findings from this chapter reveal that the same respondents are, to a great degree, concerned about the lack of safety of their personal online data, such as email accounts, social media accounts or financial information.

The survey data visibly pointed out a digital divide at various levels of urbanity, gender, caste, class, educational levels and age. There is a clear trend of the poor, non-literate, aged, SC and women respondents being less likely to both use some of the mobile banking apps or be comfortable using them. This, in a way, points to the digital marginalisation of the already marginalised. It also raises the question of the feasibility of the ongoing transition towards entirely digital financial modes, especially in the absence of equal efforts towards better financial literacy.

In addition, the findings also shed light on the state-wise distribution of the levels of concern regarding cybercrime and digital theft. The anxiety regarding an unknown person or company accessing their e-mail, social media handles and search engine history was highest in Delhi, Gujarat, Haryana, and Andhra Pradesh. As seen in Chapter 6, however, those from Gujarat were most likely to support digital surveillance by the government in various forms. This suggests that respondents who may be concerned about the security of their financial and personal information may not necessarily hold the same standards when it comes to mass surveillance by the government ostensibly for reasons of national security or public safety. Another noticeable pattern across states was that people from Karnataka were most likely to be trusting of various digital banking apps and least concerned about the online security of their personal information. This is an interesting trend, particularly in the context of Bengaluru being the IT hub of the country and also reporting the highest rates of cybercrimes in India.

Results from Haryana, on the other hand, indicate high levels of concern for digital identity and financial security. Various reports of increasing organised rings of cybercrimes have emerged from the region (Ojha & Jain, 2022), and its effects are reflected in the survey findings.

References

Ali, M., Hussin, N.& Abed, I. (2019). E-Banking Fraud Detection: A Short Review. *International Journal of Innovation, Creativity and Change*.6. 67-87.

Babu, N. (2021, September 16). Andhra Pradesh ranks seventh in cybercrimes, fraud biggest motive. *The Times of India*. Retrieved from: https://timesofindia.indiatimes.com/city/visakhapatnam/ap-ranks-seventh-in-cybercrimes-fraud-biggest-motive/articleshow/86241357.cms

Chetan, M.G. (2022, May 13). Green signal for Karnataka cyber security policy. *The New Indian Express.* Retrieved from: https://www.newindianexpress.com/states/karnataka/2022/may/13/green-signal-for-karnataka-cyber-security-policy-2452919.html

Cornelius, D. (2020, December 29). Why 'Jamtara' Connected, According to Its Co-Writer: A Clever Crime in An 'Unassuming Place'. *Scroll*. Retrieved from: https://scroll.in/reel/982656/why-jamtara-connected-according-to-its-co-writer-a-clever-crime-in-an-unassuming-place.

Digital Financial Services Security Assurance Framework 2021. (n.d.). ITU Hub. Retrieved from https://www.itu.int/hub/publication/t-tut-dfs-2021/ Accessed on 10th March 2023. Dogra, S. (2021, April 19). Over 27 million Indian adults experienced identity theft in the past 12 months, says Norton report. *India Today*. Retrieved from: https://www.indiatoday.in/technology/news/story/over-27-million-indian-adults-experienced-identity-theft-in-the-past-12-months-says-norton-report-1792553-2021-04-19. Accessed on: 8th November 2022.

Dutta, Arnab. (2018). Smartphone sales and Literacy Rates Go Hand-in-Hand in India, Reveals Study. New Delhi. *Business Standard*. Retrieved from: https://www.business-standard.com/article/technology/strong-penetration-of-smartphone-in-highest-literate-regions-study-118032301045_1.html.

Edmond, D.F. (2015, December 13). Phishing in Jamtara: What Does It Take to Carry Out Online Fraud? *The Indian Express*. Retrieved from: https://indianexpress.com/article/india/india-news-india/phishing-in-jamtara-what-does-it-take-to-carry-out-online-fraud/.

Geer, D., (2007, January 20), *Most organizations fail to manage risks associated with sharing data with third parties,* ComputerWorld. Retrieved from: https://www.computerworld.com/article/2817626/most-organizations-fail-to-manage-risks-associated-with-sharing-data-with-third-parties.html.

GSMA. (2022, June). The Mobile Gender Gap Report 2022. Retrieved from: https://www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf.

Hussain, I., & Sajjad, S. (2016). Significance of financial literacy and its implications: A discussion. Journal of Business Strategies, 10(2), 141. Iqbal, N. (2022, October 31). India's digital gender gap is stark – and it's showing. Scroll. Retrieved from: https://scroll.in/article/1036204/indias-digital-gender-gap-is-stark-and-its-showing. Accessed on: 8th November 2022.

Jha, A.M. & Upreti, P.M. (2021, June 22). Sulli Deals: Women Caught in the Tentacles of the Dark Web. *The Hindu*. Retrieved from: https://www.thehindubusinessline.com/blink/cover/sulli-deals-women-caught-in-the-tentacles-of-the-dark-web/article35460831.ece.

Livemint. (2022, May 30). FBI Report Ranks India in Top 5 Countries with Victims of Cybercrimes. Retrieved from: https://www.livemint.com/technology/tech-news/fbi-report-ranks-india-in-top-5-countries-with-victims-of-cybercrimes-11653896623002.html.

Mauthner, N.& Parry, O. (2013). Open Access Digital Data Sharing: Principles, Policies and Practices. *Social Epistemology*. 27, 47-67.

Menon, V. (2022, November 24). Mewat is India's Latest Jamtara. And Sextortion is the New Kill. *The Print.* Retrieved from: https://theprint.in/the-fineprint/mewat-is-indias-latest-jamtara-and-sextortion-is-the-new-kill/1232746/.

Ministry of Home Affairs, Government of India. (2022, July 26). Increase in Cyber Fraud Cases. Retrieved from: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2022-pdfs/LS26072022/1454.pdf.

National Crime Records Bureau. (n.d.). Ncrb.gov.in. HYPERLINK "https://ncrb.gov.in/sites/default/files/CII-%20%20%20 2021/CII_2021Volume%201.pdf" https://ncrb.gov.in/sites/default/files/CII- 2021/CII_2021Volume%201.pdf

Nielsen. (2022, May 5). Nielsen's Bharat 2.0 Study Reveals a 45% Growth in Active Internet Users in Rural India Since 2019. Mumbai, India. Retrieved from: https://www.nielsen.com/news-center/2022/nielsens-bharat-2-0-study-reveals-a-45-growth-in-active-internet-users-in-rural-india-since-2019/.

Mukherjee, S. (2020, December 19). Doxxing in India: Prevention As We Search for a Cure. *The Bastion.* Retrieved from: https://thebastion.co.in/covid-19/doxxing-in-india-prevention-as-we-search-for-a-cure/.

Niraj, S. (2022, August 30). Delhi logs over 110% rise in cybercrime cases in 2021: Report. *India Today.* Retrieved from: https://www.indiatoday.in/cities/delhi/story/delhi-logs-rise-in-cybercrime-cases-in-2021-details-here-1994389-2022-08-30.

Ojha, A. and Jain, N. (2022, October 20). Mewat Fraud Dot Com: Inside the New Epicentre of Cybercrime. *India Today*. Retrieved from: https://www.indiatoday.in/india/story/mewat-fraud-dot-com-inside-the-new-epicentre-of-cybercrime-near-delhi-2287874-2022-10-20.

Raghavan, R. (2021, December 8). Cyber fraud cases in Gujarat grew by 67% in 2020-21. *The Times of India*. Retrieved from: https://timesofindia.indiatimes.com/city/ahmedabad/cyber-fraud-cases-in-state-grew-by-67-in-2020-21/articleshow/88152757.cms.

Rajam, V., Reddy, A. B., & Banerjee, S. (2021, December). Explaining Caste-Based Digital Divide in India. *Telematics and Informatics,* 65.

Reshetnikova, Natalia & Magomedov, M & Buklanov, D. (2021). Digital Finance Technologies: Threats and Challenges to the Global and National Financial Security. IOP Conference Series: Earth and Environmental Science. 666. 062139. 10.1088/1755-1315/666/6/062139. Romansky, R. (2014). Digital Privacy in the Network World. *International Conference on Information Technologies.*

The Times of India. (2022, March 30). Cybercrime Losses Rise to Rs 63 Crore in FY20-21: Government. Retrieved from: https://timesofindia.indiatimes.com/business/india-business/cyber-crime-losses-rise-to-rs-63-crore-in-fy20-21-govt/articleshow/90532711.cms.

The Wire. (2018, October 28). Indian Children Most Cyber-Bullied in the World: Study. Retrieved from: https://thewire.in/tech/indian-children-most-cyber-bullied-in-the-world-study.

The Wire (2021, August 4). Pegasus Project: 174 Individuals Revealed by the Wire On Snoop List So Far. Retrieved from: https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance. Traynor, Patrick. (2018). Digital Finance and Data Security: How secure is data used in digital credit? Center for Financial Inclusion. Retrieved from https://www.centerforfinancialinclusion.org/digital-finance-and-data-security-2.

Chapter 9:

Privacy and Targeted Surveillance

Key findings

- Only about one in six respondents have heard about the right to privacy judgement by the Supreme Court. About one out of two persons fully agree with the judgement.
- Scheduled Tribes are most anxious about sharing GPS location with the police.
- Government employees are most anxious about sharing their location with their employers.
- One out of two respondents are concerned about the confidentiality of their medical information.
- More than two out of five respondents expressed strong support for government applications—the AarogyaSetu and CoWIN apps.
- Nearly two out of three respondents believe that political parties surveil citizens for electoral gains.

CHAPTER 9

Privacy and Targeted Surveillance

In a progressively networked and connected digital environment, the concept of privacy continues to garner increased attention. Although the idea of privacy represents distinct connotations under different jurisdictions, the rudimentary conceptualisation remains a matter of deliberation. The universal articulation of the term is thereby difficult and privacy, as a concept, is in disarray (Solove, 2008). Despite debates on its theorisation, the idea of privacy is agreed to be essential for freedom, primarily in democracies. Privacy is considered to be a significant prerequisite to achieving the most basic of fundamental rights in democratic countries such as those relating to one's own body and information.

Surveillance as an institutional tool finds its roots in history where measures were taken to monitor the actions of people for both defined and undefined purposes. One defined and crucial purpose that is often used to justify surveillance by the state, is to preserve and maintain national security. Thereby, security from threats which are both internal and external in nature becomes an impetus for surveillance. The gradual yet remarkable advancement in technology has made surveillance architecture more intrusive and threatening to individual democratic fundamentals. The state, presently, is utilising digital surveillance tools such as CCTVs and facial recognition to track the actions of the masses. This has further advanced both the degree of surveillance as well as the multiplication of the number of tools being deployed. According to a Forbes survey, New Delhi has about 1,826.6 cameras per square mile, making it the most surveilled city in the world (Shekar and Mehta, 2022).

Further, in addition to mass surveillance, the state is also encouraging lateral surveillance to motivate citizens to report 'unlawful' activities (Ibid). For instance, the Indian Cyber Coordination Centre (I4C), under the Ministry of Home Affairs launched the Cyber Crime Volunteers Program that allows citizens to register themselves as "Cyber Crime Volunteers" with the purview of identifying, reporting and removing illegal and unlawful online content. Another crucial state-sponsored form of lateral surveillance was adopted in Uttar Pradesh in the form of the C-Plan App that was launched to keep a tab on 'anti-social elements'. It was designed to receive inputs from certain identified individuals who have been given the responsibility to "solve local problems" such as providing information about emerging communal tensions or land disputes taking place in their own villages through the mobile application (NDTV, 2019).

With the advent of applications and technologies that cater to both mass and lateral surveillance, the principles of privacy stand contested. While surveillance and cyber security are gaining traction due to the increasing rates of cybercrime, they are also being seen as a major hindrance to securing individual privacy. The collection and, at times, unconsented sharing of personal data has raised a number of concerns involving scrutiny which may place specific communities at a higher risk and much greater disadvantage than others. The heightened risk of targeted surveillance has further increased concerns over the privacy and safety of marginalised groups and communities and hints towards the absence of a robust surveillance framework that sets in place the prerequisites for both privacy and surveillance techniques.

With the advancement in surveillance technologies, the fear of privacy and data protection is increasing. The networked societies that we live in make data collection in today's world inevitable. However, this has also given rise to apprehensions around data storage, third-party interference, and intrusion into one's life, placing citizens under constant watch, with or without substantial suspicion of them posing a threat to national security. For instance, the Pegasus snooping scandal revealed that hacking and tapping operations might take place without the target even possessing any information about infringement. Pegasus spyware infected nearly 300 phone numbers in India, which largely belonged to human rights activists, journalists, ministers and opposition leaders (Indian Express, 2021).

The regularity and increased presence of surveillance technologies at both national and international levels are raising significant concerns over violations of human rights and the failure of state protection systems. In order to understand the customary presence of surveillance technologies by different institutions across the country, this study attempts to understand public opinion and anxiety related to multiple variations of surveillance techniques. The following chapter focuses on privacy and its corroborative experience across people in different communities.

- **Section 1** analyses awareness surrounding privacy and its legal framework in the country. It also focuses on reporting the respondents' opinion on the right to privacy along with their agreement/disagreement on the judgement.
- **Section 2** focuses on the nuanced interconnection between technology and privacy. The study focuses on GPS technology and looks at the degree of anxiety expressed by the respondents while sharing their location with various individuals and organisations.
- **Section 3** aims to look at the response of the population when it comes to disclosing personal data and information and also sharing device access in multiple forms.
- **Section 4** explores the growing and increasingly digitised medical sector with a comparative analysis of government and private sector ventures in the field. In a post-pandemic world, we look at the level of anxiety while sharing medical information with telemedicine and pharmacy.
- **Section 5** analyses the level of institutional and organisational surveillance and the awareness surrounding it.
- **Section 6** attempts to speculate on the prospective focus on distinct communities and discuss the concept of targeted community surveillance.

9.1. Privacy: Notion and framework

McLuhan's (1962) idea of a global village is becoming more salient in today's deeply networked world. It is also becoming an influential notion across nations as a governance practice. The United Nations Conference on Trade and Development Global Cyberlaw Tracker, in an attempt to globally map cyber laws, focuses on, "e-commerce legislation in the field of e-tractions, consumer protection, data protection/privacy and crime adoption in the 194 UNCTAD member states". Among its concerns are also issues regarding the collection, usage and sharing of data and especially personal information with third parties without notice or consent of the individuals. According to the report, 137 out of

Table 9.1: Only about one in six respondents have heard about the right to privacy judgement by the Supreme Court

State	Heard about the Puttaswamy judgement
Overall	**16**
Karnataka	33
Andhra Pradesh	28
Kerala	18
Maharashtra	17
Haryana	16
NCT Of Delhi	16
Uttar Pradesh	16
West Bengal	15
Tamil Nadu	13
Punjab	12
Gujarat	8
Assam	7

Note: All figures are in percentages. Rest did not hear.
Question asked: Do you know about the Supreme Court case of 2017, Puttuswamy vs Union of India, which declared privacy as a fundamental right?

194 countries have legislation in place for data protection and privacy.

India is a signatory both to the Universal Declaration of Human Rights (UDHR, Article 12) and the International Convention on Civil and Political Rights (ICCPR, Article 17), both of which recognise privacy as a fundamental right. In terms of a national approach, the right to privacy was recognised by the Indian Supreme Court in the 2017 *Puttaswamy and Anr. Vs. Union of India and Ors judgement*. The nine-judge bench held that the right to privacy is protected as a fundamental right under the Constitution of India. Despite being a landmark judgement, more than four out of five (84%) of the respondents surveyed were not aware of it. Those who were most aware belonged to the age bracket of 26 to 35 years. Further, the highest level of awareness about the judgement was in Karnataka, where one-third of the respondents had heard of the judgement (33%), followed by Kerala (18%) and the state where people were the least aware was Assam (less than one in every ten, i.e., 7%) (Table 9.1). One reason for the greater awareness in Karnataka could be due to the fact the petition was filed by Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court.

When it comes to the religious concentration of those who were aware of the judgement, the Christian, Hindu and Sikh communities were almost at the same level of awareness, while those who were least aware were Muslims (10%). The data also suggests that people having a higher level of educational attainment and those belonging to upper economic classes were more likely to be aware of the judgement (Table 9.2).

Table 9.2: Those belonging to the upper class and with college and above level of educational attainment are most likely to have heard about the Puttaswamy judgement

	Heard about Puttaswamy judgement
Poor	7
Lower	14
Middle	19
Upper	28
Non Literate	3
Upto Primary	5
Upto Matric	7
Intermediate-under graduate	11
College and above	26

Note: All figures are in percentages.
Question asked: Do you know about the Supreme Court case of 2017, Puttuswamy vs Union of India, which declared privacy as a fundamental right?

Additionally, of those who have heard about the judgement, nearly half of them (48%) fully agree that privacy is a fundamental right and a little over one in three (36%) somewhat agree with the judgement. Seventy percent of respondents from the NCT of Delhi fully agreed with the judgement, which was the highest among all states. Despite the fact that the state had the highest level of awareness about the judgement, the percentage share for those who fully agreed with the judgement was the lowest in Karnataka (17%).

Table 9.3: About one out of two persons fully agrees with the Supreme Court judgement on right to privacy

State	Level of agreement			
	Fully agree	Somewhat agree	Somewhat disagree	Completely disagree
Overall	**48**	**36**	**8**	**3**
NCT Of Delhi	70	24	1	1
Kerala	62	24	2	2
Haryana	61	31	6	1
West Bengal	60	26	8	2
Uttar Pradesh	56	30	2	
Andhra Pradesh	52	42	3	1
Gujarat	52	39	3	3
Tamil Nadu	48	35	11	1
Punjab	47	36	1	2
Maharashtra	34	19	27	12
Assam	32	51	11	2
Karnataka	17	62	14	4

Note: All figures are in percentages. Rest did not respond. (n=1607)
Question asked: To what extent do you agree or disagree with the judgement?

There was also a difference in agreement with the *Puttaswamy* judgment among those who were non-users of digital platforms such as social media, internet or email (refer to Index 1 in Appendix 5) with those who used digital platforms. While 39 percent of those who were non-users of digital platforms fully agreed with the judgement, about one out of two respondents (49%) among those who used the digital platforms fully agreed with the judgement (Table 9.4).

Table 9.4: Users of digital platforms are more likely to support the Supreme Court judgement on the right to privacy, compared to non-users

	Level of agreement			
	Fully agree	Somewhat agree	Somewhat disagree	Completely disagree
Non-user of digital platforms	39	38	11	5
Users of digital platforms	49	36	7	2

Note: All figures are in percentages. Rest did not respond. (n=1607)
Question asked: To what extent do you agree or disagree with the judgement?

9.2. Tracking and privacy

Data collection in today's world is ubiquitous (Bajaj, 2010). Surveillance in modern societies is becoming an increasingly crucial governing tactic for state authorities, corporations and individuals. The rationale behind data-driven security practices is that harvesting personal and meta-data would allow authorities to intervene in targeted intelligence-led activities, focus their resources on emerging threats, and avoid their occurrence (Friedewald, 2017).

Location becomes an essential factor in surveillance and the geographical profiling of individuals. The Global Positioning System (GPS) is increasingly being adopted by private and public organisations to track and monitor individuals for location-based services. The miniaturisation of the GPS chipset has also allowed for its usage in relatively smaller devices such as wristwatches, mobiles and bracelets. However, the ethical considerations behind this monitoring raise rather complex concerns, especially with third-party involvement. However, most ethical issues in GPS tracking pertain to control as a rather intrusive method of supervision (Michael et.al., 2006). A common justification for the usage of GPS tracking is to help prevent criminal acts. This includes checks on suspected offenders such as criminals, and terrorists but it also involves employee monitoring. We asked our respondents how anxious or not they would be while sharing their location with the following institutions/people and received the following responses.

9.2.1. Police

The survey found that a little over one-third (36%) of people felt anxious while sharing their location with the police. When it comes to the caste constitution of those who feel anxious, Scheduled Tribes are the most apprehensive about sharing location data with the police (49%) (Table 9.5).

Some of the findings of our past report, SPIR 2018: A Study of Performance and Perceptions, suggest that STs hold the most negative perception of the police across caste categories and are most likely to face police harassment. They are also more likely to associate greater police presence with the fear of being wrongfully implicated, indicating a taut relationship between the community and the police. Thus, greater apprehension within this community regarding the sharing of location data with the police falls in line with our past findings of STs and other vulnerable groups being more anxious about police contact.

A state-wise analysis reveals that nearly 36 percent of respondents from Karnataka were

Table 9.5. Scheduled Tribes are most anxious about sharing GPS location with the police

Caste Community	Very Anxious	Somewhat Anxious	Very little	Not at all	Can't say
Overall	**21**	**15**	**9**	**17**	**4**
Scheduled Castes	20	15	7	12	6
Scheduled Tribes	28	21	10	12	8
Other Backward Classes	21	13	10	18	4
General	21	16	8	19	4

Note: All figures are in percentages. Rest reportedly have never shared their locations with police
Question asked: How anxious do you feel while sharing your GPS location with the police - very anxious, somewhat anxious, very little or not at all anxious?

very anxious while sharing their GPS location with the police, followed by Tamil Nadu (26%). On the other hand, respondents from Kerala were the least anxious about sharing their location (Table 9.6).

9.2.2. Food delivery apps

With the ever-expanding market of services, food delivery is now a billion-dollar industry. Although the e-commerce industry continues to grow and expand, the customer base has only expanded in the past few years. An essential feature of the industry remains food delivery at the doorstep and quite often, it requires access to one's GPS location.

When questioned about their anxiety when it comes to sharing their GPS location with a food delivery app, around 31 percent of respondents felt some level of anxiety; though nearly 30 percent of people said they never shared their location with such apps (Table 9.7). What was also particularly significant was that people from mid-sized cities were not as anxious as those from small and capital cities (Table 9.5).

Table 9.6: Respondents from Karnataka most anxious about sharing their GPS location with the police

	Very Anxious	Somewhat	Very little	Not at all
Karnataka	36	26	12	8
Tamil Nadu	26	19	12	15
West Bengal	20	17	4	8
NCT Of Delhi	20	17	12	16
Punjab	21	17	7	17
Haryana	29	17	9	22
Assam	18	16	8	8
Maharashtra	29	14	11	14
Uttar Pradesh	20	12	7	9
Andhra Pradesh	10	11	4	25
Kerala	6	6	9	33
Gujarat	19	6	8	28

Note: All figures are in percentages. Rest reportedly have never shared their locations with police
Question asked: How anxious do you feel while sharing your GPS location with the police - very anxious, somewhat anxious, very little or not at all anxious?

Table 9.7. More than one-third of respondents from capital cities were anxious while sharing their location with food delivery apps

Type of city	Very	Somewhat	Very little	Not at all	Can't say	Never shared
Overall	**12**	**19**	**15**	**20**	**6**	**28**
Capital City	18	17	12	23	4	26
Mid-sized City	8	21	18	19	6	28
Small City	11	18	16	18	6	31

Note: All figures are in percentages.
Question asked: How anxious do you feel while sharing your GPS location with apps such as Swiggy, Zomato, Amazon etc. - very anxious, somewhat anxious, very little or not at all anxious?

9.2.3. Family/Spouse

When it came to sharing their GPS location with their spouse or family members, around one-fourth of the respondents (26%) expressed some form of anxiety while about one in three (33%) expressed no form of anxiety. However, a little over a quarter (27%) said that they never shared their locations with their family or spouse. Out of those who felt some form of anxiety about sharing their location, the difference between men (27%) and women (24%) was not that significant. But 30 percent of the women said that they never shared their GPS location with their families or spouse. A possible reason for this could be that women don't use phone (smartphones) as much as their male counterparts (Table 9.8). In a report 'Media in India' (Lokniti-CSDS, 2022) it was found that 44 percent of the survey women don't have their own phones; though one in three women use smartphones whereas a quarter has a basic phone. On the contrary, more than half (54%) of the surveyed men claimed to use smartphones.

9.2.4. Employer

Of those surveyed, nearly 40 percent have never shared their location with their employer; and hence did not feel anxious about it. However, about one-fourth (25%) have felt some level of anxiety while sharing their location with their employers (Table 9.9). Of them, the highest percentage of people are government employees (30%). A potential reason why anxiety levels among government employees are higher than others could be due to the fact that post removal of the Covid-19 lockdown restrictions, the Department of Personnel and Training (DoPT) has resumed the marking of attendance through the Aadhaar-Enabled Biometric Attendance Control System (AEBAS) (IANS, 2022).

Table 9.8. One out of four people are anxious about sharing their GPS location with their family or spouse

Gender	Very	Somewhat	Very little	Not at all	Can't say	Never shared
Overall	**16**	**10**	**9**	**32**	**6**	**27**
Men	16	11	9	33	6	25
Women	15	9	9	31	6	30

Note: All figures are in percentages.
Question asked: How anxious do you feel while sharing your GPS location with family/Spouse - very anxious, somewhat anxious, very little or not at all anxious?

Table 9.9. Government employees are most anxious about sharing their location with their employers

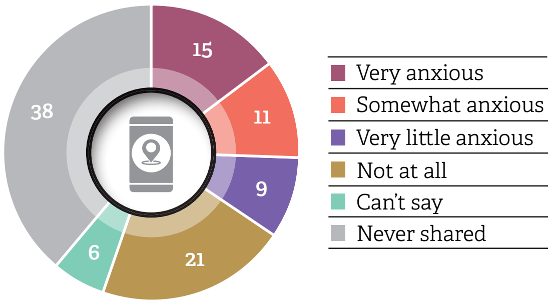
Occupation	Very Anxious	Somewhat Anxious	Very little	Not at all	Can't say	Never shared
Overall	**11**	**14**	**12**	**19**	**6**	**38**
Business	11	17	13	20	7	32
Farmers	7	13	11	19	8	42
Government Employees	15	15	15	23	5	27
Housewives/stay at home	7	11	11	14	7	50
Other Occupations	12	13	11	13	6	45
Professionals	13	18	14	25	6	24
Labourer	10	10	10	16	8	46
Students	10	16	13	21	7	33

Note: All figures are in percentages.
Question asked: How anxious do you feel while sharing your GPS location with employer - very anxious, somewhat anxious, very little or not at all anxious?

9.2.5. Female safety apps

With reported crimes against women increasing annually and reaching a six-year high in 2021 (NCRB, 2016-2021), safety applications have emerged as a one-click solution for women during any emergency. Both government, as well as private companies, have developed mobile applications for women's safety. For instance, the *Himmat* app was launched by the Delhi Police. The findings on this question present an ironical conundrum where in order to ensure their safety, women are expected to surrender their location-related privacy. This dilemma is also reflected in the responses of the women, as 15 percent feel very anxious while sharing their location with such apps. However, these are relatively newer technologies, and 38 percent of the female respondents have never shared their locations on these apps and therefore not shared their opinion too on this question (Figure 9.1).

Figure 9.1. Close to one in six women felt very anxious while sharing their GPS location with a female-safety mobile application

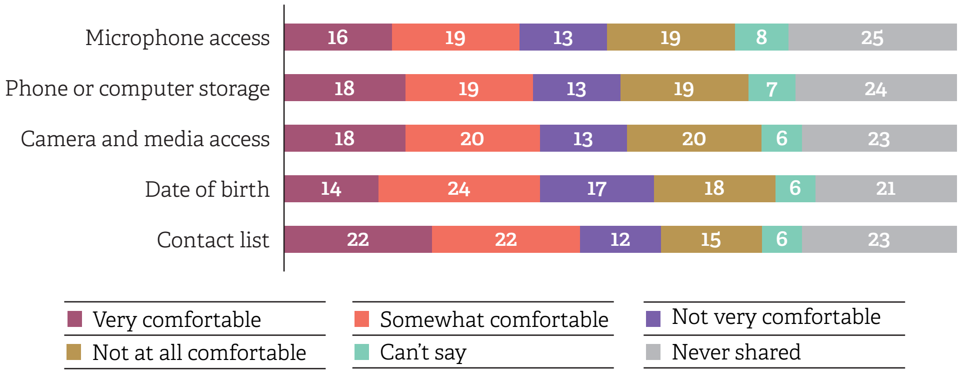


Note: All figures are in percentages. N=3994
Question asked: (Only female respondents were asked) How anxious do you feel while sharing your GPS location with apps that ensure women's safety - very anxious, somewhat anxious, very little or not at all anxious?

9.3. Personal data and device access

In India, there is no comprehensive set of privacy rights that address data collection, use, and disclosure. While information privacy and surveillance are becoming areas of concern due to their relation to various forms of cybercrimes, mass surveillance can also hinder larger democratic processes and impact human dignity and personal rights. With growing interest in the internet and associated surveillance technology developments, the collection and retention of mass information from users have also given rise to the concern for privacy. The discourse around privacy thereby represents the way the information

Figure 9.2: On an average close to one in three felt uncomfortable while sharing their device information with apps or websites



Note: All figures are in percentages.
Question asked: How comfortable do you feel while sharing your contact list with an app or website on your phone or computer - very comfortable, somewhat comfortable, very little or not at all comfortable?

is handled and information is used. This implies its further connection to data security and protection when it comes to consumer information. The risk dimension of privacy is known as "intimacy risk" which concerns itself with how commercial endeavours utilise data for their own interests and financial gain. It also includes how the customer database is sold to third parties which consequently exposes customers to unwanted advertising (Malakar & Choudhary 2020).

With the increasing accessibility of internet connectivity and lower costs of internet data as compared to other markets across the world, India is becoming the leading consumer of cyber information in the world today. However, what is also evident is the absence of any legal framework that deals with commercial data collection, storage and transfer. This, therefore, poses a difficult challenge with reference to data security.

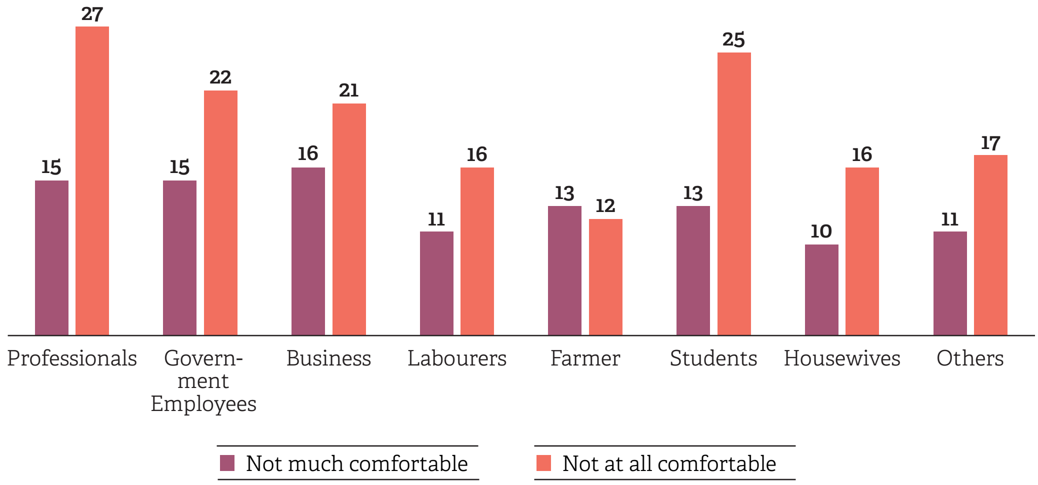
Several websites, mobile applications and other web domains seek access to personal data in multiple forms, either through location access, camera access, storage access or contact list access. In this sub-section, we report common people's opinions about sharing such data.

While sharing their contact list with an application or website about a little over one-fourths (27%) of those surveyed felt some level of discomfort (very and somewhat categories are clubbed). When it came to phone and computer storage, around one-third (32%) of those surveyed expressed some level of discomfort while giving applications and websites access to their phone and computer storage and exactly the same proportion felt some level of discomfort while sharing access to their microphone (32%) and camera and media (33%) access respectively (Figure 9.2).

There has been a rise in applications and websites which essentially have a more interactive interface with the audience. A prominent feature of these websites and applications is access to the devices' storage which includes the camera and media access. For the survey, those who felt some amount of discomfort while sharing their data constituted about one-third of the total population. Analysing this group further revealed that the highest level of discomfort in sharing device storage access was reported by working professionals (42%), followed by students (38%) and then government officials and business persons (37%) (Figure 9.3).

Sharing of date of birth information with applications and website is a significant aspect of personal data sharing. This allows companies to get a greater, more in-depth sense of their consumer base. Information regarding the birth date of an individual could lead to a very significant form of identity theft. The

Figure 9.3: Working professionals are most uncomfortable sharing their camera and media access with websites and applications



Note: All the figures are in percentages.
Question asked: How comfortable do you feel while sharing your camera and media access with an app or website on your phone or computer - very comfortable, somewhat comfortable, very little or not at all comfortable?

date of birth falls in the category of Personally Identifiable Information (PII) i.e. information or data that when used alone or with other relevant data, can identify an individual (Chellappan & Kannan, 2021). PII consists of direct indicators which could identify a person such as their passport information or national identity cards. However, it also entails quasi-identifiers such as race or gender, which when combined with other quasi-identifiers help in successfully identifying an individual. For instance, in the United States, there are four personal data points, that when used together, would make for identity theft. This includes one's name, address, date of birth and social security number. It is for this very reason that date of birth is often used by banks and hospitals to verify one's identity. In this survey, about one out of three respondents (35%) felt some level of discomfort while sharing their date of birth (Figure 9.2).

9.4. Medical information

Medical history and details constitute an essential component of one's personal details. The ability to process the data of thousands of patients automatically has been a pertinent addition for many healthcare providers and facilities. For data miners, it poses two sets of options, either anonymising patient information or just making it available to physicians alone. While doctor-patient confidentiality is a very crucial part of the medical field, it is not a universal rule or law across every country. Now, with the increased presence of other stakeholders, agencies and service providers such as external pathology laboratories, insurers and pharmaceutical manufacturers, it poses a moral dilemma when it comes to the personal data of patients. Similarly, anonymising information can also prove to be ineffective as sometimes the de-identified information may also be traced back to the individual. Another matter of concern here is that the rising administrative costs of data processing in developed countries have also resulted in the outsourcing of patient information to under-regulated jurisdictions (Srinivas and Biswas, 2012).

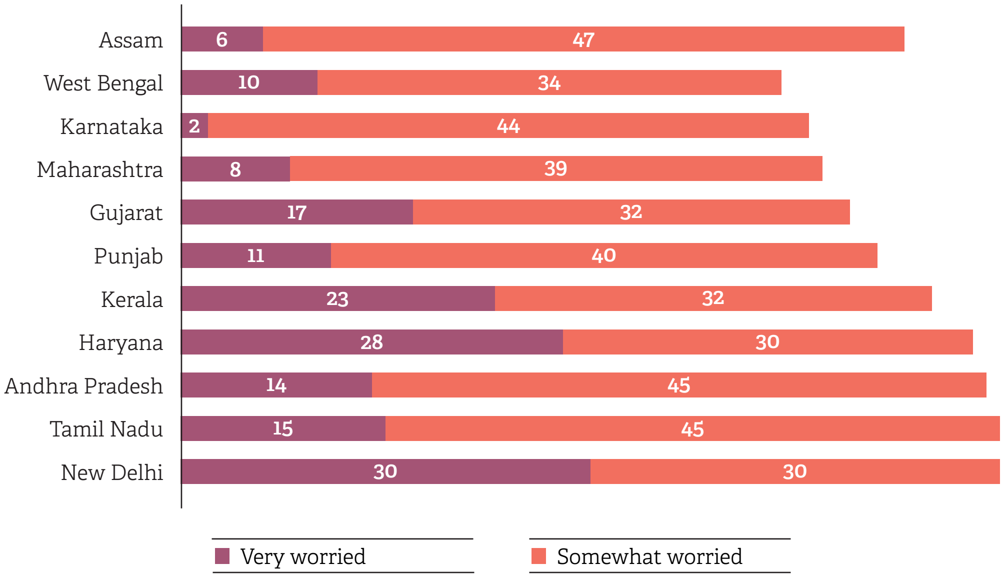
Respondents were asked about the level of anxiety pertaining to the confidentiality of their medical information. More than half the respondents were worried to some extent that their medical information could be shared with other institutions and organisations. Across occupations, working professionals were most concerned about the status of their medical information (59%), followed by farmers and students (Table 9.10).

Table 9.10: One out of two respondents is concerned about the confidentiality of their medical information

Occupation	Very worried	Somewhat worried	Least Worried	Not at all	Can't say
Overall	**15**	**37**	**21**	**16**	**11**
Business	13	43	21	13	10
Farmers	16	38	20	11	15
Government Employees	13	41	25	15	6
Housewife/Stay at home	16	34	19	21	10
Other occupations	13	32	20	22	13
Professionals	19	40	21	15	5
Labourer	15	33	22	17	13
Students	15	39	22	16	8

Note: All figures are in percentages.
Question asked: How worried do you feel that the medical information provided by you to the hospitals/doctors can be shared with other companies or institutions– very worried, somewhat worried, least worried or not at all worried?

Figure 9.4: Respondents from Delhi and Tamil Nadu most worried about the confidentiality of their medical information



Note: All figures are in percentages.
Question asked: How worried do you feel that the medical information provided by you to the hospitals/doctors can be shared with other companies or institutions– very worried, somewhat worried, least worried or not at all worried?

9.4.1. Government applications/websites

With the onset of the Covid-19 pandemic, a major challenge was to track and trace the spread of the virus, so as to take essential precautionary measures. Most of this was regionally focused. All over the world, technology was being used in the form of contact tracing applications by governments to control the spread of the virus. A similar application was introduced by the Government of India, namely, Aarogya Setu, the National Health Application. Launched on 2nd April 2020, Aarogya Setu is aimed at, "contract tracing, syndromic mapping and self-assessment". Based on a digital interface, it is a mobile app developed by the National

Informatics Centre under the Ministry of Electronics and Information Technology. The Aarogya Setu Data access and knowledge sharing protocol was issued to ensure,

> ***"The secure collection of data by the Aarogya Setu mobile application, protection of personal data of individuals, and the efficient use and sharing of personal or non-personal data for mitigation and redressal of the COVID-19 pandemic."***
> (Government of India, Ministry of Electronics and Information technology, National Informatics Centre, 2021)

When asked for their opinion regarding this app, over 50 percent of respondents felt some level of comfort while sharing their medical history with the Aarogya Setu App. Quite a significant chunk of these were people in government jobs (72%) and mainly constituted men (61%). Further, around 70 percent of those who felt some level of comfort while sharing their medical history lived in a rich household. In contrast, those who felt a certain level of discomfort while sharing their medical history with the Aarogya Setu App belonged to a lower-income household (14%).

Another major by-product of the Covid-19 management strategy was the launch of another significant web portal by the Indian government, namely, CoWIN. Launched by the Ministry of Health and Family Welfare, the major driving idea behind the digital portal is the participation of healthcare providers in providing access to Covid-19 immunisation. It allows individuals to book vaccination slots area-wise and also provides an e-certificate for the vaccination which has now become an essential document, especially for travelling.

Out of those surveyed, a little less than two-thirds (62%) were comfortable sharing their medical history with CoWIN. Respondents from Karnataka (82%) were most comfortable with sharing their information on the portal. Similar to Aarogya Setu, government employees were the most comfortable with sharing their medical history (75%) on the CoWIN portal.

A major trend that could be observed was that those who are more educated are also more likely to be comfortable sharing their medical information with either the Aarogya Setu app or the CoWIN portal whereas respondents having no education or with lower educational attainment were more likely to say that they never used these applications.

9.4.2. Private applications

With the e-commerce boom taking over the world, India is no exception. In 2022, India's e-commerce market is expected to increase by 21.5 percent reaching USD 74.8 billion. Further, India's e-commerce market is expected to reach USD 350 billion by 2030. The overall commerce market in India is expected to reach USD 60 billion by FY27 (Indian Brand Equity Foundation, 2022).

The private sector seems to have applications that allow for remote patient diagnosis and collaboration. This accessibility has allowed for a more integrated healthcare system where doctors and patients are very closely linked in real-time through a digital interface.

Table 9.11: More than two out of five respondents expressed strong support for government applications

App/website	Very	Somewhat	Very little	Not at all	Can't say	Never used
Aarogya Setu	40	18	8	5	3	26
CoWIN	44	18	5	5	4	24

Note: All figures are in percentages.
Question asked: How comfortable do you feel sharing your medical history while using the following apps/websites - very comfortable, somewhat comfortable, little or not at all comfortable?

These telemedicine applications allow for quicker consultations and even the booking of diagnostic tests.

We asked our respondents how comfortable they felt sharing their medical history with applications such as Practo, Lybrate, Mfine etc. A significant proportion of the respondents (48%) have never used any telemedicine applications. Kerala stands out among the states in terms of those who have never used any telemedicine applications; close to four out of five (79%) respondents from Kerala said they never used this platform.

During the pandemic, there has been a substantial rise in the purchase of consumer goods online and also in terms of delivery services. The pandemic pushed the sales of fast-moving consumer goods online. According to Kantar Worldpanel, about 10.7 million households bought these products between April 2020 and March 2022. With mobility being restricted and store opening schedules being regulated, more consumers moved to online shopping. This prompted the categories such as medical services to also go digital and expand their consumer base.

We asked our respondents if they are comfortable sharing their medical history with pharmacy applications such as PharmEasy, Tata 1mg, Apollo Pharmacy and the like. Similar to previous findings, nearly half (47%) have never used the applications or related services before (Table 9.12).

As with telemedicine apps, nearly four of five respondents from Kerala (78%) have never used any pharmacy applications. This could perhaps be attributed to Kerala's healthcare model, which relies more on state services than private players (Chathukulam & Tharamangalam, 2021). The state government also provides free medicines through public healthcare centres.

9.5. Institutional surveillance

The greater availability and accessibility of information across countries have given rise to more informed and aware citizens. This ability of citizens to process large amounts of information has not only enabled them to make well-informed choices but has also opened possibilities for political parties to contribute to this information pool and motivate the decision-making power of the voter base. For instance, the success of the Obama campaign in 2008 and 2012 in USA and the use of advanced technologies to target voters was centred on its remarkable ability to capture the profile personal data of the American voting public and tailor specific messages in multiple formats (Bennett, 2013).

This "voter surveillance" has further motivated political counterparts in other countries to find and target potential voters. The micro-targeting of voters has been supported by parties and candidates in democratic countries on the basis of spreading relevant political messages for voter education and mobilisation. Political parties have for years, legally, maintained membership lists. However, voter management databases are a more recent phenomenon and are tailored to cater to a broader range of voters. Recently, voter databases have become essential to many aspects of elections— campaigning, fundraising and garnering support for governing practices *(Ibid)*.

Table 9.12: Almost half of the respondents have never used any private telemedicine or pharmacy application

Type of applications	Very	Somewhat	Very little	Not at all	Can't say	Never used
Telemedicine	16	13	10	7	6	48
Pharmacy	16	14	10	7	6	47

Note: All figures are in percentages.
Question asked: How comfortable do you feel sharing your medical history while using the following apps/websites - very comfortable, somewhat comfortable, little or not at all comfortable?

While in countries where privacy is a stricter and more well-defined legally, it provides a stronger basis for arguing against electoral surveillance and information databases. However, elsewhere, it falls within a very grey ambit of ambiguity, argued as a necessary prerequisite for electoral and voting information. This also gives rise to concerns regarding unsanctioned access to people's data and information.

In this survey, we asked respondents if they felt that political parties view their photos, messages, videos or searched objects from their phones or computers. A little less than two-thirds, about 65 percent, disagreed. Additionally, out of the 16 percent that agreed, a significant proportion of 27 percent belonged to Gujarat and Karnataka. Conversely, a significant proportion of respondents from Kerala (83%) and Tamil Nadu (74%) disagreed that political parties can view their data (Table 9.13).

The use of big data is gradually becoming a very significant tool for political parties, especially in democratic countries where elections play a chief role. We asked our respondents to what extent they think that political parties use surveillance and snooping techniques for winning elections. The majority of the respondents, about 62 percent believe that political parties use surveillance to some extent. In order to analyse the role played by third parties or other stakeholders in influencing electoral processes, when respondents were asked whether they think that private companies or NGOs collect common people's data in order to influence their electoral choices. About 56 percent agreed that private companies and NGOs collect data and influence people's electoral choices. When further asked to what extent people think that private companies, NGOs and political parties work together to spread fake news on the internet in the country, a significant proportion (57%) agreed with the statement. The study also asked respondents if they think that the elected government of the country could snoop on its citizens illegally, and around 48 percent of the respondents agreed (Figure 9.5).

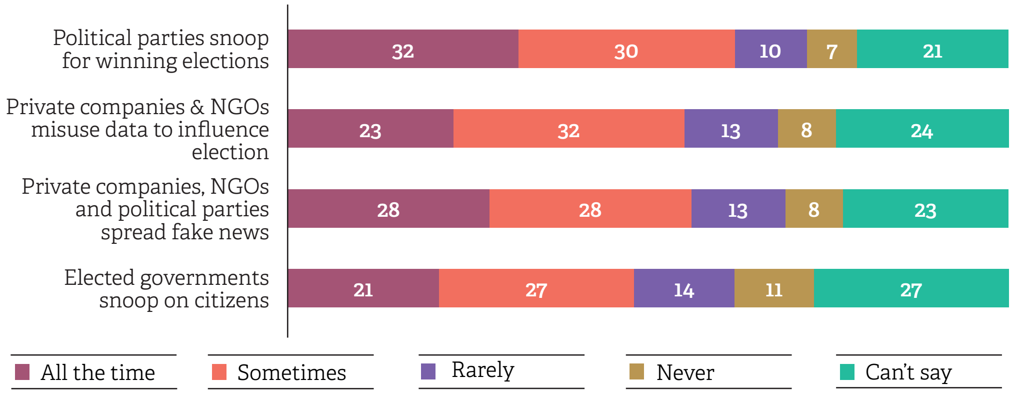
Respondents from Kerala (78%), followed by Delhi and Andhra Pradesh (77%) were most likely to agree that political parties use

Table 9.13: Two out of three people believe that political parties cannot view personal content on phone

	Political parties can view personal content on phone	Political parties cannot view personal content on phone	Can't say
All	**16**	**65**	**19**
Gujarat	27	52	21
Karnataka	27	67	6
NCT Of Delhi	22	64	14
Haryana	19	66	15
Uttar Pradesh	18	53	29
Tamil Nadu	18	74	8
Andhra Pradesh	12	53	35
Assam	11	67	22
Maharashtra	11	65	24
Punjab	11	68	21
West Bengal	10	69	21
Kerala	4	83	13

Note: All figures are in percentages.
Question asked: Do you think political parties can view your photos, messages, videos or searched objects from your phone or computer without your knowledge or consent?

Figure 9.5: Nearly two out of three respondents believe that political parties surveil citizens for electoral gains



Note: All figures are in percentage.
Question asked: To what extent do you think these things happen in our country - all the time, sometimes, rarely or never
a. Political parties use surveillance and snooping techniques for winning elections
b. Private companies or NGOs collect common people's data in order to influence their electoral choices
c. Private companies, NGOs and political parties work together to spread fake news on the internet
d. Elected governments of country snoop on their own citizens illegally

surveillance and snooping techniques to win elections. The state where the maximum number of respondents, (approximately three out of four) agreed that private companies, NGOs and political parties work together to spread fake news on the internet in the country were also from Kerala and Andhra Pradesh respectively (Table 9.14).

Table 9.14: Respondents from Kerala and Andhra Pradesh most likely to believe that various agencies snoop on voters

	Political parties snoop for winning elections	Private companies & NGOs misuse data to influence election	Private companies, NGOs and political parties spread fake news	Elected governments snoop on citizens
Kerala	78	66	73	56
Andhra Pradesh	76	68	72	56
NCT Of Delhi	72	64	67	50
Haryana	71	63	65	54
Punjab	67	64	66	62
Tamil Nadu	65	59	54	53
Uttar Pradesh	64	53	51	44
Maharashtra	60	56	58	45
West Bengal	59	49	56	46
Karnataka	57	50	45	55
Gujarat	48	45	42	35
Assam	32	23	25	21

Note: All figures are in percentage. Figures are only for those who said all the times and sometimes.
Question asked: To what extent do you think these things happen in our country - all the time, sometimes, rarely or never
a. Political parties use surveillance and snooping techniques for winning elections
b. Private companies or NGOs collect common people's data in order to influence their electoral choices
c. Private companies, NGOs and political parties work together to spread fake news on the internet
d. Elected governments of country snoop on their own citizens illegally

9.6. Targeted surveillance

In the past few years, police in several Indian states have regularised the use of fingerprint and facial recognition technology (FRT) to screen people on grounds of suspicion. From polling booths, public spaces, and public transport systems, to schools and hospitals, there has been a rapid increase in the installation and usage of CCTV and FRT on both adults and children (Mahapatra, 2021).

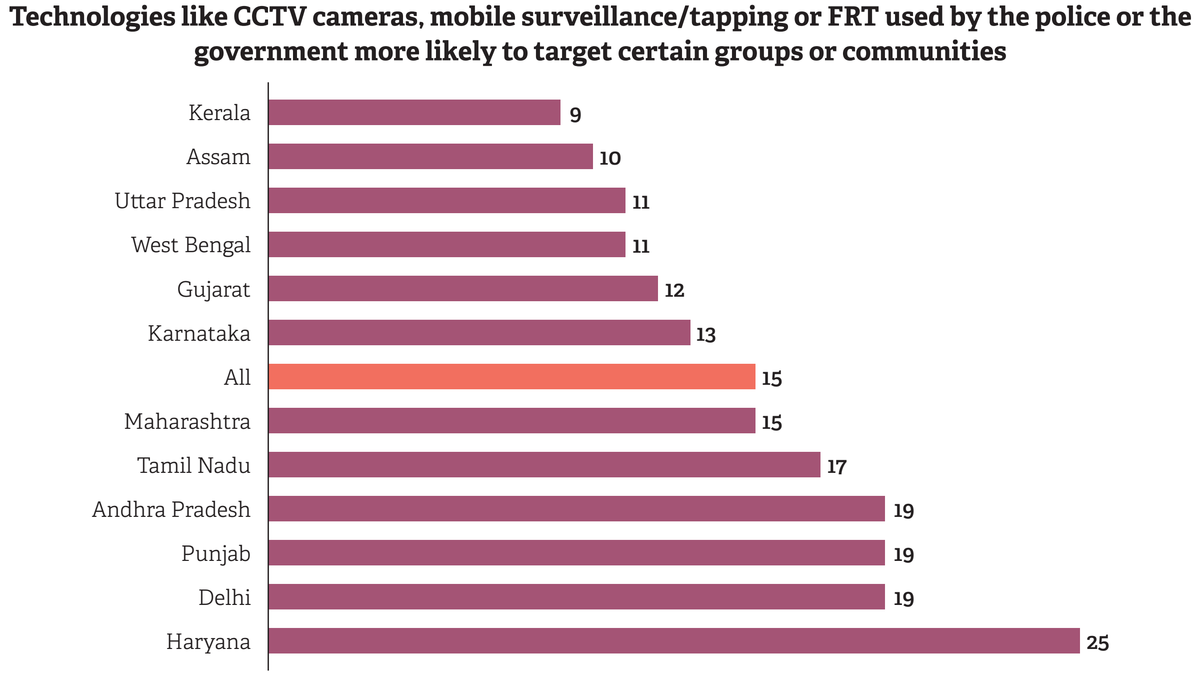
A significant aspect of mass surveillance is security which also involves policing. Thereby, digital surveillance enables dragnet surveillance which in turn makes everyone a suspect (Ibid). In recent years, many countries have begun to use more advanced digital and technical tools for censorship and surveillance. Advancements in information and communication technology (ICT) have not only transformed economic, political and social life but have also had a significant impact on every single individual in the world.

We asked our respondents if they feel that technologies like CCTV cameras, mobile surveillance/tapping or FRT used by the police or the government are more likely to target certain groups or communities. While half of the respondents disagreed, around 15 percent agreed, and 35 percent did not respond. A state-wise bifurcation reveals that nearly one-fourth (25%) of the respondents from Haryana, highest proportion across states, agreed that technologies like CCTV cameras, mobile surveillance/tapping or FRT used by the police or the government are more likely to target certain groups or communities (Figure 9.6).

For the respondents who agreed that technologies like CCTV cameras, mobile surveillance/tapping or FRT used by the police or the government are more likely to target certain groups or communities, we further asked which communities they think are more likely to be targeted. The most common response, 12 percent, stated that they feel that Muslims are more likely to be targeted. This was followed by criminals and anti-government/rebels, at nine percent.

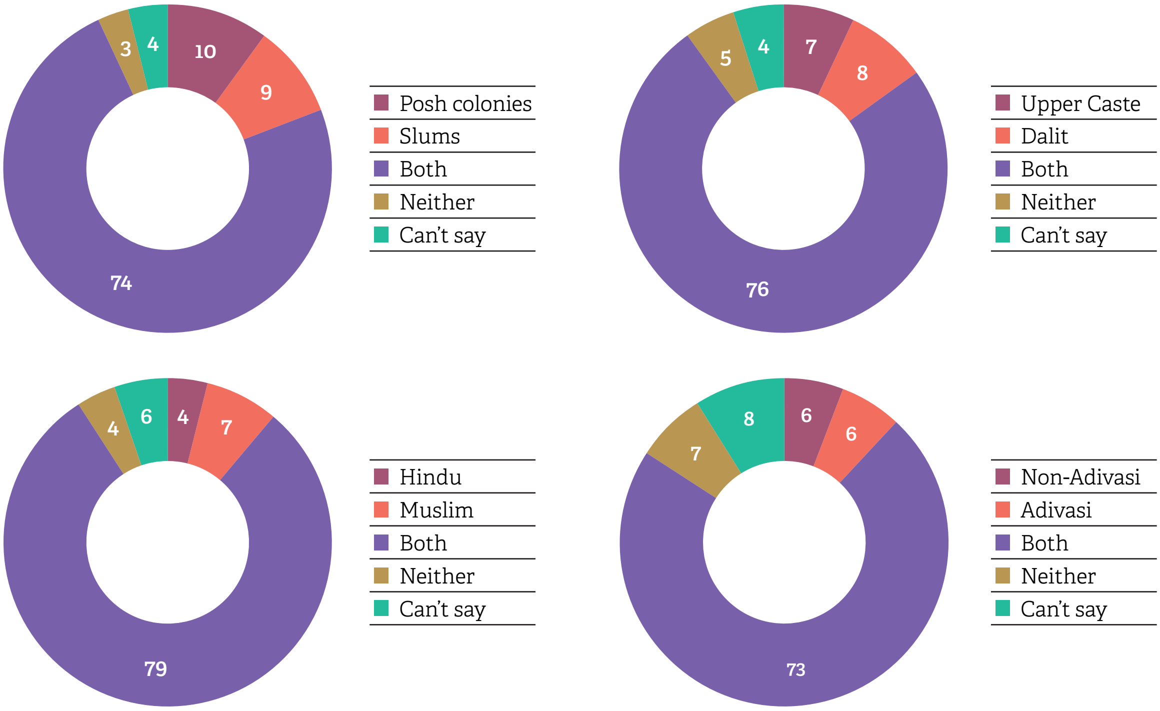
When it comes to community-specific localities, we gave our respondents a choice between

Figure 9.6: Respondents from Haryana most likely to believe that technologies used by the police or govt. are more likely to target certain groups or communities.



Note: All figures are in percentage.
Question asked: In your opinion, are technologies like CCTV cameras, mobile surveillance/tapping or FRT used by the police or the government more likely to target certain groups or communities?

Figure 9.7: More than three out of four respondents felt that surveillance technologies should be used across all types of localities



Note: All figures are in percentage.
Question asked: In your opinion, in which of the following localities it is more important to use surveillance technologies like CCTV cameras, mobile surveillance or phone tapping, etc. to reduce or control crimes:
a. 1. In posh colonies with big houses or 2. Slums
b. 1. In upper caste localities or 2. Dalit basti
c. 1. In Hindu localities or 2. Muslim localities
d. 1. In non-Adivasi localities or 2. Adivasi localities

two localities and asked them in which locality they think it is important to use surveillance technologies like CCTV cameras, mobile surveillance or phone tapping and the like, to reduce or control crimes and we received the following responses.

The majority of respondents felt that it is important to use surveillance technologies to reduce or control crimes, with negligible variations based on caste, religion or class-based localities. There was general support towards the idea of mass surveillance across localities.

Conclusion

The widening opportunities for networking are giving rise to a society where there is recognition for the need of greater vigilance. While the institutional defence of surveillance remains security and safety, there is also a much greater understanding of the moral and ethical intricacies attached to it, especially in reference to privacy. The underlying rationale that support data-driven security practices are that the harvesting of personal and meta-data would permit authorities to intervene in a targeted and intelligence-led fashion and will allow them to focus attention on their resources on emerging threats and possibly disrupt them before their occurrence (Friedewald et.al., 2017). Becoming an essential prerequisite for significant governance, the idea of data-driven democracy is slowly becoming a newer and more “acceptable” norm.

The survey findings reflect a complicated relationship between the public and the right to privacy. Even as there is little awareness about the legal scope and meaning of the right, people are generally, at least in theory, supportive of the concept. Yet, a significant proportion of the respondents expressed little anxiety about sharing their location data with food delivery apps, family/spouses, employers or women's safety app.

Notably, though, respondents are significantly more anxious about sharing location data with the police, with respondents from the ST community being most apprehensive. However, when it comes to sharing medical and personal information with official government apps/portals such as the Aarogya Setu app or the CoWIN portal, the people are largely comfortable doing so.

While people may be willing to share their data with the government for specific purposes, they are also to a great extent aware of the possibility of its misuse for political purposes. Nearly half of the respondents believe that elected government of the country could snoop on its citizens illegally to some extent. A little more than half also felt private companies and NGOs collect data and influence people's electoral choices.

Reference

Bennett, C. (2013). The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. First Monday, 18(8). https://doi.org/10.5210/fm.v18i8.4789

Chathukulam, J., & Tharamangalam, J. (2021). The Kerala model in the time of COVID19: Rethinking state, society and democracy. World development, 137, 105207.

Chellappan, Kavitha & Kannan, M.K.Jayanthi. (2021). PII classification and Applicability in Personal Data Protection Bill 2019. GIS-Zeitschrift fü Geoinformatik. 1. 1417-1424.

Common Cause and Centre for Study of Developing Societies (2018). Status of Policing in India Report 2018: A Study of Performance and Perceptions. Retrieved from: https://commoncause.in/pdf/SPIR-2018-c-v.pdf.

Friedewald, Michael & Cas, Johann & Bellanova, Rocco & Burgess, J. & Peissl, Walter. (2017). Surveillance, Privacy and Security: Citizens' Perspectives. 10.4324/9781315619309.

IANS. (2022, February 17). Centre resumes biometric attendance for employees, work from home stopped. Retrieved from:https://www.business-standard.com/article/current-affairs/centre-resumes-biometric-attendance-for-employees-work-from-home-stopped-122021700377_1.html

Indian Brand Equity Foundation. (2022). E-commerce in India: Industry Overview, Market Size & Growth| IBEF. (n.d.). https://www.ibef.org/industry/ecommerce#:~:text=Major%20segments%20such%20as%20D2C Lokniti-CSDS (2022). Media in India Report.

Mahapatra, S. (2021). Digital Surveillance and the Threat to Civil Liberties in India. (GIGA Focus Asien, 3). Hamburg: German Institute for Global and Area Studies (GIGA) - Leibniz-Institut für Globale und Regionale Studien, Institut für Asien-Studien.

Malakar, Kapou & Choudhury, Rizwan. (2020). Information privacy and surveillance: a study of the use of digital media by the consumer. Waffen-und Kostumkunde. Volume XI. 165-180.

Michael, K., McNamee, A., & Michael, M. (2006, June 1). *The Emerging Ethics of Humancentric GPS Tracking and Monitoring.* IEEE Xplore. https://doi.org/10.1109/ICMB.2006.43

National Crime Records Bureau (2017). Crime in India, 2016. *Ministry of Home Affairs, Government of India.*

National Crime Records Bureau (2018). Crime in India, 2017. *Ministry of Home Affairs, Government of India.*

National Crime Records Bureau (2019). Crime in India, 2018. *Ministry of Home Affairs, Government of India.*

National Crime Records Bureau (2020). Crime in India, 2019. *Ministry of Home Affairs, Government of India.*

National Crime Records Bureau (2021). Crime in India, 2020. *Ministry of Home Affairs, Government of India.*

National Crime Records Bureau (2022). Crime in India, 2021. *Ministry of Home Affairs, Government of India.*

Solove, Daniel J., *Understanding Privacy*. Harvard University Press, May 2008, GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420, Available at SSRN: https://ssrn.com/abstract=1127888

Srinivas, N & Biswas, A. (2012). *Protecting Patient Information in India: Data Privacy Law and its Challenges – NUJS Law Review.* Retrieved from http://nujslawreview.org/2016/12/05/protecting-patient-information-in-india-data-privacy-law-and-its-challenges/ Accessed on 20th October 2022.

Chapter 10:

Legal Mechanisms and Crime Control

Key findings

- Four out of five people will approach the police in case of a breach of their privacy.
- People feel a greater need for an independent forum to deal with illegal surveillance by government agencies such as the police, as against forum for dealing with illegal surveillance by private companies.
- Only 16 percent people believe that the police are adequately trained to use surveillance technologies such as CCTVs, drones and FRT.
- Two out of five people are aware of incidents CCTV footage tampering or manipulation.
- Forty-four percent people believe that CCTV cameras in police stations are very helpful in preventing human rights violations against those in custody.
- Forty percent people believe that police should not have any freedom to check people's phones without a warrant.
- Two out of five people believe that police should always obtain a search warrant before tracking anyone's laptop or phone.
- Three out of five people strongly believe that the police should be able to tap an accused person's phone or CCTV footage without a warrant, while one-third believe they should be able to do so with the victim or any other relevant person.

CHAPTER 10

Legal Mechanisms and Crime Control

Data security has become immensely valuable for states and individuals alike in a technology-driven world order. The dilemma that haunts the democratic framework of countries is the adoption of strategies that strike a balance between individual privacy and national security. Several developed countries have introduced legislation and provisions to safeguard their citizens from not just cyber-attacks but also breaches of privacy. However, the question remains – are these legislations enough to protect citizens and do these laws carry a risk of impinging upon basic human rights, primarily the right to privacy?

India, the largest democracy in the world, is yet to frame a proper and uniform data protection law. The existing legal provisions for data security are considered inadequate to tackle the complex nature of technology surrounding us today. The history of legislation for data protection can be traced back to the Information Act passed in 2000 (known as IT Act, 2000). One of the main objectives of this legislation was to provide a smooth framework for e-commerce (Bharuka, 2002). With the introduction of Section 43A under the IT Act Amendment of 2008, it became mandatory for companies to protect all sensitive personal data and information they possessed, dealt with or handled in a computer resource by implementing and maintaining reasonable security practices and procedures (Sodhi, et al., 2022). A new legal provision was introduced in 2011, which came to be known as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. It required corporations to provide an accessible privacy policy, obtain customer consent before collecting personal sensitive data, and state the purpose and usage for data acquisition. Nonetheless, with the rapid developments in the IT sector, all of these provisions were considered largely insufficient. In order to establish a unified legislation for data protection, the Supreme Court in the 2017 *Justice (Retd.) Puttaswamy vs Union of India case* concluded that the right to privacy is a fundamental right, guaranteed primarily under Article 21 of the Indian Constitution. The Court specified that this right includes, inter alia, the right to informational privacy (Subramaniam & Das, 2022). A Personal Data Protection Bill was introduced in parliament in 2019 but was later withdrawn in the Lok Sabha in August 2022 amid concerns over government overreach. Following this, the Digital Personal Data Protection Bill was introduced in November 2022 and is currently in the public consultation phase.

Against this background, this chapter tries to assess people's opinions on the need for legal mechanisms to deal with breaches of privacy or cybercrime and the capacities of state agencies in dealing with surveillance technologies. Further, the chapter explores the intricacies of the legal mechanisms that could safeguard the privacy of individuals against potential breaches by state or non-state agencies. The chapter is divided into four sections:

- **Section 1** investigates which institutions and agencies people are most likely to approach for the redressal of a privacy breach.
- **Section 2** reports people's opinions about the need for such a legal framework or a forum for redressal against private or government agencies in case of privacy breaches.
- **Section 3** studies public perceptions on the extent to which state agencies should have the power to use advanced surveillance technology.
- **Section 4** analyses issues related to the capacity of the police in handling advanced surveillance technologies.

10.1. Existing institutional support for dealing with breach of privacy

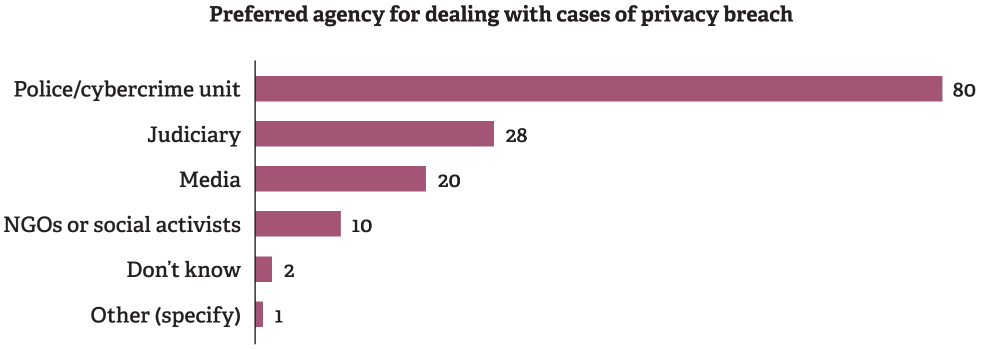
Privacy breach or data breach is the leak of personal, protected and sensitive information to an unauthorised third party. Around the world independent institutional regulatory authorities exist to deal with such breaches. For instance, the Estonian Data Protection Inspectorate founded in 1999, the Information Regulator, an independent body functioning in South Africa, the Independent National Privacy Commission in the Philippines, and the Information Commissioner in the UK, to name a few. Such institutional mechanisms are absent in India. This leaves individuals with no other alternatives other than to refer such cases to traditional law enforcement agencies for the protection of their privacy.

When respondents were asked where they seek redressal in case of a privacy breach, almost four in every five respondents (80%) said that they will contact either the police or the cybercrime unit (a unit with the police system). Three in 10 people (28%) said that they would approach the judiciary in case of a privacy breach and one-fifth (20%) also said that they would approach the media (Figure 10.1).

Across states, people's choice of institution for seeking redressal varied across the types of agencies. In Delhi and Kerala, more than 90 percent said that they would approach the police or a cybercrime unit to complain about such a breach, while contrastingly, in Tamil Nadu, only a little over half said that they would go to the police. However, notably, one out of five respondents from Tamil Nadu could not respond to this question as they have not yet experienced such cases (Table 10.1).

In Karnataka, while eight out of every 10 persons (83%) preferred the police or cybercrime unit for redressal at the same

Figure 10.1: Four out of five people will approach the police in case of a breach of their privacy



Note: All figures are in percentages. The figure may not add up to hundred as respondents could name multiple agencies.
Question asked: Whom will you approach for redressal, in case of a privacy breach?

Table 10.1: Those from Tamil Nadu least likely to approach the police in case of a privacy breach, those from Delhi and Kerala most likely to

States	Most preferred institution for seeking redressal for privacy breach			
	Police/ cybercrime unit	Judiciary	Media	NGOs or social activists
NCT Of Delhi	92	8	6	4
Kerala	92	40	12	6
Haryana	85	13	7	3
Gujarat	85	22	9	6
Maharashtra	84	28	26	18
Karnataka	83	59	65	33
West Bengal	81	32	31	15
Andhra Pradesh	79	32	21	4
Uttar Pradesh	76	20	13	6
Assam	76	34	12	6
Punjab	70	26	19	7
Tamil Nadu	54	28	23	11

Note: All figures are in percentages. The figure may not add up to hundred as respondents could name multiple agencies.
Question asked: Whom will you approach for redressal, in case of a privacy breach?

time, close to two-thirds (65%) and three-fifths (59%) said that they would approach the media and judiciary respectively in case their privacy is breached. Across states, the most preferred agency for redressal of such cases was the police followed by the judiciary, with few people opting for media or NGOs/ social activities, thus indicating that people were much more likely to approach government institutions in such matters than alternate agencies. Other than Karnataka, a notable proportion of respondents from Kerala, Assam, and West Bengal also said that they would approach the judiciary in case they encounter any incidents of a privacy breach. In Karnataka, one-third also said that they would go to an NGO or social activists to seek help in redressing the issue (Table 10.1).

10.2. Support for independent forums to deal with privacy breach

At the time of writing of this report, there exists no comprehensive data protection law and forum in India where an individual can complain about a breach of privacy. However, the IT Act 2000 does provide some space for redressal if the disclosure of information has taken place (Kumar, 2021). In the absence of such laws and forums, people are left vulnerable to cyber attacks and illegal surveillance both by state as well as non-state actors. In both these cases, their privacy can be compromised, in violation of the values of a democratic political system.

The survey tried to assess the extent of public demand for such an independent body, seeking people's opinions on the need for an independent forum where complaints can be registered against various state and non-state actors for privacy breaches. The findings suggest that people strongly endorsed the need for a forum to register complaints against government agencies such as the police, as compared to private agencies.

More than half of respondents (55%) said that there should be an independent forum to handle complaints against government agencies such as the police for breach of privacy or illegal surveillance. A little over

Table 10.2: People feel a greater need for an independent forum to deal with illegal surveillance by government agencies such as the police, as against illegal surveillance by private companies

Illegal surveillance and breach of privacy by the following agencies	Independent forum to complain against digital privacy breach			
	Required	Maybe	Not required	Can't say
Private companies	35	25	19	21
Government agencies such as the police	55	21	7	17

Note: All figures are in percentages.
Question asked: In your opinion, should the government establish independent forums where people can complain against digital breach of privacy or illegal surveillance by the following agencies: (a.) private companies (b) government agencies such as the police?

one in three (35%) said that there is a need for such forums for complaints against private companies. About one in five people felt that no such forum is required for dealing with complaints against private companies, while just seven percent said that there was no need for such a forum for dealing with complaints against government agencies (Table 10.2). The data suggests that according to the larger public opinion, the lacunae in legal mechanisms is far more glaring when it comes to dealing with illegal surveillance and privacy breach by government agencies, as compared to private entities.

The findings also suggested that, across occupational categories, working professionals formed the biggest strata of people wanting a forum to complain for both private (42%) and government agencies (64%). Interestingly, close to two-thirds (63%) of government employees were also in support of establishing a forum to complain against government agencies, while just about one in three government employees (36%) felt the need for a forum for dealing with complaints against private companies (Table 10.3).

In chapters 6 and 9, we saw that government employees were also more likely to hold the opinion that personal information on phones can be accessed by the government without the person's consent or knowledge, and were also the most anxious about sharing their GPS location with their employers. Seen together, these findings may suggest that across

Table 10.3: Professionals and government employees most likely to support the establishment of an independent forum to deal with illegal surveillance by the government

Occupation	Forum to complaint against private companies	Forum to complaint against government agencies
Professionals	42	64
Government Employees	36	63
Business	33	50
Labourer	31	49
Farmers	25	42
Student	39	60

Note: All figures are in percentages. Response categories of "not required", "maybe" and can't say" have not been reported here.
Question asked: In your opinion, should the government establish independent forums where people can complain against digital breach of privacy or illegal surveillance by the following agencies: (a.) private companies (b) government agencies such as the police?

occupational groups, government employees who are highly, if not the most, sceptical of government agencies respecting people's right to privacy.

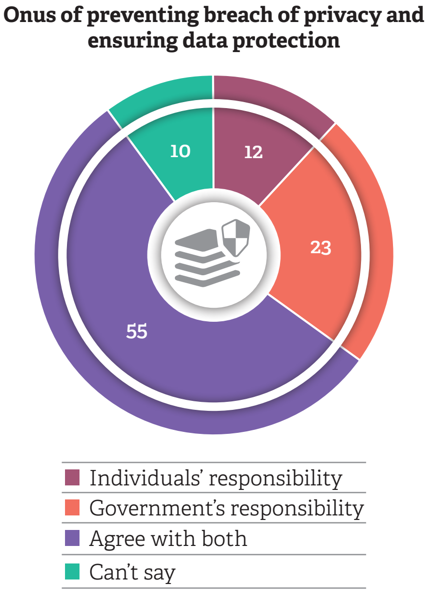
Consent is a fundamental component of personal data protection laws across the world. Rules and regulations are formulated to ensure that the privacy of individuals must be protected and any collection and usage of data without informed consent could be deemed as unlawful. According to the World Bank practitioner's guide on data and privacy laws, there must be a genuinely independent institutional regulatory authority which would establish principles for the protection of the privacy of individuals and investigate the violations of privacy and data rights (World Bank 2019). The Organisation for Economic Co-operation and Development (OECD) has clearly mentioned in its 2013 guidelines that a national government must have privacy enforcement authorities which can implement data protection laws, besides providing sanctions and remedies in case of non-compliance. It also maintains that the central government should take the initiative to educate people and provide necessary skills to make citizens aware of the importance of data privacy (OECD Legal Instruments 2013). Both these international guidelines emphasise that the responsibility of protecting the right to privacy falls primarily upon the government, which has the capacity to formulate and adjudicate privacy regimes. However, there is a correlation between rights and duties, where the state is considered the protector of rights, and citizens are expected to fulfill their duties. Keeping in mind this debate, the survey asked the general public their opinion on who is primarily responsible for protecting people's right to privacy and preventing its violation—the state or the citizens themselves.

It was found that more than half (55%) of the respondents believed that both government and the individuals were responsible for preventing illegal surveillance, hacking or cybercrimes, while one in 10 feel (12%) that it is an individual responsibility and close to a quarter (23%) believe that it is primarily the government's responsibility (Figure 10.2).

Respondents from Haryana (18%) and Tamil Nadu (17%) were most likely to believe that it's the individual's responsibility to ensure their protection against privacy breaches. Surprisingly, one out of two people (54%) from Karnataka believed it is the responsibility of the government, while in other states this proportion is far smaller. In contrast, Andhra Pradesh (75%) and Assam (64%) had an overwhelming majority of people who believed that it's the responsibility of both the government and the individual (Table 10.4).

Moreover, the data indicated that the rich people were less likely to believe that it was the government's responsibility to ensure citizens' protection against privacy

Figure 10.2: More than half of the respondents believe that the government and individuals share equal responsibility in preventing privacy breach



Note: All figures are in percentages.
Question asked: Which of the following statements do you agree with the most?
a. It is the individuals' responsibility to ensure that they protect their data against any kind of illegal surveillance, hacking or cybercrime
b. It is the responsibility of the government to enforce data protection laws and educate its citizens about the right to privacy

Table 10.4: More than one out of two respondents from Karnataka feels that data protection and preventing privacy breach is the responsibility of the government

States	Responsibility in ensuring protection from illegal surveillance, hacking or cybercrime		
	Individuals' responsibility	Government's responsibility	Both are responsible
Andhra Pradesh	11	10	75
Assam	10	9	64
Uttar Pradesh	12	10	60
Kerala	14	22	60
Gujarat	13	20	60
Maharashtra	7	20	57
Punjab	10	18	56
West Bengal	13	26	51
NCT Of Delhi	12	32	48
Haryana	18	27	48
Tamil Nadu	17	29	44
Karnataka	13	54	31

Note: All figures are in percentages. Rest did not respond.
Question asked: Which of the following statements do you agree with the most?
a. It is the individuals' responsibility to ensure that they protect their data against any kind of illegal surveillance, hacking or cybercrime
b. It is the responsibility of the government to enforce data protection laws and educate its citizens about the right to privacy

breaches—18 percent of the rich believed so, against 27 percent of those from the lower class. However, those from the rich class were also most likely to believe that it was the joint responsibility of both the government and the citizens (64%) (Table 10.5).

10.3. Police's capacity for handling advanced surveillance technologies

Numerous technological innovations are now used for crime prevention and reduction. Law

Table 10.5: Rich are least likely to believe that prevention of illegal surveillance and privacy breach is the government's responsibility

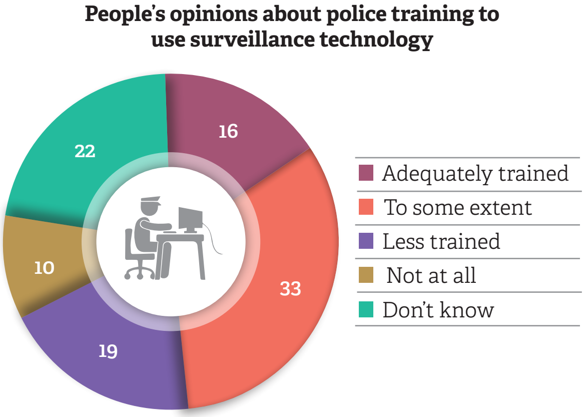
Class	Responsibility in ensuring protection from illegal surveillance, hacking or cybercrime			
	Individuals' responsibility	Government's responsibility	Both are responsible	Can't say
Poor	11	22	47	20
Lower	13	27	52	8
Middle	14	23	58	5
Rich	12	18	64	6

Note: All figures are in percentages.
Question asked: Which of the following statements do you agree with the most?
a. It is the individuals' responsibility to ensure that they protect their data against any kind of illegal surveillance, hacking or cybercrime
b. It is the responsibility of the government to enforce data protection laws and educate its citizens about the right to privacy

enforcement agencies are increasingly inducting advanced technologies to deal with modern-day challenges. Technologies such as CCTV cameras, GPS location tracking, facial recognition, drones, and voice recognition are being employed for the prevention or investigation of crimes. Indore police, for instance, unveiled a fingerprint-based criminal record data fetching system to control crime. It can be connected to a smartphone to gather information through fingerprints in public places and if the fingerprint matches, the criminal record of that person will emerge (Meshram, et.al, 2022).

There is no doubt that such technologies can be effective tools for crime prevention and investigation. Keeping aside the debates as to the possible misuse of such technologies, here we look at people's perceptions about the extent to which the police are trained and equipped to be able to deal with such technologies. This assessment of public opinion regarding how well-equipped the Indian police is to effectively employ technological products also indirectly reflects the people's trust in the police to be able to use these technologies without impinging upon the basic rights of individuals.

Figure 10.3: Only 16 percent people believe that the police are adequately trained to use surveillance technologies such as CCTVs, drones and FRT



Note: All figures are in percentages.
Question asked: To what extent do you think the police in your locality have received adequate training to use and to store data of technologies like CCTV cameras, drones or FRT – adequately trained, trained to some extent, less trained or not at all trained?

When the respondents were asked for their opinion on the extent to which the police in their locality are trained to use and store data collected from CCTV cameras, drones and FRT, only 16 percent felt that they were adequately trained. One out of three people felt that the police were somewhat trained to use these technologies. On the other hand, three in 10 respondents felt that the police are either inadequately trained or not at all trained in handling the data of such technologies (Figure 10.3).

Technological innovations in the 21st century have reshaped the functioning and organisation of the police. Technology has become integral to policing and without technology, it is impossible to imagine the functioning of modern-day police forces. The reliance on technology has intensified in recent years as the police face new challenges in their functioning (Laufs & Borrion, 2021). The Indian cyber watchdog, Computer Emergency Response Team (CERT-In) reported that:"In the year 2020, CERT-In handled 11,58,208 incidents. The type of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breach and Vulnerable Services" (CERT-In 2020).

In 2021, the Indian healthcare industry reported the second-highest global malware attacks. It faced 7.1 percent (71 lakhs) of cyberattacks, second only to the US health industry, which faced 28 percent of the global attacks (PTI, 2022). Such challenges are driving engines for law enforcement agencies to employ technology to effectively safeguard national as well as individual security. Therefore, dependency on technology is natural for state agencies to prevent and reduce criminal activities.

In order to better understand how people perceive the usage of such advanced technologies by the police, they were asked whether there was any rise in the use of advanced surveillance technologies by the police in their localities in the past 4-5 years.

Table 10.6: Forty-four percent believe that the use of CCTVs by the police has increased a lot in the last 4-5 years

	Degree of usage of these technologies by the police in your locality in the last 4-5 years				
	A lot	To some extent	A little	Police Never used	Can't say
CCTV	44	25	11	10	10
Mobile surveillance such as phone tapping or phone checking	19	24	18	18	21
Facial Recognition Technology (FRT)	13	20	16	23	28
Drones	16	21	20	21	22

Note: All figures are in percentages.
Question asked: In the last 4-5 years, to what extent the use of the following technologies by the police has increased in your locality – has it increased a lot, to some extent, a little or never been used by the police?

Over two out of five (44%) of the respondents felt the use of CCTV cameras by the police has increased a lot in the past few years and another quarter said that its usage has increased to some extent. A significant proportion of the respondents also said that mobile surveillance by the police has also gone up—19 percent felt it has increased a lot and another 24 percent felt that it has increased to some extent. On the other hand, when it comes to slightly more advanced surveillance technologies such as drones and FRTs, more than one in five people were of the opinion that the police never used them and just 16 and 13 percent respectively felt that its use by the police had gone up by a lot in the last few years (Table 10.6).

Table 10.7: More than two out of three respondents from Gujarat reported an increase in the use of mobile surveillance and drones by the police in the last 4-5 years

State	Increased use of advanced technologies across states			
	CCTV	Mobile Surveillance	FRT	Drones
Andhra Pradesh	87	53	38	46
Gujarat	85	66	55	68
Karnataka	76	42	59	48
Haryana	75	52	28	37
Tamil Nadu	73	52	47	48
Maharashtra	73	41	36	41
West Bengal	67	39	32	29
NCT Of Delhi	62	35	18	28
Uttar Pradesh	62	55	29	37
Punjab	58	35	23	24
Kerala	56	19	13	16
Assam	43	28	16	25

Note: All figures are in percentages. A lot and somewhat increase categories are clubbed.
Question asked: In the last 4-5 years, to what extent the use of the following technologies by the police has increased in your locality – has it increased a lot, to some extent, a little or never been used by the police?

A state-wise analysis revealed that in Andhra Pradesh and Gujarat, more than 85 percent believed that the use of CCTVs by the police in their areas has increased. More than two out of three respondents from Gujarat also reported a significant increase in the use of mobile surveillance and drone technologies by the police in their localities in the past 4-5 years (Table 10.7).

Such advanced technologies are also not immune to errors and misidentification, as has been demonstrated by different studies across the globe. The accuracy of technologies such as FRT and CCTV cameras depend upon numerous factors, such as the positioning and lighting of the object, which on the field tends to be unsteady, or facial features such as race and ethnicity of the person whose image is being captured. Therefore, the accuracy of such technologies can vary to a great extent, depending upon many such factors (Crumpler, 2020). In order to understand whether the common public is aware of such nuances and drawbacks of these technologies, the respondents were asked whether they were aware of any incidents of either the misuse or the inaccuracies of the technology. Two out of five respondents (39%) said that they were aware of incidents where CCTV camera footage has been manipulated or tampered with. Another 19 percent said that they knew of instances in other countries wherein FRT misidentified people (Table 10.8). The lower awareness of the latter can possibly be associated with the lack of awareness and paucity of news coverage related to FRT, as is evident from the media content analysis presented in Chapter 4.

Table 10.8: Two out of five people are aware of incidents CCTV footage tampering or manipulation

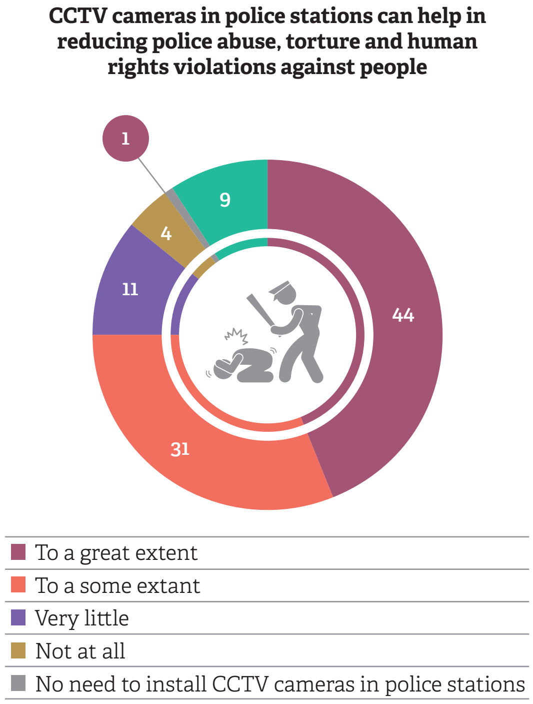
Are you aware of?	Yes
In other countries, FRT has misidentified people	19
The footage of the CCTV camera has been manipulated or tampered with	39

Note: All figures in percentages.

10.4. Opinions about the use of advance surveillance technologies by the police

In the case of *Paramvir Singh Saini vs Baljit Singh & Others*, 2020, the Supreme Court directed all states to install CCTV cameras within police stations in order to monitor human rights abuses by the police. In an attempt to understand people's opinions on the issue, the respondents were asked about the extent to which they think CCTV cameras in police stations can help in reducing police abuse, torture and human rights violations against people in custody. Two-fifths (44%) of the respondents were of the opinion that CCTV cameras are very helpful in preventing human rights violations against those in custody. Another one-third (31%) felt that it can be helpful to some extent (Figure 10.4).

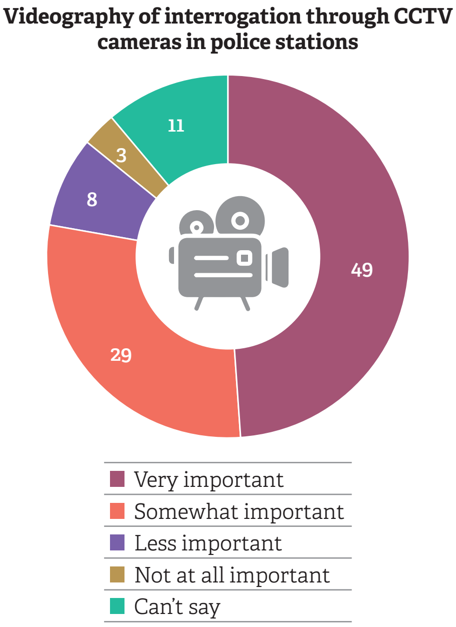
Figure 10.4: Forty-four percent people believe that CCTV cameras in police stations are very helpful in preventing human rights violations against those in custody



CCTV cameras in police stations can help in reducing police abuse, torture and human rights violations against people

Note: All figures are in percentages.
Question asked: To what extent do you think CCTV cameras in police stations can help in reducing police abuse, torture and human rights violations against people in custody – to a large extent, to some extent, very little or not at all?

Figure 10.5: Close to half of the respondents strongly believe that interrogations by the police should be recorded on CCTVs



Note: All figures are in percentages.
Question asked: In your opinion, how important is it for any interrogation in a police station to be video graphed through CCTV cameras–very important, somewhat important, less important or not at all important?

Often, criminal interrogations involve the use of violence by the police. Further, since interrogations by the police can often be violent and violative of human rights, respondents were asked for their opinion on the importance of videography of interrogation in a police station. Close to half of the respondents (49%) said that it was very important and three in 10 said it was somewhat important (Figure 10.5).

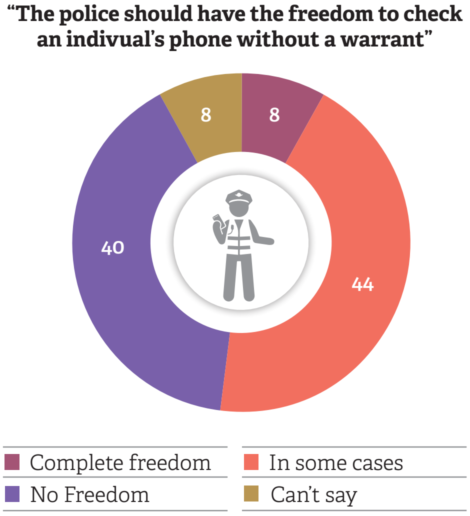
Across states, respondents from Kerala were the most supportive of the installation of cameras in police stations, with more than two-thirds believing that the installation of CCTV cameras in police stations would be very helpful in reducing police atrocities in custody. Four out of five people from Kerala also believe that it was very important that interrogation in police stations be videographed. In Andhra Pradesh, three out of four respondents considered videography of any interrogation very important. Those from Karnataka and West Bengal, on the other hand, were the least supportive of the installation of CCTV cameras in police stations, although even in these states more than half the respondents were in support of its installation.

10.5. Police access to private devices

In a surveillance state, the police and state agencies often bestow upon themselves uninhibited powers to access any personal data and information of the people, even if it needs to be accessed on their private devices. In this survey, we find that according to larger public opinion, while there is significant support for the use of mass surveillance technologies by the police and state, there is also simultaneously significant concern regarding intrusion and leakage of private data from personal devices. In chapter 6, when people were asked about their opinion on different agencies getting unconsented access to their phone's content, close to half of the respondents were very anxious about police getting unconsented access to their phones.

Similar opinions are also reflected in response to a question regarding the extent of freedom

Figure 10.6: Forty percent people believe that police should not have any freedom to check people's phones without a warrant



Note: All figures are in percentages.
Question asked: How much freedom should the police have to check your phone at any time without a warrant - complete, in some cases, or no freedom at all?

that the police should have to check one's phone anytime without a warrant. Merely one in every 10 said that police should be given complete freedom to check someone's phone without a warrant. More than two out of five respondents said that the police should be able to check phones without a warrant in some cases only. On the other hand, two in five respondents said that the police should not be given any freedom to check one's phone with a warrant (Figure 10.6).

More than three out of four respondents from Karnataka (76%) believed that complete freedom to the police should be available in some cases, while close to six of every 10 respondents from Delhi and Kerala (57%) held the opposite opinion. In contrast, respondents in Gujarat (16%) and Tamil Nadu (12%) showed comparatively a higher inclination towards complete freedom to police to check people's phones without a warrant (Table 10.9).

According to the Code of Criminal Procedure (CrPC) 1973, the police have the power to conduct a search with a warrant when they are investigating a criminal offence (Poddar, 2021). There are also multiple legislations which lay down the rules of conducting a search with the due process of law if law enforcement agencies have to conduct a search. Police have to serve a prior notice under Section 91 of the CrPC or a search warrant under Section 93 of the same law (Poddar, 2021). However, if the police randomly check the phones of individuals without a warrant, it is legally considered to be a violation of the basic rights of citizens enshrined in Article 21 of the Indian Constitution (protection of life and liberty) and the practice is also against the right to privacy upheld by the Supreme Court in the *Puttaswamy* judgement of 2017 (Fazili, 2021).

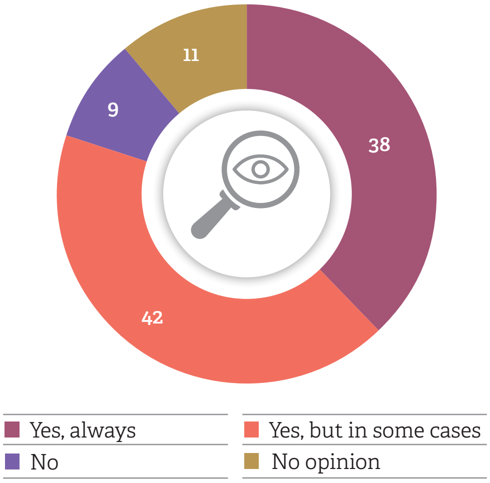
Table 10.9: Three out of four people from Karnataka believe that the police should have the freedom to check people's phones without a warrant in some cases

States	The degree of freedom police should have to check an individual's phone without a warrant		
	Complete freedom	In some cases	No Freedom
Karnataka	5	76	17
Assam	8	57	16
Tamil Nadu	12	56	24
Maharashtra	8	50	29
Gujarat	16	45	34
Andhra Pradesh	4	45	48
Uttar Pradesh	5	39	47
Punjab	6	39	45
West Bengal	10	36	45
Haryana	9	35	53
NCT Of Delhi	6	34	57
Kerala	8	32	57

Note: All figures are in percentages. Rest did not respond.
Question asked: How much freedom should the police have to check your phone at any time without a warrant - complete, in some cases, or no freedom at all?

Figure 10.7: Two out of five people believe that police should always obtain a search warrant before tracking anyone's laptop or phone

"Investigative agencies must obtain a search warrant before checking or tracking anyone's phone or computer/laptop"



Note: All figures are in percentages.
Question asked: Do you think that to prevent abuse of power, investigative agencies must obtain a search warrant before checking or tracking anyone's phone or computer/ laptop?

Against this backdrop, people's opinions on the need for the police to obtain a search warrant for checking a person's phone or laptop was obtained. Nearly four out of five (80%) were of the opinion that the police should obtain a search warrant before doing so, of which 38 percent strongly agreed and 42 percent somewhat agreed with the statement. On the other hand, just nine percent felt that there was no need for a warrant for the police to access people's phones or laptops (Figure 10.7).

While further analysing the data it was found that more than five out of 10 people in Haryana (57%), Kerala (55%), and Delhi (55%) believed that investigative agencies should always have awarrant before investigating one's private property. In contrast, a small number of respondents in Karnataka (17%) and Tamil Nadu (16%) believed that they should be allowed to investigate regardless.

While people tend to hold a strong opinion regarding the need for a search warrant before the police can access anyone's personal devices, as seen above, when it comes to those involved in a criminal matter, these opinions change drastically. When respondents were asked whether the police should be able to tap phones and check CCTV cameras of the accused, victim, or anyone linked with that case, without any kind of warrant or permission, three in five respondents fully agreed. Support declined for surveilling the victims and other persons related to the case, although more than three in 10 respondents fully agreed with this as well (Table 10.10).

Table 10.10: Three out of five people strongly believe that the police should be able to tap an accused person's phone or CCTV footage without a warrant, one-third believe they should be able to do so with the victim or any other relevant person

	Degree of freedom police should have in tapping their phones or check their CCTV cameras footage without warrant				
	Fully agree	Somewhat agree	Somewhat disagree	Fully disagree	Can't say
The accused	61	20	5	6	8
The victim	30	27	15	15	13
Any other person who may have relevant information linked with related to the case	36	29	11	10	14

Note: All figures are in percentages.
Question asked: To investigate any crime, the police should be able to tap phones and check CCTV cameras of the following persons,linked with that case, without any kind of warrant or permission. Please tell me whether you agree or disagree with this.

Further, in the case of the victims, strong support for police checking people's phones and laptops without a warrant was apparent in states such as Andhra Pradesh (44%) and Gujarat (43%). In contrast, states such as Karnataka, Kerala (38%), and Delhi had a larger share of respondents who disagreed with this.

Conclusion

This chapter tried to examine the use of advanced technology in policing against the backdrop of existing legal mechanisms. Due to the lack of a uniform data protection regime in India, individuals have no independent institutions to turn to when their privacy is breached. Therefore, in this scenario, they either approach conventional institutions such as the police/cybercrime department, judiciary, or the media. We asked respondents about the need for a statutory authority which can uphold their privacy rights and most people answered in the affirmative. The data suggests that there is a demand among the people for the establishment of such independent bodies, particularly for dealing with cases of illegal surveillance by the government.

The chapter also looked into people's opinions regarding the use of such technology to prevent police excesses. A significant proportion of the respondents feel that the incorporation of technology inside police stations is necessary to prevent human rights violations by the police.

The study found that the fallout of the absence of comprehensive data protection laws has a deeper impact on society and institutions. This absence results in the vulnerability of citizens to cyber-attacks and it also allows state agencies to violate the fundamental rights of individuals as the Indian government has provided law enforcement agencies with sweeping powers. Thus, there is a requirement for a sustainable and adequate data protection law which can ensure the protection of citizens and provide an independent forum where they can submit their grievances.

References

Bharuka, D. (2002). Indian Information Technology Act, 2000 Criminal Prosecution Made Easy for Cyber Psychos. *Journal Of The Indian Law Institute*, 44(3), 354–379.

Crumpler, W. (2020, April 14). How Accurate are Facial Recognition Systems- and Why Does It Matter? *Centre for Strategic & International Studies*. Retrieved from:https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter

Fazili, Sana. (2021, November 3) Can The Police Check Your Whatsapp Chats Without Warrant? *Boom Live*. Retrieved from:https://www.boomlive.in/explainers/right-to-privacy-police-checking-phones-whatsapp-messages-hyderabad-15439. Accessed on 5thNovember 2022.

Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics and Information Technology (MeitY) Government of India. Annual Report2020.

Kumar, U. (2021, February 12). Why India is indifferent to the data privacy issue. *Financial Express*. Retrieved from: https://www.financialexpress.com/brandwagon/why-india-is-indifferent-to-the-data-privacy-issue/2193807/. Accessed on 3rd November 2022.

Laufs, J., & Borrion, H. (2022). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management*, 24(2), 190–209.

Sodhi, S.D., Samant, B., & Sinha, T. (2022). The Journey of India's Data Protection Jurisprudence. *Lexology*. Retrieved from: https://www.lexology.com/library/detail.aspx?g=57720842-f709-4dd4-947b-44c3c6e4ed10. Accessed on 28th October 2022.

Meshram, S., Ravindranath, M. & Kinger, H. (2022, March 5) Technology can make policing better and also more dangerous. *Indian Express*. Retrieved from: https://indianexpress.com/article/opinion/columns/technology-can-make-policing-better-and-dangerous-7835030/. Accessed on 3rd November 2022.

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data OECD/LEGAL/0188. Retrieved from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

PTI. (2022, September, 20). Indian health care sees second highest number of cyber-attacks in the world: CloudSEK. *The Hindu.* Retrieved from: https://www.thehindu.com/sci-tech/technology/cyber-attacks-on-indian-healthcare-industry-second-highest-in-the-world-cloudsek/article65914129.ece.

Paramvir Singh Saini vs Baljit Singh & Others, July 2020. Special Leave Petition (Criminal) No. 3543 of 2020. Retrieved from: https://main.sci.gov.in/supremecourt/2020/13346/13346_2020_33_1501_24909_Judgement_02-Dec-2020.pdf.

Poddar, U. (2021, November 4). Can the police in India force someone to hand over their phone and check their messages? *Scroll.* Retrieved from: https://scroll.in/article/1009529/can-the-police-in-india-force-someone-to-hand-over-their-phone-and-check-their-messages. Accessed on 5th November 2022.

Subramaniam, A. & Das, S. (2022, October 2022). The Privacy, Data Protection and Cybersecurity Law Review: India. *The Law Reviews.* Retrieved from: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india.Accessed on 29th November 2022.

World Bank. (2019). ID4D Practitioner's Guide: Version 1.0. Washington, DC: World Bank. Retrieved from: https://id4d.worldbank.org/guide/data-protection-and-privacy-laws.

Appendices

APPENDIX 1

Technical Details of Study Design and Sample

This report is based on findings from a survey-based study conducted in 12 Indian states. The study was conducted by Lokniti- Centre for the Study of Developing Societies (CSDS), in collaboration with Common Cause. The objective of the study was to understand people's opinion and their experiences with government or non-government surveillance through CCTV cameras, phone tapping and data collection by government and private companies in India.

1. Sampling

Stage 1: At the first stage, we listed Indian states (missing UTs, except Delhi) on the basis of their urban population as per the census 2011 ranging from high urbanised state to low. We selected the first 12 states in the list including the NCT of Delhi, Goa, Mizoram, Kerala, Tamil Nadu, Maharashtra, Gujarat, Karnataka, Punjab, Haryana, Andhra Pradesh, and West Bengal. But we dropped two small states – Goa and Mizoram- and replaced Mizoram with Assam (representing North-east India) and Goa with Uttar Pradesh.

Stage 2: At the second stage, we selected three cities from the sampled states. The first city from each state is its capital city except Haryana (as it shares its capital with Punjab, so we selected Gurugram) and in Assam, we selected Guwahati instead of Dispur. For Andhra Pradesh, we selected Hyderabad instead of the new capital Amravati as Hyderabad

Table A1.1: Selected states and cities

Sr. No.	Name	Urban population census 2011 (%)	State capital	Mid-sized city	Small town
1	NCT Of Delhi	98	Delhi	Faridabad	Ghaziabad
2	Uttar Pradesh	22	Lucknow	Bareilly	Kasganj
3	Assam	14	Guwahati	Silchar	Dibrugarh
4	Kerala	48	Thiruvananthapuram	Kozhikode	Kollam
5	Tamil Nadu	48	Chennai	Tiruchirappalli	Tirunelveli
6	Maharashtra	45	Mumbai	Solapur	Malegaon
7	Gujarat	43	Gandhinagar	Bhavnagar	Junagadh
8	Karnataka	39	Bengaluru	Mysore	Belgaum
9	Punjab	37	Chandigarh	Ludhiana	Patiala
10	Haryana	35	Gurugram	Rohtak	Panipat
11	Andhra Pradesh	33	Hyderabad	Guntur	Kurnool
12	West Bengal	32	Kolkata	Durgapur	Maheshtala

was the capital of Andhra Pradesh for a long time; though after dividing the state, Hyderabad was given to Telangana (but for some time it was a shared capital of both Andhra Pradesh and Telangana). Then mid-sized (population between 5-10 lakhs) and small cities (1-5 lakhs) were selected. Both types of cities from each state had the highest population in the given population brackets.

Stage 3: At stage three, we have to select 12 localities from each state. At this stage, our state teams were contacted and they were suggested to sample 12 localities keeping the economic status of areas in consideration. They were asked to select three localities each from poor, lower, middle and high income group localities.

2. Questionnaire

The English questionnaire was designed after a rigorous dialogue in a series of meetings and discussions within the research team comprising colleagues from Lokniti and Common Cause. Comments and suggestions were also taken from external experts. The main objective of the survey was to understand people's perceptions on the issue of surveillance by various agencies. Most questions in the questionnaire were structured, i.e., close-ended. However, there were some questionnaires that were kept open-ended in order to find out the respondent's spontaneous feelings about an issue without giving her/him a pre-decided set of options.

Pre-testing and Finalising the questionnaire: To check the efficacy of the questions on the ground, we conducted a pilot study. A research team of Lokniti went into the field to conduct the pilot study on 12th July 2022. The team interviewed people in Delhi from different localities (on the basis of economic status), age groups, educational statuses and gender to get an idea of how cross-sections perceive the question and their level of understanding. Overall, the questions worked well in the field; but we got some suggestions like rephrasing some questions, changing the order of the questions and adding response categories in some of the questions

Translation: After finalising the questionnaires on the basis of inputs received from the pilot study, the questionnaire was translated into 10 Indian languages with the help of each state team. The questionnaire was translated into ten languages (Assamese, Bangla, Hindi, Gujarati, Kannada, Malayalam, Marathi, Punjabi, Tamil, and Telugu).

App designing for the questionnaire: For this study, a specially designed App was used. All translated questionnaires were made available in the Apps so that FIs could use the regional language for the interview.

3. Training workshops and fieldwork

Training workshops: To train the field investigators, rigorous training workshops for all sampled states were conducted. In the workshops, the FIs were informed about the objective of the study and the logic of sample selection. As the fieldwork was to

Table A1.2: Numbers of field investigators in each state

Sr. No.	States	Numbers of field investigators
1	NCT of Delhi	26
2	Uttar Pradesh	18
3	Assam	18
4	Kerala	18
5	Tamil Nadu	18
6	Maharashtra	18
7	Gujarat	18
8	Karnataka	18
9	Punjab	18
10	Haryana	44
11	Andhra Pradesh	18
12	West Bengal	18
	Total	**250**

be done on the App, therefore they were taught about the installation of the App and then feed the responses collected from the respondents through using the questionnaire. They were also asked to complete one dummy interview so that they can understand the logic of each question asked in the questionnaire.

Fieldwork: The fieldwork for the study was conducted in the month of August 2022 between the 6th – 28th. Our team was monitoring the data quality during the fieldwork and wherever we found any discrepancies we immediately contacted the concerned team to notify the FIs and warn them. In case of any doubt about the quality of the interviews, the FIs were asked to do extra interviews. In total, 250 FIs were engaged in the fieldwork. The table A1.2 shows state-wise the numbers of FIs.

4. Data processing & data cleaning

Data processing: The data was saved on the server of the App, used for the study. Once the fieldwork was over, the overall data was down-loaded and then converted into the SPSS format.

Data cleaning: Preliminary analysis was done to check whether there are any invalid entries or unexplained data points. If we located any such cases, we rectified and cleaned the file before the final analysis.

5. Achieved sample

Here are details of the targeted and achieved sample.

Table A1.3: Achieved sample from each state

Sr. No.	Name	Targeted sample	Achieved sample
1	NCT of Delhi	792	820
2	Uttar Pradesh	792	798
3	Assam	792	796
4	Kerala	792	911
5	Tamil Nadu	792	788
6	Maharashtra	792	810
7	Gujarat	792	819
8	Karnataka	792	752
9	Punjab	792	760
10	Haryana	792	903
11	Andhra Pradesh	792	829
12	West Bengal	792	793
	Total	**9504**	**9779**

APPENDIX 2

Methodology Note on Media Analysis

Similar to SPIR 2020-21, Vol. II, we have included a chapter on media discourse of surveillance as part of policing. The idea behind analysing news items on surveillance is to understand how the media portrays the same. For this analysis, news items from six media outlets were selected for the sample--two each of English and Hindi newspapers of mainstream media, and one each of English and Hindi digital-only outlets. The newspapers were selected mainly on the basis of their circulation and reach. News stories from the Times of India and The Indian Express were identified and selected in English, and Dainik Jagran and Dainik Bhaskar in Hindi. It needs to be noted, however, that only the digital archives from the newspapers' websites were used during the sampling process. Amongst the digital-only media outlets, The Print from English and The Wire from Hindi were selected. However, no reliable sources of ranking of digital-only media outlets were available. The selected sample of news outlets is given in Table A2.1.

For the data collection, a pool of keywords was created in both languages, Hindi and English. These keywords were used to search for relevant news items from the selected media outlets. The time frame for the sample was one year beginning from 1st July 2021 to 30th June 2022. The study uses media reports on surveillance of all shades including mass and targeted surveillance, surveillance by the individual, state actors, private companies, pressure groups, etc.

An elaborate coding sheet was created after multiple brainstorming sessions to analyse the stories for a pilot. Inputs from the pilot were further used to improve the coding sheet. The process was repeated twice prior to the final data entry. The coding of the stories was done by a team of coders. All the members of the coding team were given a couple of training sessions and further advice on their doubts.

Table A2.1: Selected sample of news outlets for the analysis

Name of the outlet	Language	Type of publication	Ranking of the news outlet (language-wise)
The Times of India	English	Print and digital	1*
The Indian Express	English	Print and digital	6**
Dainik Jagran	Hindi	Print and digital	1*
Dainik Bhaskar	Hindi	Print and digital	5*
The Print	English	Digital only	No ranking available
The Wire	Hindi	Digital only	No ranking available

Note: Even for the print media, the data was collected using keyword search on the respective websites.

Sources: *Audit Bureau of Circulations, Highest Circulated Daily Newspapers (Language-wise), January-June 2022

**Indian Readership Survey, 2017

Table A2.2: Selected keywords for the analysis

Keywords	
English	Hindi
CCTV	सीसीटीवी
Facial Recognition Technology (FRT)	फेशियल रिकॉग्निशन टेक्नोलॉजी
Face Recognition Technology (FRT)	फेस रिकॉग्निशन टेक्नोलॉजी, चेहरे की पहचान
GPS Surveillance	जीपीएस सर्विलांस
Mobile Application Surveillance	मोबाइल एप्लीकेशन सर्विलांस
Drone	ड्रोन
Mobile Network Surveillance	मोबाईल नेटवर्क सर्विलांस
Hacking	हैकिंग
Surveillance	सर्विलांस,निगरानी
Phone Tapping	फोन टैपिंग
Pegasus	पेगासस
Aadhaar	आधार
Patrolling	पेट्रोलिंग
Phone Tracking/Tracing	फोन ट्रैकिंग / ट्रेसिंग

A total of 1,162 news items were selected from the six media outlets. Prior to the analysis, the data was vetted and cleaned after weeding out duplicate entries and non-relevant stories. The data cleaning process involved filling up the compulsory responses to some of the questions on the coding sheet.

The responses were further clubbed by narrowing down the categories for the questions related to the main actors, the origin of the story, primary sources of the story, who is conducting/organising surveillance and the mode of surveillance. The responses to 'others' were also further processed and either clubbed with the existing category or a new category was created.

Post data cleaning, the final sample size was 1,113 news items, which were used for the final analysis. The distribution of the sample across the various media outlets is provided in Table A2.3. Several questions had multiple choice responses. Hence, while analysing the data, the aggregate of such responses occurred to be greater than the sample size.

The data was collated in an excel format file. All the responses were assigned numbers. The data was then transferred to Statistical Package for Social Sciences (SPSS) software. While analysing the data, frequencies of relevant questions were carried out. Along with that permutation and combinations of different elements were calculated as reported in the chapter.

Table A2.3: Distribution of the sample across various media outlets

Content category	Percent
Hard News Story	48
News Features	39
Editorial/Op-ed/Opinion	6
Explainer	6
Others	1

Note: All Figures are rounded off.

APPENDIX 3

Questionnaire: Surveillance State and Governance

A1. Select the state: ____

A2. Name of the city: ____

A2a. Type of city

1. Capital City
2. Medium City
3. Small City/town

A3. Name of the locality: ____

A3a. Type of the locality:

1. Slums or less developed area
2. Less developed area, but well-structured houses
3. Gated societies/apartment/government flats
4. Posh area/independent houses/bungalows

A4. Investigator Name: ____

A4a. Investigator Roll Number: ____

Start the interview

A5. Field Investigator's introduction & taking the respondent's informed consent:

> *I am the student of __________________. I have come on behalf of Center for the Study of Developing Societies (CSDS) and Common Cause - research organizations based in Delhi. We are conducting a survey to understand people's opinion and their experiences on government or non-government surveillance such as CCTV cameras, phone tapping and data collection by private companies in India. The information gathered by the survey will be used for creating an all-India study on policing with the purpose of improving and reforming the service. It will also be used for legal awareness and educational purposes. This survey is an independent study and is not affiliated with any political party or government agency. The survey will take about 40 minutes. Please take out some time to answer these questions. Your identity will be kept completely secret.*

A6. Can I start the interview?

1. Yes
2. No ***(stop the conversation and go to another house)***

A7. Respondent number: ____________

A8. What is your name? ____________________ ***(If name not told type 'not told').***

Z1. What is your age?________ ***(years) (Write the age as given by the respondent and if the age is not specified then type 0).***

Z2. Gender

1. Male
2. Female
3. Others

Q1. Do you have CCTV cameras around the household/colony you live in?

1. Yes
2. No
98. Don't know

Q1a. ***(If option 1 in Q1)*** Were they installed by you or some other authority?

1. Personally installed
2. Installed by RWA
3. Installed by government
97. Any other ***(Specify)*** _________
98. Don't know

Q2. Would you support the installation of CCTV cameras at these places?

1. Yes 2. No 3. Maybe, time will tell 4. Already installed 98. Can't say

a. At the entry gate of the house
b. Inside the house
c. Inside your shop/place of employment

Q3. And what about these place, would you support the installation of CCTVs cameras?

1. Yes 2. No 3. Already installed 98. Can't say

a. In schools/colleges
b. In hospitals
c. In public parks
d. In government offices
e. In RWAs/residential societies
f. In prisons
g. In police stations
h. In market places
i. Inpublic transports like buses or trains

Q4. Now, I will read out a few statements, please tell me whether you agree or disagree with them ***(Probe further whether 'fully' or 'somewhat' agree or disagree).***

Agree		Disagree		98. Can't say
1. Fully	**2. Somewhat**	**3. Somewhat**	**4. Fully**	

a. CCTV cameras footages can be accessed only by the person who has installed it

b. CCTVs cameras in public places can be used against women to monitor them

c. There is a risk of illegal mass surveillance in public places due to CCTVs cameras

Q5. If needed, would you like to share the data of CCTV cameras, installed by you in or around your house with the followings?

1. Yes **2. No** **98. Can't say** **99. Don't have CCTV**

a. With Police

b. With other authorities like RWAs or PWD

c. Company which installed CCTV cameras

d. With neighbours

Q6. Please tell me whether you agree or disagree with the following statements: ***(Probe further whether 'fully' or 'somewhat' agree or disagree).***

Agree		Disagree		98. Can't say
1. Fully	**2. Somewhat**	**3. Somewhat**	**4. Fully**	

a. CCTV cameras help to monitor and reduce crimes

b. CCTV cameras do not help in crime investigation

c. CCTV cameras in public places do not make you feel safer

Q7. What kind of mobile phone do you have - simple phone or smart phone?

1. Simple phone

2. Smartphone

3. Don't have own phone but use someone else's phone at home

4. Nobody has a phone at home

98. No response

Q8. Do you think these people can view your photos, messages, videos or searched objects from your phone or computer without your knowledge or consent?

1. Yes **2. No** **98. Can't say**

a. Police

b. Other government authorities

c. Telephone company or internet provider

d. Other private companies/ advertisers

e. Friends/colleagues

f. People in offices or place of work

g. Political parties

h. Family/spouse

i. Hackers

Q9. How much freedom should the police have to check your phone at any time without a warrant - complete, in some cases, or no freedom at all?

1. Complete freedom

2. In some cases

3. No freedom

98. Can't say

Q10. Do you do the following things on your phone or computer: **1. Yes** **2. No**

a. Use social media

b. Access Internet

c. Access Email account

Q11. ***(If option 1 in Q10a, Q10b and Q10c)*** How scared do you feel that if you post your opinions about a political or social issue on social media,and if it hurts the sentiments of certain groups, there might be legal action against you – very scared, somewhat scared, least scared or not at all scared?

1. Very scared

2. Somewhat scared

3. Least scared

4. Not at all

98. Can't say

Q12. ***(If option 1 in Q10a, Q10b and Q10c)*** How anxious are you that this might happen to you - very anxious, somewhat anxious, least anxious or not at all anxious?

1. Very **2. Somewhat** **3. Least** **4. Not at all** **98. CS**

a. An unknown person or company can access your e-mail account

b. An unknown person or company can access your WhatsApp or other social media accounts

c. An unknown person or company can know what you search for on Google or other search engines

d. An unknown person or company can know what you download, read or watch on the Internet or your phone

e. Information you provide for one purpose online can be used for another purpose

f. Someone else can damage your reputation by posting about you online

g. Your bank account transactions can be tracked by an unknown person or company

h. An unknown person or company can steal your digital identity ***(like using your personal information to create fake profiles, clone your banking data, etc.)***

i. Your personal data such as Adhaar number, PAN number, etc. can be leaked online

Q13. ***(If option 1 in Q10a, Q10b and Q10c)*** How comfortable do you feel while making digital or online transactions using the following modes – very, somewhat, not much or not at all comfortable?

1. Very **2. Somewhat** **3. Not much** **4. Not at all** **98. CS** **99. No account**

a. Paytm, Phone Pay, and other digital wallets

b. Debit or credit card online transactions

c. Net banking

d. UPI such as BHIM app, Google pay, etc.

Q14. Has it ever happened to you or someone close to you that someone else shared your personal photos and videos online without your permission?

1. Yes

2. No

98. Don't remember

Q14a. ***(if option 1 in Q14)*** So, with whom did this happen? ***(post-coding will be done later)***

____

Q15. Have you or someone close to you, ever lost money from your bank account due to online fraud?

1. Yes

2. No

98. Don't remember

Q15a. ***(if option 1 in Q15)*** So, with whom did this happen? ***(post-coding will be done later)***

____

Q16. How safe do you think these security measures are - very, somewhat, very little or not at all safe?

1. Very **2. Somewhat** **3. Very little** **4. Not at all** **98. CS**

a. Creating your own password according to the instructions

b. OTP verification by bank on your registered mobile/email prior to payment

c. Bank alerts for every transaction made after payment

Q17. To what extent, do you think your phone has fool-proof privacy, i.e. nobody else can access to its contents like photos, messages, videos or surfing history without your permission – to a great extent, to some extent, very little or not at all?

1. To a great extent

2. To some extent

3. Very little

4. Not at all

98. Can't say

Q18. Private companies, in general, collect data in the name of improving their services to deliver products that are more relevant to the consumers. How concerned do you feel that this information can be misused - to a great extent, somewhat, very little or not at all?

1. To a great extent

2. Somewhat concern

3. Very little

4. Not at all concern

98. Can't say

Q19. According to you, how helpful are the data collected by private companies from customers like you for these things– very helpful, somewhat helpful, not very helpful or not at all helpful?

1. Very **2. Somewhat** **3. Not very helpful** **4. Not at all helpful** **98. CS**

a. Ads are shown to you according to your interests

b. You don't have to enter your card/ payment details every time when you make a purchase

c. You get calls and messages regarding products and services you might be interested in

d. You get news or other information as per your interest

Q20. Do you think that private companies share or sell your data or information collected from you, such as purchase history, online activity and personal details with other companies or business promotors?

1. Yes

2. Maybe some data

3. No

98. Can't say

Q21. How frequently do you receive advertisements or targeted messages based on these activities – Frequently, sometimes or never?

1. Frequently **2. Sometimes** **3. Never** **98. No response**

a. Based on what you search online

b. Based on your likes on social media

c. Based on your conversations on phone

d. Based on your conversations on messaging apps such as WhatsApp, Facebook messenger, etc.

e. Based on your face-to-face conversations with someone

Q22. Do you think it would be right or wrong for the government to do these things?

1. Right **2. Right, but in some cases** **3. Wrong** **98. Can't say**

a. Monitor what you post on social media or the Internet

b. Find out who you talk to on the phone

c. Track your online/phone activity like what you download, read or watch

d. Restrict what you write or share on social media or internet

e. Track your location

f. Create your social and financial profile by collecting information from different sources

Q23. Do you support or oppose legal action against people who criticize the government and its laws or policies on social media? ***(Probe further whether 'fully' or 'somewhat' support or oppose)***

1. Fully support

2. Somewhat support

3. Somewhat oppose

4. Fully oppose

98. No opinion

Q24.Do you think that to prevent abuse of power, investigative agencies must obtain a search warrant before checking or tracking anyone's phone or computer/laptop?

1. Yes, always

2. Yes, but in some cases

3. No

98. No opinion

Q25. Do you support or oppose the linkage of Aadhar with the following items?

1. Support **2. Don't support** **98. No response** **99. Don't have Aadhar card**

a. Bank/ PAN

b. Mobile number

c. Voter ID

d. Welfare schemes such as pension scheme, ration, LPG cylinder etc.

e. Access to vaccines and health services

Q26. How comfortable do you feel in sharing your Aadhaar number with private companies such as telephone companies or internet service provider sand banks, etc. – very much, somewhat, very less or not at all comfortable?

1. Very much

2. Somewhat

3. Very less

4. Not at all

98. Can't say

99. Do not have Aadhar number

Q27. Do you think the police should be able to collect the biometric details (such as fingerprint, footprint, iris, retina scan, facial recognition, etc.) of all suspects, including those who haven't been declared guilty by the court?

1. Yes

2. No

98. Can't say

Q28a. To what extent do you support or oppose the use of drones by the following agencies? ***(Probe further 'strongly' or 'somewhat' support or oppose).***

Support Oppose 98. CS 99. Not aware about drones

1. Fully 2. Somewhat 3. Somewhat 4. Fully

a. By the government

b. By private companies or agencies

c. By individuals

d. By police

e. By armed forces

Q28b. To what extent do you support or oppose the use of facial recognition technology (FRT) by following agencies? ***(Probe further 'strongly' or 'somewhat' support or oppose)***.

Support Oppose 98. CS 99. Not aware about FRT

1. Fully 2. Somewhat 3. Somewhat 4. Fully

a. By the government

b. By private companies or agencies

c. By individuals

d. By police

e. At traffic signals

Q29. To what extent do you think it's justified for the government to use the following technologies to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

1. To a great extent 2. To some extent 3. Very little 4. Not at all 98. CS

a. Through CCTV cameras

b. Through mobile surveillance such as phone tapping, hacking

c. Through Facial Recognition Technology (FRT) that recognizes faces and identifies people

d. Through drones

e. Through voice recognition technique

Q29a. Could you suggest the name of other type of technology that can be used to curb political movement or protests against policies & laws enforced by the government? ***(Please note down the exact response, the coding will be done later at CSDS)***.______________________________ 98. Can't say/Don't know

Q30. In your opinion, to what extent is the use of drones justified in the following cases - to a great extent, to some extent, very little or not at all?

1. To a great extent 2. To some extent 3. Very little 4. Not at all 98. CS

a. Enforcement of rules and regulations by the police; for example, enforcing a lockdown during a pandemic

b. For regular surveillance of the public by the government or police

c. For providing services and essential goods to the public during difficult times such as droughts, famines, natural calamities, etc.

d. To provide services and essential goods to the public by private companies

Q31. How worried do you feel that drones could be misused to collect data/photos of people like you - a lot, somewhat, least worried or not at all worried?

1. A lot

2. Somewhat

3. Least worried

4. Not at all worried

98. Can't say

Q32. To what extent is the use of Facial Recognition Technology (FRT)by the police or the government justified in the following circumstances - to a great extent, to some extent, very less or not at all?

1. To a great extent 2. To some extent 3. Not much 4. Not at all 98. CS

a. To keep a database of people who have been convicted of offences

b. To keep a database of people who have been charged, but not convicted

c. To keep a database of people who have been convicted for serious offences such as rape, sexual assault, crimes against children, etc.

d. To identify people who participate in protests against government policies or laws

e. To identify people who engage in communal riots and disturb law and order

f. To identify any common citizen, even if they have not committed any crime

Q33. Have you been challaned at traffic signal through the CCTV?

1. Yes

2. No

98. Don't remember

Q34. Which of the following statements do you agree with the most?

Sentence 1. The government should consult experts before making rules and regulations for using advanced surveillance technologies like FRT and drones.

Sentence 2. The government can make its own rules and regulations for using advanced surveillance technologies like FRT and drones without any outside consultation.

1. Agree with 1st statement

2. Agree with 2nd statement

98. Can't say

Q35. How anxious do you feel while sharing your GPS location with the following - very anxious, somewhat anxious, very little or not at all anxious?

1. Very 2. Somewhat 3. Very little 4. Not at all 98. CS 99. Never shared

a. With the police

b. With apps such as Swiggy, Zomato, Amazon etc.

c. With family/spouse

d. With employer

e. With apps that ensure women's safety ***(Ask to women)***

Q36. How comfortable do you feel while sharing this information with an app or website on your phone or computer - very conformable, somewhat comfortable, very little or not at all comfortable?

1. Very 2. Somewhat 3. Very little 4. Not at all 98. CS 99. Never shared

a. Contact list

b. Date of birth

c. Camera or media access

d. Phone or computer storage

e. Microphone access

Q37. How worried do you feel that the medical information provided by you to the hospitals/doctors can be shared with other companies or institutions– very worried, somewhat worried, least worried or not at all worried?

1. Very worried

2. Somewhat worried

3. Least worried

4. Not at all worried

98. CS

Q38. How comfortable do you feel in sharing your medical history while using the following apps/websites - very comfortable, somewhat comfortable, little or not at all comfortable?

1. Very 2. Somewhat 3. Little 4. Not at all 98. Can't say 99. Never used

a. Cowin

b. Arogyasetu app

c. Telemedicine apps like practo or Lybrate, Mfineetc

d. Online pharmacy apps like PharmEasy, Tata 1mg, Apollo Pharmacy etc.

Q39. Do you know about the Supreme Court case of 2017, Puttuswamy vs Union of India, which declared privacy as a fundamental right?

1. Yes

2. No

Q39a. ***(If option 1 in Q39)*** To what extent do you agree or disagree with the judgement? ***(Probe further 'fully' or 'somewhat' agree or disagree).***

1. Fully agree

2. Somewhat agree

3. Somewhat disagree

4. Completely disagree

98. Can't say

Q40. Have you heard of the Pegasus software which was used by governments of various countries, including India,to listen to the calls and read the messages of some people, including politicians, journalists and judges?

1. Heard

2. Not heard

98. Don't remember

Q41. Should the government use Pegasus or similar software for phone hacking, location tracking etc. of these people, even if there is no criminal case against them?

1. Yes **2. Yes, in some cases** **3. No** **98. Don't know**

a. Journalist

b. Judge

c. Lawyer

d. MP/MLA

e. Other politicians

f. Suspected criminal

g. Ordinary citizens

h. Businessman

i. Bureaucrat

j. NGO/ Social worker

Q42. In your opinion, should the government establish independent forums where people can complain against digital breach of privacy or illegal surveillance by:

1. Yes **2. Maybe** **3. Not required** **98. CS**

a. Private companies

b. Government agencies such as the police

Q43. Whom will you approach for the redressal, in case of privacy breach? ***(Respondent can give multiple responses)***

1. Police/cybercime unit

2. Judiciary

3. Media

4. NGOs, social activists

97. Other ***(specify)*** _____

98. Don't know

99. Never experienced

Q44. Which of the following statements, do you agree with **the most?**

a. It is the individuals' responsibility to ensure that they protect their data against any kind of illegal surveillance, hacking or cybercrime

b. It is the responsibility of the government to enforce data protection laws and educate its citizens about the right to privacy

1. Agree with statement 1

2. Agree with statement 2

3. Both

98. Can't choose

Q45. To investigate any crime, the police should be able to tap phone and check CCTV cameras of the following persons, linked with that case, without any kind of warrant or permission. Please tell me whether you agree or disagree with this. ***(Probe further whether 'fully' or 'somewhat' agree or disagree).***

Agree **Disagree** **98. Can't say**

1. Fully **2. Somewhat** **3. Somewhat** **4. Fully**

a. The accused

b. The victim

c. Any other person who may have relevant information linked with related to the case

Q46. In the last 4-5 years, to what extent the use of the following technologies by the police has increased in your locality – has it increased a lot, to some extent, a little or never used by the police?

1. A lot **2. To some extent** **3. A little** **4. Police Never used** **98. CS**

a. CCTV

b. Mobile surveillance such as phone tapping or phone checking

c. Facial Recognition Technology (FRT)

d. Drones

Q47. Now I will ask you about some such incidents which happened due to wrong use of techniques. Please tell me whether you are aware about such incidents or not?

1. Yes **2. No**

a. In other countries, FRT has misidentified people

b. The footage of the CCTV camera has been manipulated or tampered with

Q48. To what extent do you think the police in your locality has received adequate training to use and to storage data of technologies like CCTV cameras, drones or FRT – adequately trained, trained to some extent, less trained or not at all trained?

1. Adequately trained
2. To some extent
3. Less trained
4. Not at all

98. Can't say

Q49. To what extent do you think CCTV cameras in police stations can help in reducing police abuse, torture and human rights violations against people in custody – to a large extent, to some extent, very little or not at all?

1. To a great extent
2. To some extent
3. Very little
4. Not at all
5. No need to install CCTV cameras in police stations

98. Can't say

Q50. In your opinion, how important it is for any interrogation in a police station to be videographed through CCTVcameras–very important, somewhat important, less important or not at all important?

1. Very important
2. Somewhat important
3. Less important
4. Not at all important

98. Can't say

Q51. In your opinion, are technologies like CCTV cameras, mobile surveillance/tapping or FRT used by the police or the government more likely to target certain groups or communities?

1. Yes

2. No

98. Can't say

Q51(a). (If option 1 in Q51) So which community do you think, is more likely to be targeted? ***(Please note down the answer and post-coding will be done at Lokniti-CSDS*** ______________________________ 98. No Response

Q52. In your opinion, in which of the following localities it is more important to use surveillance technologies like CCTV cameras, mobile surveillance or phone tapping, etc. to reduce or control crimes:

Option 1 **Option 2** **3. Both** **4. Neither** **98. Can't say**

a. 1. In posh colonies with big houses or 2. Slums

b. 1. In upper caste localities or 2. Dalit basti

c. 1. In Hindu localities or 2. Muslim localities

d. 1. In non-Adivasilocalities or 2. Adivasi localities

Q53. To what extent do you think these things happen in our country - all the times, sometimes, rarely or never?

1. All the time **2. Sometimes** **3. Rarely** **4. Never** **98. CS**

a. Political parties use surveillance and snooping techniques for winning elections

b. Private companies or NGOs collect common people's data in order to influence their electoral choices

c. Private companies, NGOs and political parties work together to spread fake news on the internet

d. Elected governments of country snoop on their own citizens illegally

Background

Z3. How many elders (18+) and children (under 18) are there in your household? ***(Note the exact number for each; code 0 if there are no children and code 9 if more than 9 members)***

a. Above 18 years ____________________

b. Below 18 years ______________________

Z4. Upto what level have you studied?

1. Non-literate (Can't read or write at all)

2. Below Primary Class

3. Primary Pass (Class 5)

4. Middle Pass (Class 8)

5. Matriculation Pass (Class 10)

6. Studying in class 11th or 12th or junior college

7. Inter Pass (Class 12)

8. Diploma (after class X or XII)

9. Graduate or doing graduation/in college

10. Post-graduate/ doing post-graduation

11. Higher Degree (MPhil, PhD)

12. Professional courses/degree (law, engineering etc.).

98. Did not respond

Z5. What is your main occupation? **(Note down the response and then click on suitable option below; if retired, try to ascertain his/her previous occupation, if student or housewife, then note down that as well)** ____

01. Higher professionals: Engineers, Doctors, Lawyers, Chartered Accountants, Professors etc.

02. Lower professionals: Computer Operator, Data Entry, Ayurvedic Doctor, Nurse, School Teacher, Tutor, Priest, Astrologer, NGO worker etc.

03. Government managerial job: Manager, Director, Executive, MP, MLA etc.

04. Government administrative job: First-Second Class Officer, Major in Army, Colonel, Brigadier, Police Inspector

05. Government clerical jobs: Class III Officers, Clerk, Typist, Army Jawan, Police Constable etc.

06. Government class IV: Peon, Postman, Gram Sevak, Amin, Safai Karamchari etc.

07. Big and medium traders: Big Shopkeepers, Factory Owners, Hotel Owners, Petrol Pumps, Taxi Owners, Big Travel Agency, Small Hotels, Property Dealers, Jewelers etc.

08. Small trader: Grocery Shop, Small Travel Agency, Phone Booth, Broker, Parlour, Rickshaw Owner, Landlord

09. Small/temporary business: Temporary Shopkeeper, Sales Man, Delivery Boy, Shop Assistant etc.

10. Service/Service area: Cook, Waiter, Washerman, Barber, Domestic Servant, Chowkidar, Private Guard, Safai Karamchari etc.

11. Skilled workers: Driver, Mechanic, Electrician, Plumber, Jeweler, Tailor, Cobbler, Carpenter, Sailor

12. Semi-skilled workers: Artisans, bricklayers, potters, stone cutters, furniture, basketry, mat makers etc.

13. Wage labourer: Rickshaw pullers, loaders, construction workers etc.

14. Farmer: tilling own land or someone else's land

15. Agricultural labourer: Landless farm labourers

16. Dairy/Fish/Poultry/Animal husbandry work

17. Student (maybe working part time)

18. Housewife / Housewife / Live at home (maybe doing some small work to earn some money)

19. Unemployed or looking for employment

97. Any other work ***(specify)*** ________

98. Did not tell

Z5a. Are you the main earner in the family?

1. Yes

2. No

Z5b. ***(If option 2 in Z5a)*** What is the occupation of the main earner of the household?

(Note down the response and then click on suitable option below; if retired, try to ascertain his/her previous occupation, if student or housewife, then note down that as well) ______________________________ ____

01. Higher professionals: Engineers, Doctors, Lawyers, Chartered Accountants, Professors etc.

02. Lower professionals: Computer Operator, Data Entry, Ayurvedic Doctor, Nurse, School Teacher, Tutor, Priest, Astrologer, NGO worker etc.

03. Government managerial job: Manager, Director, Executive, MP, MLA etc.

04. Government administrative job: First-Second Class Officer, Major in Army, Colonel, Brigadier, Police Inspector

05. Government clerical jobs: Class III Officers, Clerk, Typist, Army Jawan, Police Constable etc.

06. Government class IV: Peon, Postman, Gram Sevak, Amin, SafaiKaramchari etc.

07. Big and medium traders: Big Shopkeepers, Factory Owners, Hotel Owners, Petrol Pumps, Taxi Owners, Big Travel Agency, Small Hotels, Property Dealers, Jewelers etc.

08. Small trader: Grocery Shop, Small Travel Agency, Phone Booth, Broker, Parlour, Rickshaw Owner, Landlord

09. Small/Temporary business: Temporary Shopkeeper, Sales Man, Delivery Boy, Shop Assistant etc.

10. Service/Service area: Cook, Waiter, Washerman, Barber, Domestic Servant, Chowkidar, Private Guard, SafaiKaramchari etc.

11. Skilled workers: Driver, Mechanic, Electrician, Plumber, Jeweler, Tailor, Cobbler, Carpenter, Sailor

12. Semi-skilled workers: Artisans, bricklayers, potters, stone cutters, furniture, basketry, mat makers etc.

13. Wage labourer: Rickshaw pullers, loaders, construction workers etc.

14. Farmer: tilling own land or someone else's land

15. Agricultural labourer: Landless farm labourers

16. Dairy/Fish/Poultry/Animal husbandry work

17. Student (maybe working part time)

18. Housewife / Housewife / Live at home (maybe doing some small work to earn some money)

19. Unemployed or looking for employment

97. Any other work ***(specify)*** ________

98. Did not tell

Z6. Are you married?

1. Yes

2. Yes, widowed

3. Yes, but separated

4. Yes but divorced

5. No, Single/unmarried

98. Did not respond

Z7. Which religion do you belong to?

1. Hindu

2. Muslim

3. Christian

4. Sikh

5. Buddhist/Neo-Buddhist

6. Jain

7. Parsi

97. Other religion ***(specify)***________

99. Atheist

Z8. And what is your caste group?

1. Scheduled Caste (SC)

2. Scheduled Tribe (ST)

3. Other Backward Classes (OBC)

4. General

Z8a. What is your Caste/Jati-biradari/Tribe name? **(Note down the response and then click on suitable option below** ____

1. Brahmin

2. Other upper caste

3. Peasant proprietors

4. Upper OBCs
5. Service OBC
6. SCs
7. STs
30. Muslims
31. Sikhs
32. Christians
97. Other ***(specify)*** ______________________
98. No response

Z9. Type of house where Respondent lives
1. House/Flat/Bunglow
2. House/Flat with 5 or more rooms
3. House/Flat with 4 rooms
4. Houses/Flat with 3 rooms
5. Houses/Flat with 2 rooms
6. House with 1 room
7. Mainly Kutcha house
8. Slum/JhuggiJhopri

Z10. Do you or members of your household have the following: **1. Yes** **2. No**
a. Car/Jeep/Van
b. Own auto or e-rickshaw
c. Scooter / Motorcycle / Moped
d. Air Conditioner (AC)
e. Electric fan
f. Cooler
g. Washing machine
h. Fridge
i. Bank account
j. Credit Card
k. Indoor toilet (or adjacent to the house that only belongs to you)
l. Your own house

Z11. What's your monthly household income after putting together the income of all members? ***(First note down the response in the space given below and then click on the right/most suitable option from the menu provided)*** ____

01. Upto 1,000
02. 1,001 to 2,000
03. 2,001 to 3,000
04. 3,001 to 5,000
05. 5,001 to 7,500
06. 7,501 to 10,000
07. 10,001 to 15,000
08. 15,001 to 20,000
09. 20,001 to 30,000
10. 30,001 to 50,000
11. Over 50,000
98. No answer

APPENDIX 4

Code Sheet SPIR 2022 - Media Content Analysis Form

*Required

1. Coder's Name*

   ____

2. Link of the story*

   ____

3. Story headline

   ____
   ____
   ____

4. Name of the Outlet*

   Mark only one oval.

   ○ Times of India
   ○ The Indian Express
   ○ The Print
   ○ Dainik Bhaskar
   ○ Dainik Jagran
   ○ The Wire

5. Language*

   Mark only one oval.

   ○ Hindi
   ○ English

6. Author/Agency/ Pickup Publication Name

   ____

7. Publication/Updated On*

   ____

   Example: January 7, 2019

8. Date line

   ____

9. Content Category*

   Mark only one oval.

○ Hard news story
○ Editorial/Op-ed/Opinion
○ Explainer
○ Business/Economy etc.
○ News features
○ Magazine/lifestyle
○ Other:

Prominence

10. No. of Words

____

11. Subheading*

Mark only one oval.

○ Yes

○ No

12. Value addition*

Check all that apply.

○ Picture/Visuals chart/Graphics/Map

○ Cartoon

○ Embedded video/audio

○ No visuals

○ Other: ______________________________

13. Visual remarks

____

____

14. Story type

Mark only one oval.

○ By line story

○ Agency copy

○ Staff/Desk reporter

○ By Paper's correspondent

○ Standalone cartoon

○ Standalone picture

○ Pick up from other publications

○ Editorial without author

○ Opinion

○ Others: ______________________________

15. Origin of the story

Mark only one oval.

○ Govt. order

○ Press conference / Press release

○ On the spot reporting

○ Exclusive Report - Own investigation

○ International journalistic collaboration

○ Parliament proceedings

○ Assembly proceedings

○ Dharna / Protest rally

○ Public meeting

○ Expert view

○ Conference / Seminar / Webinar / Report release or other similar events

○ Public statement by key stakeholders/ politicians/ authorities

○ Social media content/comments

○ TV / Radio programs

○ Court proceedings

○ Study / Research report

○ Personal/agency opinion

○ Police complaint/report (FIR)

○ Other: ______________________________

16. Primary source of the story

Mark only one oval.

○ Prime Minister

○ Home Minister- Center

○ Home Minister- State

○ Top Central government officials

○ Top State government officials

○ Other government officials

○ Police

○ Leader of opposition

○ Other senior opposition leaders

○ The Chief Minister

○ Local MLA/MP

○ Other ruling party representatives/sources (Center-Level)

○ Other opposition party representatives/sources (Center-Level)

○ Other ruling party representatives/sources (State-level)

○ Other opposition party representatives/sources (State-level)
○ Senior or local bureaucrat
○ Sarpanch/ Panchayat leader/ Urban local body leader/ other local elected representative
○ Supreme court/ High court
○ Lower court
○ Civilians
○ NGOs/ Civil society organizations
○ Trade unions
○ Academic studies/ report experts/ academics
○ Without source
○ Unidentified sources
○ First person account
○ Journalistic investigations
○ Other: ____

17. Name/ Designation

Primary source of the story

____

18. Are the following mentioned in the story:

Mark only one oval per row.

	Yes	No	Unclear
Police	○	○	○
Prisons	○	○	○
Judiciary	○	○	○

19. Does the story talk about following:

Mark only one oval per row.

	Yes	No	Unclear
Surveillance	○	○	○
Legality of surveillance	○	○	○
Constitutionality of surveillance	○	○	○
Right to privacy	○	○	○

20. Who is conducting/organizing surveillance?

Check all that apply.

○ Police
○ Local government
○ Public welfare department intelligence agencies
○ Any other government authority (please specify)
○ Residential welfare associations school/college/university/hospital/court administration
○ Transport authority
○ Private companies individual(s) unknown

○ Central government

○ State government

○ Ruling political party other political party

○ Other: ____________________

21. Specify

Related to previous question (Any other government authority)

____

22. Main actors

Check all that apply.

○ Central government

○ State government

○ Police

○ Intelligence agencies

○ Other security forces

○ Armed forces

○ Other state actors (specify)

○ Digital intermediaries/social media platforms (specify)

○ Private actors (individuals) (specify)

○ Private actors (business entities)

○ Public-Private partnership

○ NGOs/ Civil society groups/ charities

○ UN// World bank/ IMF/ other multilateral organizations

○ Ruling party

○ Opposition party

○ People's movement/ street protest

○ Domain experts

○ Courts and judges

○ Foreign governments

○ No agent specified

○ Army officials

○ Top defense officials

○ Human rights officials

○ Maoists/ Naxalites/ Guerrilla fighters

○ RWA

○ Top police officials

○ CISF officials

○ Peer-pressure groups

○ Other: ____________________

23. Name of the main actors

Part of previous question

____

24. Mode of surveillance

Check all that apply.

○ Illegal phone tapping

○ Authorized phone tapping

○ GPS/IP/Phone location tracing

○ CCTV

○ FRT

○ Drones

○ Hacking Phone/personal devices

○ Pegasus

○ Spywares, malwares, etc.

○ Other tools of hacking /personal devices

○ Video surveillance in personal spaces/through hacking of personal devices

○ RFID chips/tags

○ Stingray devices

○ Biometric data

○ GPS on vehicles

○ Automatic Number Plate Recognition (ANPR)

○ Body Cams

○ Other: ____

Frames

25. Does the story fall under following frame?*

Check all that apply.

○ Human rights

○ National security

○ Public safety

○ Technology

Human Rights Frame

26. Human rights frame category

Check all that apply.

○ Individual's Privacy/ Snooping/ Spying

○ Freedom of expression

○ Freedom of movement

○ Data privacy

○ Data protection

○ Medical information

○ Discrimination against/targeting Minority

○ Discrimination against/targeting caste

○ Discrimination against/targeting poor

○ Discrimination against/targeting Women

○ Discrimination against/targeting Sexual/Gender

○ Minorities violation of freedom of religion/faith

○ Aadhaar

○ Legality/Constitutionality

○ Controlling/Criminalizing dissent

○ Hate Speech

○ Controlling political opposition

○ Falsely implicating someone by planting digital evidence

○ Other: ____________________

National Security Frame

27. National security frame category

Check all that apply.

○ Cross border security

○ Terrorism

○ Separatism/ Insurgency

○ Maoism / Naxalism

○ Seditious/ anti-national acts

○ Maritime security

○ Internal conflict

○ Inciting violence/public unrest

○ Data protection

○ Cyberattacks

○ Debarring or preventing trespassing of unauthorized persons

○ Other: ____________________

Public Safety Frame

28. Public safety frame category

Check all that apply.

○ Women safety

○ Child safety

○ Sexual/Gender minorities

○ Crime reduction

○ Crime solved
○ Criminal investigation
○ Crime prevention
○ Compromising medical/financial/sensitive data of an individual
○ CCTV footage access/storage
○ Drone footage access/storage
○ Cyber crimes (specify)
○ Road safety
○ Big data for crime prevention
○ The demand for surveillance for public safety
○ Contact tracing application
○ Maintaining public order
○ Other: ____________________

29. Cyber crime (specify) related to previous question

____

Technology Frame

30. Technology frame category

Check all that apply.

○ FRT
○ GPS tracking
○ Algorithm
○ IOT
○ Smart watch
○ Smart cities
○ Interception of SMS/Email
○ Spyware, malware, etc.
○ CCTVs
○ Other video surveillance devices
○ Unauthorized access to personal cameras
○ Drones surveillance
○ Phone tapping
○ Pegasus
○ IP tracing
○ RFID chips/tags
○ Stingray devices
○ Biometric data
○ Police body cameras
○ Audio surveillance
○ Night vision technology (Camera)
○ Contact tracing application
○ Other: ____________________

Concluding Part

31. Story slant (vis-a-vis government)

Mark only one oval.

○ Clear pro-government slant

○ Clear anti-government slant

○ No discernible Slant

32. Approach to surveillance

Mark only one oval.

○ Supportive

○ Critical

○ No discernible approach

33. Remarks to previous question, if any

____

____

34. Does the story talk about the impact of surveillance on individuals?

Mark only one oval.

○ Yes

○ No

○ Unclear

35. Remarks to previous question, if any

____

____

36. Does the story talk about the use of big data technology?

Mark only one oval.

○ Yes

○ No

○ Unclear

37. Remarks to previous question, if any

____

____

38. Does the story talk about the differential impact of surveillance on certain groups/ communities?

Mark only one oval.

○ Yes

○ No

○ Unclear

39. Remarks to previous question, if any

____

____

40. Does the story raise issues of the possible misuse of surveillance technology?

Mark only one oval.

○ Yes

○ No

○ Unclear

41. Remarks to previous question, if any

____

____

42. Does the story cover legal aspects of the surveillance technologies/processes?

Mark only one oval.

○ Yes

○ No

○ Unclear

43. Remarks to previous question, if any

____

____

44. (If the story is about the police) Does the story talk about the police capacity touse/store surveillance technology and data?

Mark only one oval.

○ Yes

○ No

○ Unclear

○ Not about police

45. Remarks to previous question, if any

____

____

46. (If the story is about any government authority, including police) Does the story mention the role of any private players in the management, storage, etc. of the surveillance technology?

Mark only one oval.

○ Yes

○ No

○ Unclear

○ Not about police/govt authority

47. If yes to the above question, mention the name of the private company. Also note remarks, if any

____

____

48. Does the story talk about any grievance redressal in case of misuse/complaints against surveillance technologies?

Mark only one oval.

○ Yes

○ No

○ Unclear

49. Remarks to the above question, if any

____

____

50. Does the story talk about the funding/budgeting of surveillance technology?

Mark only one oval.

○ Yes
○ No
○ Unclear

51. If yes in above question, mention the type of funder (Public, Private etc.) and the name

____

____

52. Does the story mention the installation of any surveillance technology?

Mark only one oval.

○ Yes

○ No

○ Unclear

53. If yes, what type of surveillance technology

Check all that apply.

○ CCTV

○ Drone

○ Facial Recognition Technology

○ Stingray devices

○ Body cameras

○ Biometrics RFiD chips

○ Big data analysis spywares

○ Audio recognition technology

○ Other: ____________________________________

54. If yes to the above, what is the stated purpose for the installation of the technology?

____

____

55. Overall remarks

____

____

APPENDIX 5

Details of Indices Used in Analysis

Index 1: Users of digital platforms

The Index was constructed by taking into account 3 questions asked in the survey. They are: -

Q10. Do you do the following things on your phone or computer:

Q10a. Use social media

Q10b. Access Internet

Q10c. Access Email account

In each question, the response options offered to the respondent were 'yes', or 'no'.

Step 1: A 'yes' answer was scored as 1 and a 'no' answer as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 3.

Step 3: These summated scores were then distributed into two newly created categories: -

1. A total score of 0 was categorized as "Non-user of digital platforms"
2. A total score of 1, 2 and 3 were categorized as "Users of digital platforms".

Index 2: People's perception on digital intrusion

The Index was constructed by taking into account 9 questions asked in the survey. They are: -

Q8. Do you think these people can view your photos, messages, videos or searched objects from your phone or computer without your knowledge or consent?

Q8a. Police

Q8b. Other government authorities

Q8c. Telephone company or internet provider

Q8d. Other private companies/ advertisers

Q8e. Friends/colleagues

Q8f. People in offices or place of work

Q8g. Political parties

Q8h. Family/spouse

Q8i. Hackers

In each question, the possible response options were 'yes' and 'no'.

Step 1: A 'yes' answer was scored as 1 and a 'no' answer or no response was scored as 0. Across all the questions, a no response category was also provided, in case the respondent refused to answer the question.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 9.

Step 3: These summated scores were then distributed across four newly created categories that indicated different levels of people's perception on digital intrusion –

1. A total score of 0 was categorised as 'No intrusion at all'.
2. A total score of 1 to 2 was categorised as 'A little intrusion'.
3. A total score of 3 to 4 was categorised as 'Some intrusion.
4. A total score of 5 to 9 was categorised as 'High intrusion'.

Index 3: Support for targeted digital surveillance by the Government

The Index was constructed by taking into account 6 questions asked in the survey. They are:

Q22. Do you think it would be right or wrong for the government to do these things?

Q22a. Monitor what you post on social media or the Internet

Q22b. Find out who you talk to on the phone

Q22c. Track your online/phone activity like what you download, read or watch

Q22d. Restrict what you write or share on social media or internet

Q22e. Track your location

Q22f. Create your social and financial profile by collecting information from different sources

In each question, the response options offered to the respondent were 'right', 'right, but in some cases', or 'wrong'. Across all the questions, a can't say category was also provided, in case the respondent refused to answer the question.

Step 1: A 'right' answer was scored as 3 and a "right, but in some cases' answerwas scored as 2, a 'wrong' answer was scored as 1 and a no response was scored as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 18.

Step 3: These summated scores were then distributed across four newly created categories that indicated different levels of support for Individual digital surveillance by the Government –

1. A total score of 0 was categorised as 'No opinion'.
2. A total score of 1 to 6 was categorised as 'Least support'.
3. A total score of 7 to 12 was categorised as 'Somewhat support'.
4. A total score of 13 to 18 was categorised as 'Strong support'.

Index 4: Support for mass surveillance by the government through various technologies

The Index was constructed by taking into account 5 questions asked in the survey. They are:

Q29. To what extent do you think it's justified for the government to use the following technologies to curb political movement or protests against policies & laws enforced by the government - to a great extent, to some extent, very little or not at all?

Q29a. CCTV cameras

Q29b. Mobile surveillance such as phone tapping, hacking

Q29c. Facial Recognition Technology (FRT) that recognizes faces and identifies people

Q29d. Drones

Q29e. Voice recognition technique

In each question, the response options offered to the respondent were 'To a great extent', 'To some extent', 'Very little', or 'Not at all'. Across all the questions, a can't say category was also provided, in case the respondent refused to answer the question.

Step 1: 'To a great extent' answer was scored as 4, a 'To some extent' answer was scored as 3, a 'Very little' answer was scored as 2, a 'not at all' answer was scored as 1 and a no response was scored as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 20.

Step 3: These summated scores were then distributed across four newly created categories that indicated different levels of support for mass surveillance by the government through various technologies –

1. A total score of 0 was categorised as 'No opinion'.
2. A total score of 1 to 8 was categorised as 'Least support'.
3. A total score of 9 to 14 was categorised as 'Somewhat support'.
4. A total score of 15 to 20 was categorised as 'Strong support'.

Index 5: Support for drone surveillance by government agencies

The Index was constructed by taking into account 3 questions asked in the survey. They are:

Q28a. To what extent do you support or oppose the use of drones by the following agencies?

Q28aa. By the government

Q28ad. By police

Q28ae. By armed forces

In each question, the response options offered to the respondent were 'Fully support', 'Somewhat support', 'Somewhat oppose', or 'Fully oppose. Across all the questions, 'can't say' and 'not aware about drones' categories were also provided, in case the respondent refused to answer the question or not aware about the drone technology.

Step 1: 'Fully support' answer was scored as 4, a 'Somewhat support' answer was scored as 3, a 'Somewhat oppose' answer was scored as 2, a 'Fully oppose' answer was scored as 1 and 'can't say' and 'not aware about drones' were clubbed together and scored as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 12.

Step 3: These summated scores were then distributed across three newly created categories that indicated different levels of support for drone surveillance by government agencies –

1. A total score of 0 was set as system missing.
2. A total score of 1 to 6 was categorised as 'Low support'.
3. A total score of 7 to 10 was categorised as 'Moderate support'.
4. A total score of 11 to 12 was categorised as 'High support'.

Index 6: Support for drone surveillance by private actors

The Index was constructed by taking into account 2 questions asked in the survey. They are:

Q28a. To what extent do you support or oppose the use of drones by the following agencies?

Q28ab. By private companies or agencies

Q28ac. By individuals

In each question, the response options offered to the respondent were 'Fully support', 'Somewhat support', 'Somewhat oppose', or 'Fully oppose. Across all the questions, 'can't say' and 'not aware about drones' categories were also provided, in case the respondent refused to answer the question or not aware about the drone technology.

Step 1: 'Fully support' answer was scored as 4, a 'Somewhat support' answer was scored as 3, a 'Somewhat oppose' answer was scored as 2, a 'Fully oppose' answer was scored as 1 and 'can't say' and 'not aware about drones' were clubbed together and scored as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 8.

Step 3: These summated scores were then distributed across three newly created categories that indicated different levels of support for drone surveillance by private actors –

1. A total score of 0 was set as system missing.
2. A total score of 1 to 3 was categorised as 'Low support'.
3. A total score of 4 to 6 was categorised as 'Moderate support'.
4. A total score of 7 to 8 was categorised as 'High support'.

Index 7: Support for FRT surveillance by government agencies

The Index was constructed by taking into account 3 questions asked in the survey. They are:

Q28b. To what extent do you support or oppose the use of facial recognition technology (FRT) by following agencies?

Q28ba. By the government

Q28bd. By police

Q28be. At traffic signals

In each question, the response options offered to the respondent were 'Fully support', 'Somewhat support', 'Somewhat oppose', or 'Fully oppose. Across all the questions, 'can't say' and 'not aware about drones' categories were also provided, in case the respondent refused to answer the question or not aware about the drone technology.

Step 1: 'Fully support' answer was scored as 4, a 'Somewhat support' answer was scored as 3, a 'Somewhat oppose' answer was scored as 2, a 'Fully oppose' answer was scored as 1 and 'can't say' and 'not aware about drones' were clubbed together and scored as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 12.

Step 3: These summated scores were then distributed across three newly created categories that indicated different levels of support for FRT surveillance by government agencies –

1. A total score of 0 was set as system missing.
2. A total score of 1 to 6 was categorised as 'Low support'.
3. A total score of 7 to 10 was categorised as 'Moderate support'.
4. A total score of 11 to 12 was categorised as 'High support'.

Index 8: Support for FRT surveillance by private actors

The Index was constructed by taking into account 2 questions asked in the survey. They are:

Q28b. To what extent do you support or oppose the use of facial recognition technology (FRT) by following agencies?

Q28bb. By private companies or agencies

Q28bc. By individuals

In each question, the response options offered to the respondent were 'Fully support', 'Somewhat support', 'Somewhat oppose', or 'Fully oppose. Across all the questions, 'can't say' and 'not aware about drones' categories were also provided, in case the respondent refused to answer the question or not aware about the drone technology.

Step 1: 'Fully support' answer was scored as 4, a 'Somewhat support' answer was scored as 3, a 'Somewhat oppose' answer was scored as 2, a 'Fully oppose' answer was scored as 1 and 'can't say' and 'not aware about drones' were clubbed together and scored as 0.

Step 2: The scores of all questions were summed up. The summated scores of all questions ranged from 0 to 8.

Step 3: These summated scores were then distributed across three newly created categories that indicated different levels of support for FRT surveillance by private actors –

1. A total score of 0 was set as system missing.
2. A total score of 1 to 3 was categorised as 'Low support'.
3. A total score of 4 to 6 was categorised as 'Moderate support'.
4. A total score of 7 to 8 was categorised as 'High support'.

APPENDIX 6

RTI Applications

An RTI application was filed before the Public Information Officer, Public Works Department, Govt. of NCT of Delhi to seek information about the protocols surrounding CCTV cameras installed in public places across the Capital.

1. How many CCTV Cameras have been installed by PWD in the public places across Delhi?
2. Who monitors the CCTV footage collected across Delhi?
3. Who can access the data gathered through CCTV?
4. What are the standard operating procedures for accessing the data gathered through CCTV?
5. Whether officers are trained to deal with CCTV Equipment?
6. If yes, what is the minimum eligibility criteria for such training?
7. Whether officers are trained to analyse the data gathered through CCTV?
8. If yes, what is the minimum eligibility criteria for such training?
9. How long the data gathered through CCTV stored?
10. What are the guidelines concerning the storage of data collected through CCTV?
11. What are the guidelines concerning the disposal of data collected through CCTV?
12. What are the activities delegated to the third parties (start-ups, private companies, etc.)?

PWD gave the following question-wise response (as of January 31, 2022):

S. No.	Information
1.	Till date 133253 Nos. CCTV Cameras have been installed by throughout Delhi Constituency.
2.	Bharat Electronics Limited who is custodian of installed CCTV Cameras in Delhi
3.	Bharat Electronics Limited who is custodian of installed CCTV Cameras in Delhi
4.	As per latest guideline by the Hon'ble Minister (PWD) House Owner at which house CCTV cameras installed, RWA representative, Hon'ble Area MLA or his/her representative, Delhi Police, Area DCP and PWD can access only live view, Play back without admin right.
5.	Bharat Electronics Limited is installing CCTV Cameras have well trained executing team to installation & maintenance of CCTV Cameras.
6.	There is no such type of minimum eligibility criteria for such type of work. However, Bharat Electronic Limited have well trained and qualified engineers and technicians.
7.	There is no such type of minimum eligibility criteria for such type of work. However, Bharat Electronic Limited have well trained and qualified engineers and technicians.
8.	There is no such type of minimum eligibility criteria for such type of work. However, Bharat Electronic Limited have well trained and qualified engineers and technicians.

S. No.	Information
9.	Data can be stored for 30 days in Hard Disk.
10.	On written request of local police, Hon'ble MLA and Hon'ble Court CCTV footage can be provided.
11.	On written request of local police, Hon'ble MLA and Hon'ble Court CCTV footage can be provided.
12.	Not any activities delegates to any third party.

Simultaneously, to know more about the protocols on data collection through lawful interception and monitoring, RTI applications were filed with the Ministry of Home Affairs and the Centre for Development of Telematics (C-DOT).

The RTI Application sought the following information:

1. How many cases (in numbers) have been identified for lawful interception and monitoring in the last 5 years?
2. How many cases have been identified (state-wise) for lawful interception and monitoring in the last 5 years?
3. What are the parameters for identifying a subject for lawful interception and monitoring?
4. Are the subjects of lawful interception and monitoring provided an intimation?
5. Is any other information provided to the subjects of lawful interception and monitoring?
6. What are the standard operating procedures for conducting lawful interception and monitoring?
7. Which authority is responsible for approving the lawful interception and monitoring of the individuals?
8. Which authority is responsible for approving the lawful interception and monitoring of the devices?
9. What are the guidelines concerning the storage and management of data collected through lawful interception and monitoring?
10. What are the guidelines concerning the disposal of data collected through lawful interception and monitoring?
11. Is there an authority that addresses the grievances of the subjects of lawful interception and monitoring?
12. If yes, which authority is responsible for grievance redressal in issues arising out of lawful interception and monitoring?

The RTI application sent directly to the Ministry of Home Affairs was forwarded to the Monitoring Unit (CIS-IV Desk) of the Cyber and Information Security (CIS) Division.

Centre for Development of Telematics (C-DOT) forwarded the application to the Department of Telecommunications, Ministry of Communications. The Department of Telecommunications (Security Wing) responded:

As regards information pertaining to this CPIO is concerned, it is stated that lawful interception is done under the provisions of section 5(2) of Indian Telegraph Act 1885 read with rule 419(A) of the Indian Telegraph Rules. Lawful interception, being a matter of national security, the specific information sought falls under restricted category and is exempted as per clauses 8(1)(a), 8(1)(g) and 8(1)(h) of the RTI Act.

This application was further transferred to the Ministry of Home Affairs.

As both the applications ended up with the Monitoring Unit (CIS-IV Desk) of theCyber and Information Security (CIS) Division that deals with policy on lawful interception, audit of monitoring facilities, co-ordination for Centralized Monitoring System, secured communication systems like RAX, SDCN etc, blocking of websites in coordination with MeitY, matters related with Indian Telegraph Act, TRAI, Information Technology Act etc and related grievances, RTI and parliament questions, we received the following response:

Lawful interception and monitoring is done by the authorised Law Enforcement Agencies with due permission of the competent authority if required in the interest of sovereignty and integrity of the country, security of the state, public order or incitement of an offence, under the legal provisions of section 5(2) of the Indian Telegraph Act, 1885 and section 69 of the Information Technology Act, 2000 as per procedure defined in Rule 419A of the Indian Telegraph Rules and Information Technology Rules. MHA does not maintain any statistical data regarding lawful interception.

Another RTI application was filed before the National Crime Records Bureau (NCRB) in December 2021 to procure information about the course on "CCTV Footage Analysis" for training of the police personnel.

The RTI Application sought the following information:

1. A copy of the syllabus/course structure of the special course on "CCTV Footage Analysis" for the training of officers
2. When was the course introduced?
3. What is the minimum eligibility criteria for the officers to partake the course?
4. How many officers have successfully completed the course?

Although this was mentioned as a special course on their website, ***NCRB responded that no such course is conducted by the Bureau and disposed of the application.***

RTI applications were filed with all the States and and Union Territories to check the status of the implementation of the Supreme Court in Paramvir Singh Saini vs. Baljit Singh & Others, SLP (Cr) No. 3543 of 2020 dated December 2, 2020. The application sought the states to provide the status of mandatory installation of functioning CCTV Cameras in all the police stations, district-wise.

The RTI Application sought the following information:

1. How many police stations in the state have installed functioning CCTV cameras as ordered by the Supreme Court in Paramvir Singh Saini vs. Baljit Singh & Others, SLP (Cr) No. 3543 of 2020 dated December 2, 2020?
2. How many police stations (district-wise) in the state have installed functioning CCTV cameras as ordered by the Supreme Court in Paramvir Singh Saini vs. Baljit Singh & Others, SLP (Cr) No. 3543 of 2020 dated December 2, 2020?

The response of the states was irregular but it has been collected and arranged in the following table.

	Total Police Stations installed with functioning CCTV cameras (RTI)
	Figures
Delhi	190
Andhra Pradesh	Data Not Provided
Arunachal Pradesh	70
Assam	73
Bihar	952
Chhattisgarh	443
Goa	23
Gujarat	619
Haryana	No Response
Himachal Pradesh	73
Jharkhand	29
Karnataka	1052
Kerala	Data Not Provided
Madhya Pradesh	Data Not Provided
Maharashtra	764
Manipur	No Response

	Total Police Stations installed with functioning CCTV cameras (RTI)
	Figures
Meghalaya	20
Mizoram	40
Nagaland	19
Odisha	584
Punjab	Data Not Provided
Rajasthan	No Response
Sikkim	29
Tamil Nadu	No Response
Telangana	429
Tripura	72
Uttar Pradesh	No Response
Uttarakhand	160
West Bengal	53
Andaman & Nicobar	24
Chandigarh	16
Dadra & Nagar Haveli and Daman & Diu	6
Jammu & Kashmir	15
Ladakh	7
Lakshadweep	0
Puducherry	Data Not Provided

Common Cause is a registered society dedicated to championing public causes, campaign for probity in public life and integrity of institutions. It seeks to promote democracy, good governance and public policy reforms through advocacy, interventions by formal and informal policy engagements. Common Cause is especially known for the difference it has made through a large number of Public Interest Litigations filed in the Courts, such as the recent ones on the cancellation of the entire telecom spectrum; cancellation of arbitrarily allocated coal blocks; Apex Court's recognition of individuals right to die with dignity and legal validity of living will.

Centre for the Study of the Developing Societies (CSDS) is one of India's leading institutes for research in the social sciences and humanities. Since its inception in 1963, the Centre has been known for its critical outlook on received models of development and progress. It is animated by a vision of equality and democratic transformation. Lokniti is a research programme of the CSDS established in 1997. It houses a cluster of research initiatives that seek to engage with national and global debates on democratic politics by initiating empirically grounded yet theoretically oriented studies. The large volume of data collected by Lokniti on party politics and voting behaviour has gone a long way in helping social science scholars making sense of Indian elections and democracy.

Common Cause
Common Cause House,
5, Institutional Area, Nelson Mandela Road,
Vasant Kunj, New Delhi 110 070
Phone: +91-11-26131313
E-mail: commoncauseindia@gmail.com;
contact@commoncause.in
Website: www.commoncauseindia.in

Lokniti - Centre for the Study Developing Societies (CSDS)
29, Rajpur Road, Civil Lines, Delhi 110 054
Phone: +91-11-23942199
Email: csdsmain@csds.in;
lokniti@csds.in
Website: www.csds.in; www.lokniti.org