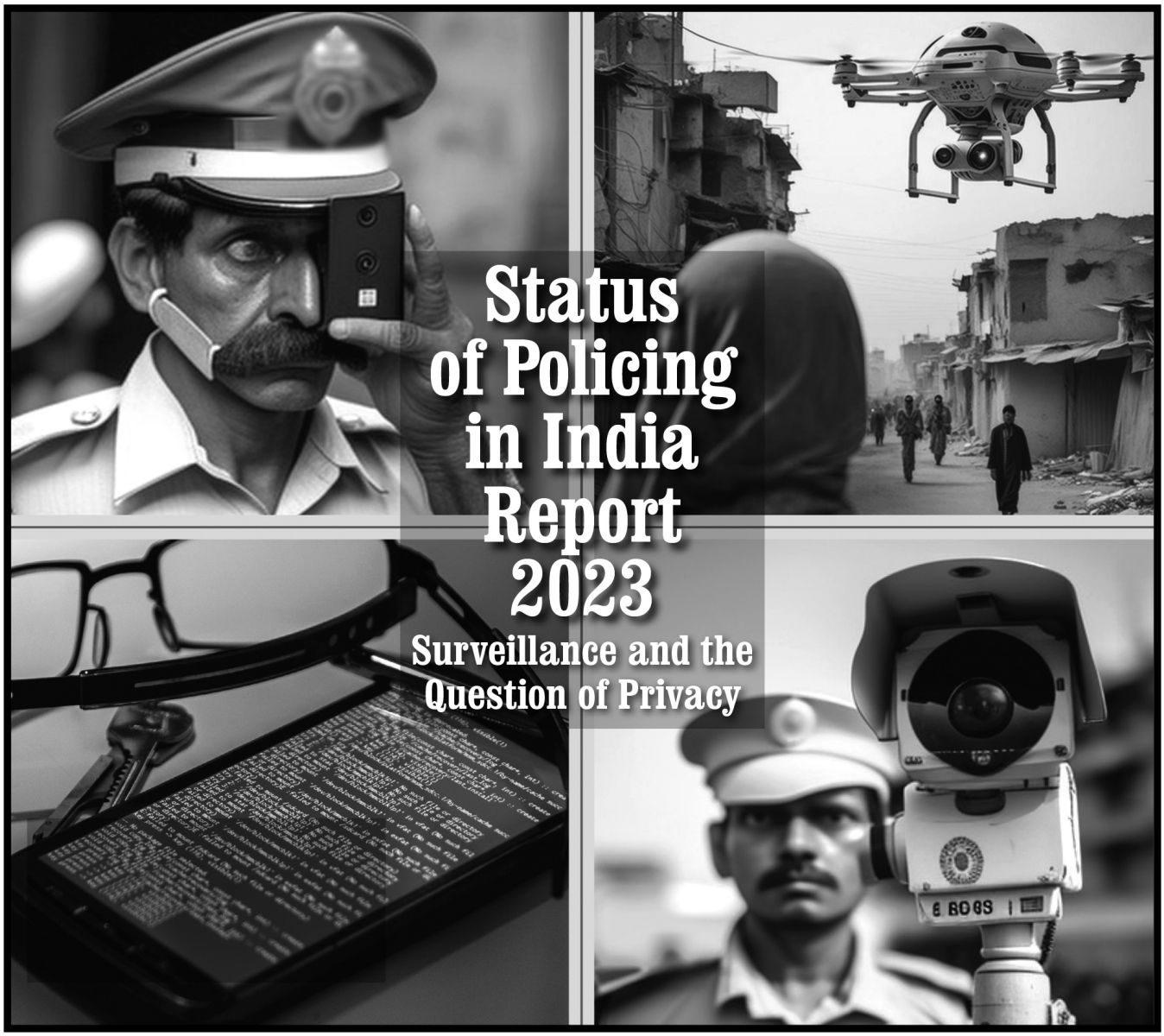
Vol. XLII No. 1 January-March, 2023

COMMON CAUSE

www.commoncause.in

POLICY-ORIENTED JOURNAL SINCE 1982



Editorial: The Surveillance Ecosystem	03	Mr Prakash Singh, Former DGP	23
SPIR 2023: Key Findings	05	Prof Ruchi Sinha, TISS, Mumbai	26
SPIR Launch Event 2023	16	Apar Gupta, Internet Freedom Foundation	28
Keynote Address: Justice Jasti Chelameswar	20	Common Cause Updates	32

Price: Free distribution to members Regn No. 39331/1982

DONATE FOR A BETTER INDIA!
DONATE FOR COMMON CAUSE!

Common Cause is a non-profit organisation which makes democratic interventions for a better India. Established in 1980 by the legendary Mr. H D Shourie, Common Cause works on judicial, police, electoral and administrative reforms, environment, human development and good governance.

Its very first Public Interest Litigation benefitted millions of pensioners. Subsequent PILs transformed the way natural resources are allocated in India. Its landmark cases include those challenging the criminalisation of politics; cancellation (and re-auction) of arbitrarily allocated 2G telecom licences and captive coal blocks; quashing of Section 66A of the IT Act; prohibiting misuse of public money through self-congratulatory advertisements by politicians in power, to name just a few. Our other prominent petitions pertain to imposing penalties on rampant illegal mining in Odisha, the appointment of Lokpal and seeking human beings' right to die with dignity through a 'Living Will.'

The impact: Telecom and coal block re-auctions leading to earning of several thousand crores rupees to the public exchequer. Even though this is a small amount in the larger scheme of things, the re-establishment of norms and institutional integrity made the process priceless. From spectrum to coal to mines, today no government can 'gift' precious resources to cronies thanks to our two PILs. (For more details about cases, please visit www.commoncause.in)

Common Cause runs mainly on donations and contributions from members and well-wishers. Your donations enable us to research and pursue more ideas for a better India. Common Cause believes that no donation is too small. Donations are exempt under Section 80-G of the Income Tax Act. Please send your cheques with your personal info at the address given below. You may also deposit directly into our bank account (details are given below) and send us an email at commoncauseindia@gmail.com, providing information such as donor's name, address and PAN number for issuance of donation receipt.

Name: Common Cause,
Bank: IndusInd Bank,
Branch: Vasant Kunj, New Delhi
S.B. Account No.: 100054373678,
IFSC Code: INDB0000161

Address: Common Cause,
Common Cause House, 5, Institutional Area,
Nelson Mandela Marg, Vasant Kunj,
New Delhi - 11 00 70
(Phone numbers: 011 26131313 and 45152796)

COMMON CAUSE VISION

An India where every citizen is respected and fairly treated

MISSION

To champion vital public causes

OBJECTIVES

To defend and fight for the rights and entitlements of all groups of citizens

Designed at GENESIS genesisadvt@hotmail.com 9810033682

THE SURVEILLANCE ECOSYSTEM

Versus the Constitutional Right to Privacy

Dear members and friends of Common Cause,

The SPIR 2023 is now out. It is India's first report of its kind on matters of surveillance and privacy. This issue of your journal presents a reader-friendly summary of the report, its conclusions, and key findings. It also sums up the salient points of the panel discussion and the keynote address at the well-attended event which marked the launch of the report on March 31, 2023.

The SPIR series is an attempt to measure the impact of policing on the ground. It is part of the organisation's campaign for police reforms. The first SPIR (2018) surveyed respondents in 22 states on citizens' trust and satisfaction levels, police excesses, diversity, etc. SPIR 2019 focused on the working conditions of police personnel, their attitudes, crime investigation, and police violence. The two volumes of the SPIR 2020-21 covered policing in areas facing extremism or insurgency and policing in the times of the Covid-19 pandemic.

The current issue is focused on matters of surveillance and privacy. We all know from experience that a variety of state and private players consistently profile us and track all our activities. Some even manipulate our emotions and beliefs in order to polarize minds. Several government agencies, at the central and state levels, also use a variety of surveillance methods such as drones, CCTV cameras, phone tapping, and Facial Recognition Technology (FRT). All this raises a plethora of legal and philosophical questions which we have tried to tackle in this study.

We understand that surveillance is not a new concept. Modern state throughout the world has been spending an enormous amount of time and resources on perfecting methods of surveillance without being detected. Their reasons could be anything from national security concerns to winning elections to witch-hunts of opponents.

The present volume uses four parallel methods of investigation, i.e., official data on the installation and use of surveillance apparatus; a focused group discussion with domain experts; an analysis of media coverage, and an extensive survey of common people. It also assesses the capacity and preparedness of the human beings behind the systems who end up conducting surveillance.

Surveillance and Democracy

We at Common Cause believe that matters of surveillance and privacy profoundly impact the state of democracy, human rights, and the process of free and fair elections. As far back as in 2010, a private company, Cambridge Analytica, 'harvested' the data of over 70 million Facebook users for manipulating opinions in the US elections. Since then, technology has improved drastically. The Pegasus spyware, developed by the Israeli company NSO – which claimed to have sold it to 'vetted' governments – used a computer virus to copy data from the smartphones of its victims, mostly dissenters, opposition leaders, and journalists across the world.

Even though surveillance is often done by individuals and private companies, a bigger cause for concern globally is targeted surveillance by state agencies. There is also a legislative void around the breach of data through surveillance. Many of these clandestine activities of the state 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 becoming all invasive, 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 state of affairs raises 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?

As of now, the only tangible instrument in the hands of the citizens is their constitutional Right to Information (RTI). It allows people to scrutinise the state's actions and to hold public servants accountable. However, many proposed changes seek to dilute that power as we write this. For instance, the draft Data Protection Bill turns the logic on its head by expanding the scope of information which can be denied on the grounds of privacy.

The application of RTI to methods and extent of surveillance is vital because the ecology of surveillance affects not just privacy but also civil liberties, internet freedom, and the existence of independent media. According to the Freedom House Report 2022, internet freedom and the freedom of expression are consistently on a decline. Another important concern is that the production, dissemination, and impact of politically vital information is in the hands of the global internet platforms that pay little respect to domestic laws and institutions.

A Democratic Fight is on

It is heartening that the onslaught on citizen's privacy is being pushed back by many individuals and institutions across the world. Some global alliances are raising their voice against illegal, unchecked, and unaccountable surveillance by the government authorities. These include coalitions of investigative journalists, citizen labs, whistle-blowers, and civil rights activists. 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.

The common people often support, or are indifferent to, surveillance because they assume it is being done in the interest of national security or 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, eventually, citizens will be 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 need to understand all its implications if we are serious about defending democratic freedoms. We hope that SPIR 2023 will be a step in the direction of improving awareness about privacy as a fundamental right and creating democratic resilience against unwanted invasions.

As always, your feedback is welcome on this issue of your journal.

Vipul Mudgal
Editor

STATUS OF POLICING IN INDIA REPORT 2023: SURVEILLANCE AND THE QUESTION OF PRIVACY

Summary and Key Findings

The Status of Policing Report is the flagship report of Common Cause and the latest edition is the first of its kind study in India to explore public perception of privacy and surveillance. SPIR 2023 has been framed against recent developments like the Right to Privacy judgement by the Supreme Court and concerns about data protection. The report thus examines the evolution of Indian policing within the ambit of the exponential growth and deployment of surveillance technologies and their implications for the privacy of citizens.

SPIR 2023 has looked into the complexities surrounding digital surveillance, the extent of surveillance by government agencies and private entities, allegations about the illegal deployment of Pegasus by the government and the enactment of the Criminal Procedure (Identification) Act, 2022, which grants the police power to collect the biometrics of suspects. The aim is to gauge public opinion about these issues.

The study by Common Cause and CSDS-Lokniti employed the following research tools:

- Face-to-face interviews with 9,779 people across 12 Indian states and Union Territories.
- Focus group discussions (FGDs) with domain experts and in-depth interviews with serving police officers.
- Filing Right to Information applications for latest government data and analysis of official data on surveillance, CCTVs in police stations, cybercrime rates, and monitoring cells.
- Analysis of media coverage of surveillance over a period of one year across six major media outlets to identify broad trends in coverage.

The findings indicate a high level of public support for certain forms of government surveillance but also reveal a lack of public awareness regarding Pegasus and the Puttaswamy judgement. Public perceptions around privacy and government surveillance demonstrate a high level of support for the use of such technology by the police and the government. However, support for any form of surveillance is directly proportional to the respondent's socio-economic status, consistent with past findings (SPIR 2018) that marginalised sections - Adivasis, Dalits, and Muslims - are least trustful of the police.

Overall, SPIR 2023 highlights the need for increased awareness and understanding of critical issues and addresses the disparities in trust and support for government and non-governmental surveillance.

Some of the broad findings of SPIR 2023 are:

Official Data Trends

Despite the limited availability of official data on compliance with the *Paramvir Singh* judgement which mandates the installation of CCTV cameras in police stations, we have analysed the existing data to identify overarching trends in surveillance across India.

- The number of CCTV camera feeds available with the police, including private ones, is significantly lower than the actual overall number of cameras within city limits.
- There is no statistically significant relationship between the number of CCTV cameras and crime rates from 2016 to 2020. In other words, the number of cameras available with the police does

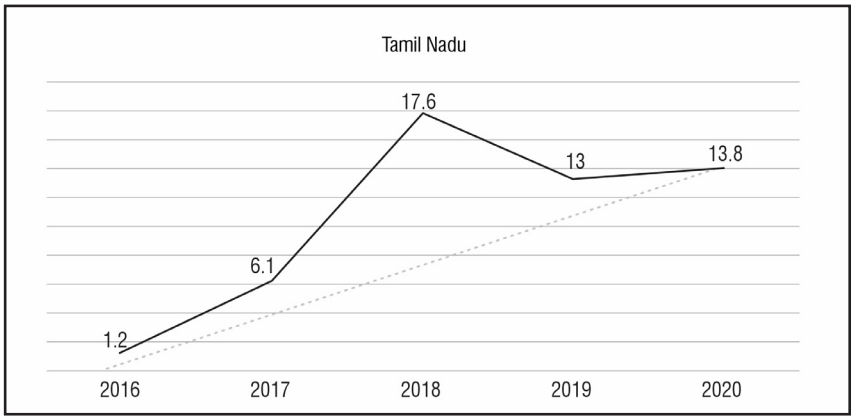
not have any statistical impact on the rate of cognisable crime, murder, and auto/ motor theft.

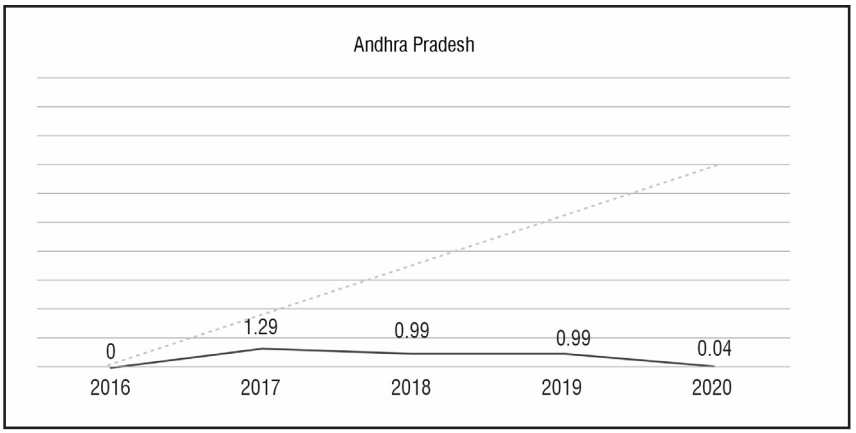
- Even amongst states that register a high number of cybercrimes, the infrastructure to solve such cases do not match the high volumes of registration of cybercrimes.
- The conviction rates for cybercrimes across the country are lower than the corresponding rates for total cognisable crimes under the Indian Penal Code (IPC) and Special and Local Laws (SLL). In Assam, for instance, despite 6096 persons being arrested in 2021 for cybercrimes, the charge sheeting rate was about 16 percent and the conviction rate was just 2.2 percent.
- States have started registering an increasing number of cybercrimes under the subhead 'political motives'. While the term itself is not defined by the National Crime Records Bureau (NCRB), its number has increased nearly nine-fold over a five-year period, from 40 in 2016 to 356 in 2020. Notable states are Tamil Nadu, Uttar Pradesh and Andhra Pradesh.

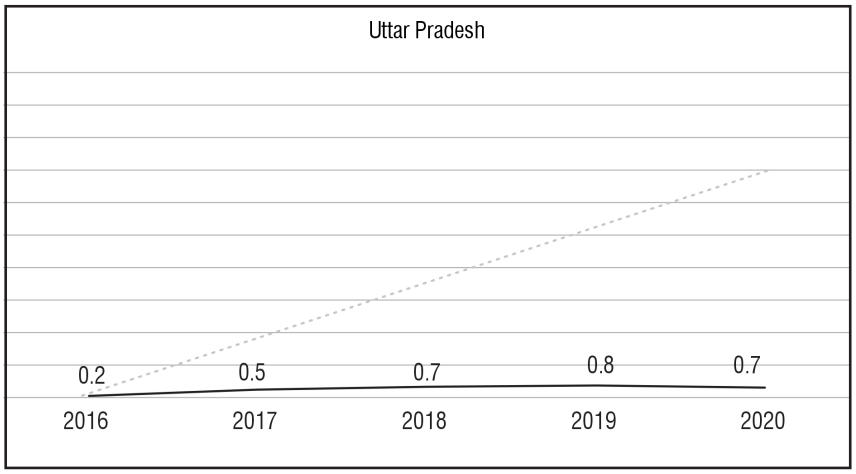
Experts' Opinions on Surveillance and Right to Privacy in India

The topic of surveillance rarely breaks out of the domain of expert conversation into broader public discourse. This has

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







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

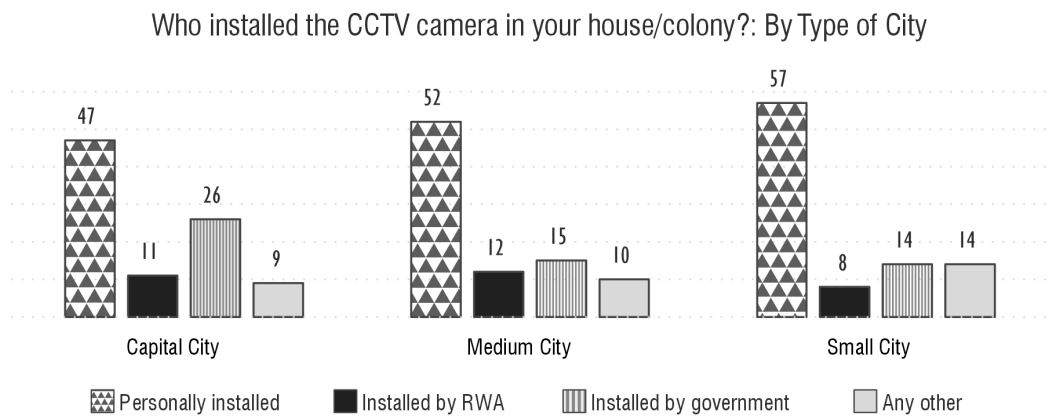
resulted in a lack of awareness about the potential threats of surveillance technologies. We aim to bridge this gap in SPIR 2023 via focus group discussions. The FGDs provide context to the survey findings on the general public's opinions. The following are some of the significant findings from the FGD and interviews.

- The experts broadly agreed that while surveillance is being conducted by various actors—state agencies, private entities, individuals—it was the unchecked targeted surveillance by the state that was the biggest cause for concern. Some of the participants felt that surveillance by private companies was being used for stifling dissent or manipulating electoral processes.
- While the participants differed on the efficacy of mass surveillance technologies such as CCTVs for controlling crime, there was consensus that oversight and accountability were required.
- The FGD participants were of the opinion that general support for surveillance technologies stemmed from ignorance of the right to privacy. It was felt that surveillance is viewed as an effective tool for public safety and national security by the masses. Some of the participants also pointed out the class differences in attitudes, with the poor being less likely to support surveillance by the police or the state.
- Participants, as well as serving police officers, pointed out that police forces in India lack the necessary infrastructure, capacity, and legal mechanisms to conduct proper surveillance. The ground reality is that the police are unable to use surveillance technologies effectively.
- Some participants pointed out that social prejudice can be keyed into the technology as well, leading to biased algorithms which could subvert the criminal justice system.

Prevalence of and Perceptions of CCTV Cameras

CCTV cameras are among the most pervasive forms of digital

The government is three times more likely to install CCTV cameras in slums/poor localities, compared to higher-income localities.



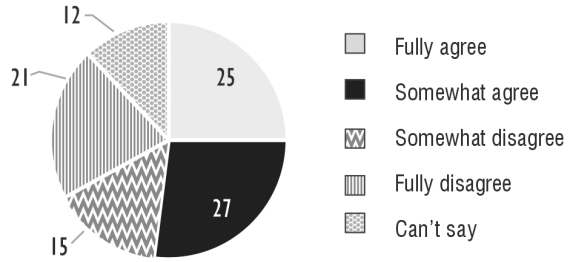
Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/ residential areas. The rest of the respondents did not answer. Question asked: Were they installed by you or some other authority?

mass surveillance, and yet regarded as seemingly harmless. Proponents argue that they help prevent crime and ensure public safety, but there is little empirical data to support these claims. Despite this, the general public's perception as indicated by the survey is largely in favour of the continued use of CCTVs, even if it means accepting the risks of mass surveillance. However, support for CCTV cameras declines significantly among respondents with lower levels of education and socio-economic status.

- Half of the respondents (51%) 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, as opposed to higher-income localities.
- The poorest sections are the least likely to support the installation of CCTVs at any location— whether at the 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 strongly believe that CCTVs help monitor and reduce crime.
- People with higher levels of education are more likely to believe that CCTVs help in crime reduction, 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

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

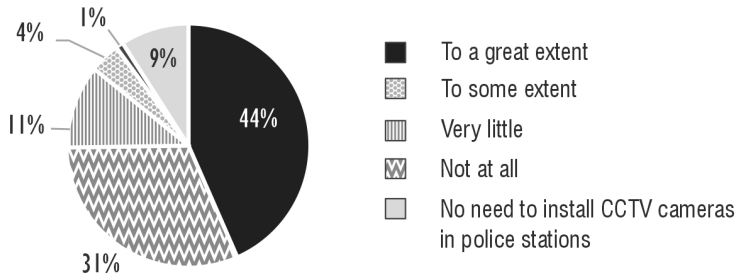
"There is a risk of illegal mass surveillance in public places due to CCTVs cameras"



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 CCTV cameras.

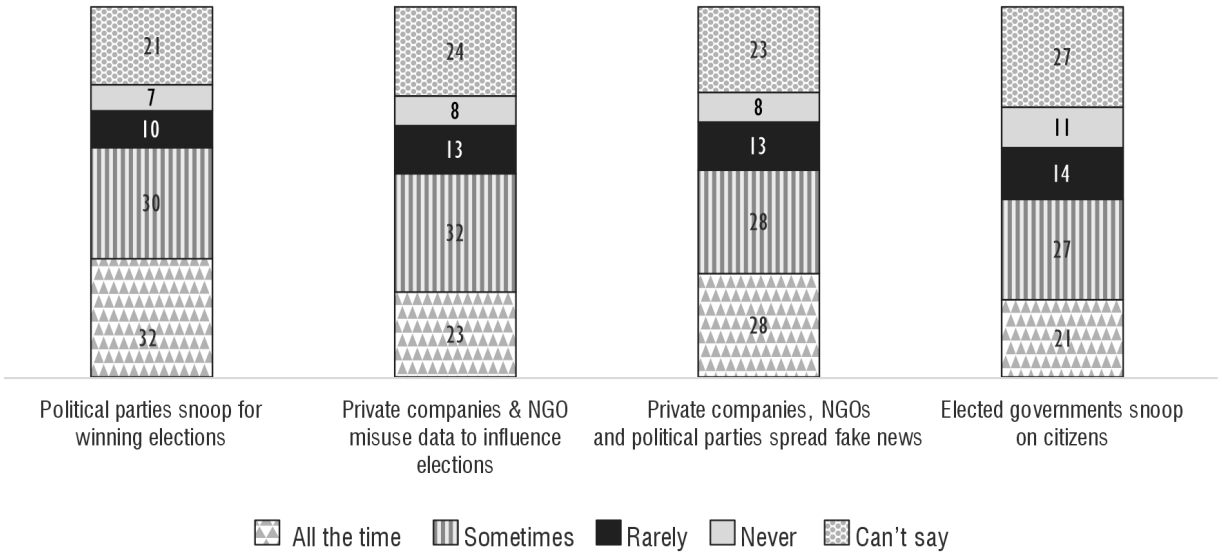
Forty-four percent people believe that CCTV cameras in police stations are very helpful in preventing human rights violations against those in custody

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?

Nearly two out of three respondents believe that political parties surveil citizens for electoral gains



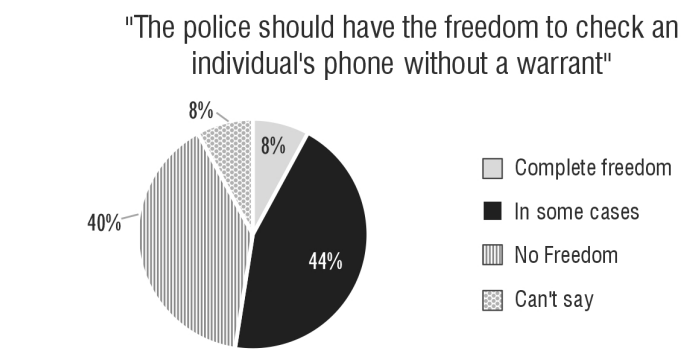
Note: All figures are in percentage.
Question asked: To what extent do you think these things happen in our country - all the time, sometimes, rarely or never
a. Political parties use surveillance and snooping techniques for winning elections
b. Private companies or NGOs collect common people's data 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

- 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.

Government and Police Surveillance

- The findings of SPIR 2023 are consistent with previous findings (SPIR 2018) that people are generally satisfied with the performance of

Forty percent people believe that police should not have any freedom to check people's phones without a warrant



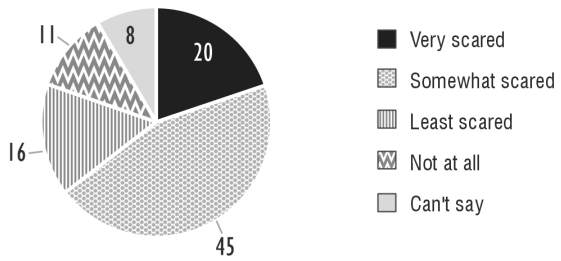
Note: All figures are in percentages.
Question asked: How much freedom should the police have to check your phone at any time without a warrant - complete, in some cases, or no freedom at all?

the police. In line with this trend, the survey data shows that people largely support the use of drones and facial recognition technology (FRT) by the government.

- About half of the respondents supported the collection of biometric details of suspects, including undertrials. Adivasis and Muslims are the most critical of the police collecting biometric details of suspects.
- More than one in two strongly support the use of drones by the armed forces, government, and the police. However, farmers and the poorest are most likely to oppose drone usage by government agencies.
- Half of the respondents fully support the use of FRT by the government and police. They are four times more likely to strongly support the use of FRT by government agencies, compared to its use by private entities.
- Nearly two out of three respondents believe that political parties surveil citizens for electoral gains
- Forty percent of people believe that police should not have the 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
- 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
- Only 16 percent of people believe that the police are adequately trained to use surveillance technologies such as CCTVs, drones and FRT

Nearly two out of three respondents are scared to post their political or social opinions online for fear of legal action

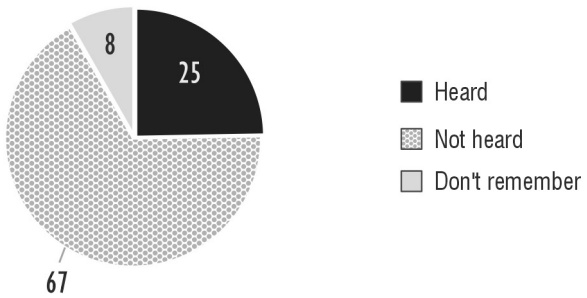
Fear of legal action for posting political or social opinion online



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?

Two out of three people have not heard of the Pegasus spyware issue

Awareness about Pegasus software



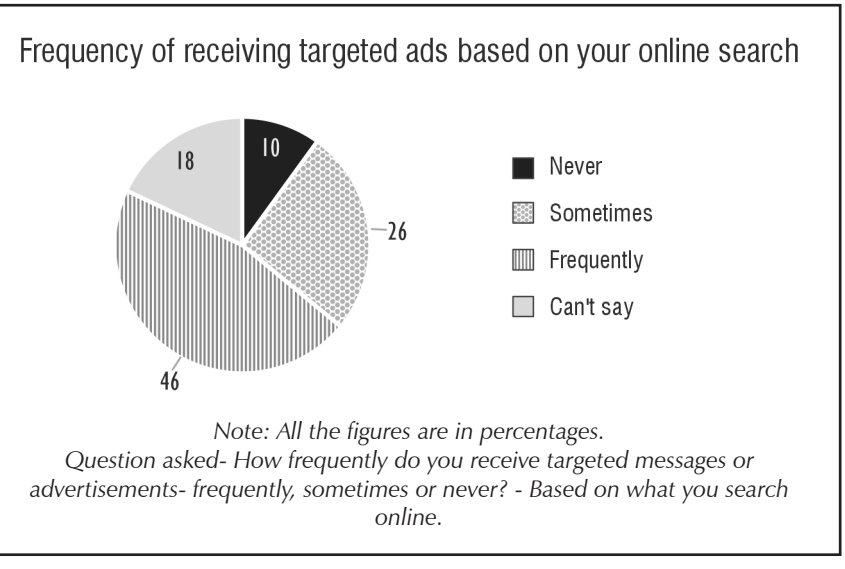
Note: All figures are in percentages.
Question asked: Have you heard of the Pegasus software which was used by governments of various countries, including India, to listen to the calls and read the messages of some people, including politicians, journalists and judges?

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 protests against government or laws	61	24	15
To identify those participating in communal riots or disturbing law and order	75	11	14
To identify common citizens, regardless of the crime	35	4417	

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 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)

Nearly one out of two persons reported frequently receiving targeted ads based on internet search history



Note: All the 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.

Right to Privacy and Freedom of Speech

The views expressed in FGDs stand in stark contrast to the opinions expressed by the common public. The survey data suggests that a large proportion of people support the use of government surveillance to curb protest and freedom of expression. Additionally, while people expressed fear about sharing their opinions online, they paradoxically supported government surveillance of online and offline activity, including the use of illegal spyware such as Pegasus. Moreover, public awareness about Pegasus and the *Puttaswamy* judgement is extremely low.

- Over half of the people strongly justify using CCTV cameras to control protests. People from small cities and poor backgrounds are least likely to support the use of CCTVs to curb political movements or protests.
- One in five believes that it is right for the government to monitor people's social media posts.
- Large sections of the respondents feel government surveillance by CCTVs (52%), drones (30%) and FRT (25%) to suppress protests and political movements is justified to a great extent. Respondents from Punjab are least likely to support government surveillance of protests while those from Gujarat are 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. More than a quarter of the respondents feel that surveillance of MPs/MLAs and other politicians using spywares such as Pegasus is completely justified.

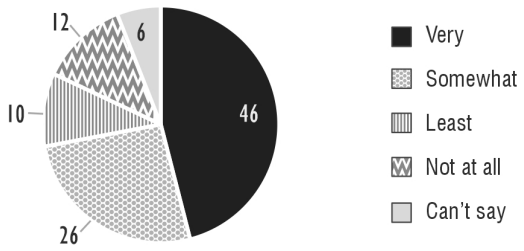
- Nearly one out of three respondents strongly support drone usage by the government to curb political protests
- More than 60 percent of the public support the use of FRT to identify protestors, while two out of five say drones should be used to identify common citizens.
- Only about one in six respondents (16%) have heard about the right to privacy (*Puttaswamy*) judgement passed by the Supreme Court. People from upper-class sections with college degrees and above are most likely to have heard about the judgement.
- About one out of two persons fully agrees with the decision in the Supreme Court judgement on the right to privacy.

Surveillance by Private Entities

The public is generally in support of the government's use of surveillance technologies, but there is a notable level of concern among people about the safety and misuse of their personal data by private entities. This is particularly evident when it comes to government-issued

Nearly three out of four people worried that their personal data such as Aadhar number or PAN can be leaked online

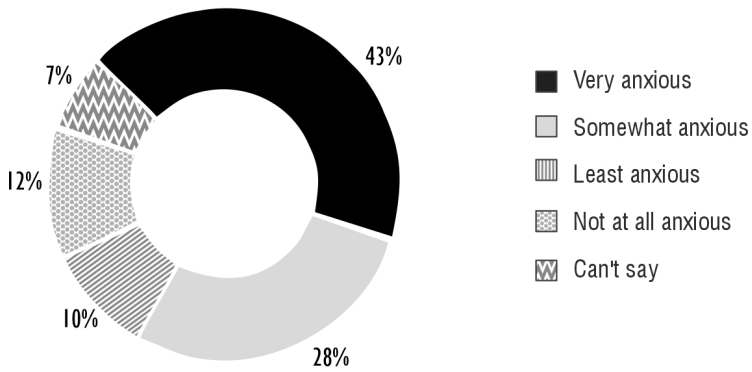
Level of anxiety about leakage of personal data such as Aadhaar or PAN



Note: All the 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? - Your personal data such as Aadhar number, PAN number, etc. can be leaked online.

Four out of ten people very anxious that their digital identity can be stolen by a person or company

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? - An unknown person or company can steal your digital identity.

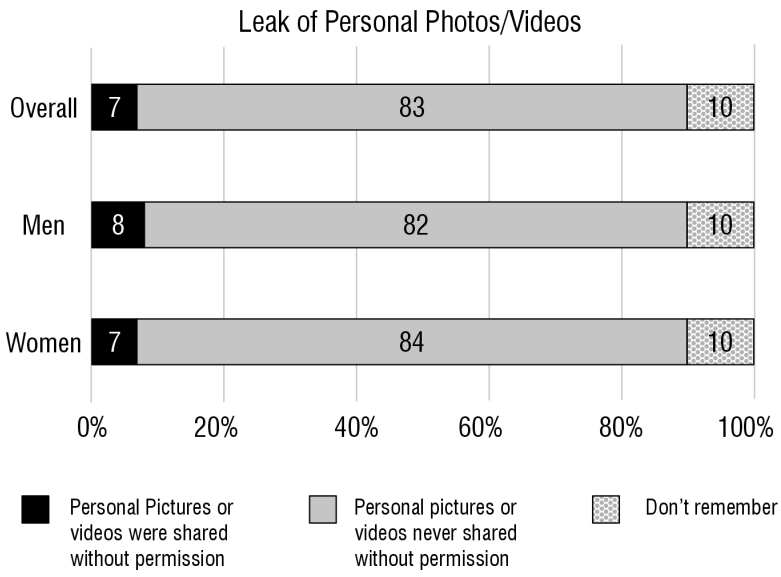
identity documents like Aadhaar or PAN cards. People are especially apprehensive about sharing these details with private companies. The survey also indicated that people have been subjected to online tracking by private companies and received targeted ads based on their profiles and past activities.

- About two out of three respondents are concerned that data collected by private entities can be misused.
- Nearly one in two frequently receives targeted ads based on their online search history.
- One out of five people are not at all comfortable sharing their Aadhaar details with private agencies.
- Forty percent of people are very anxious that information provided by them online can be misused.
- Forty-four percent of the people are 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.

Hacking and Cybercrimes

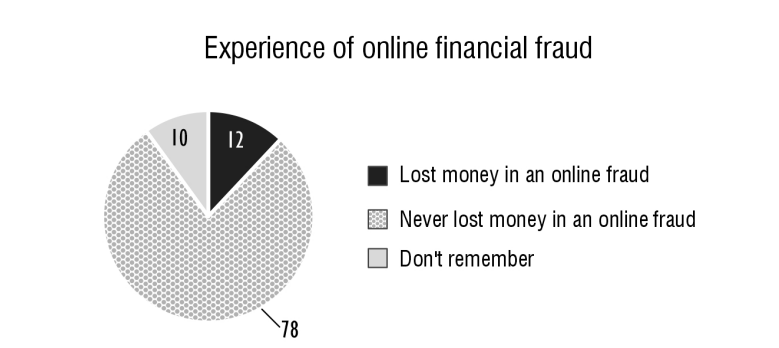
The safety of personal data - of a financial nature especially - is a major concern for the general public. This is further supported by the rise in reported cybercrimes as per

Seven percent people report having their personal photos or videos shared online without their permission



Note: All figures are in percentage.
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?

Twelve percent respondents have been victims of online financial frauds



Note: All the 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.

NCRB data since the onset of the Covid-19 pandemic, and the survey findings reflect this anxiety. Additionally, the survey sheds light on the use of digital financial platforms based on caste, class, and age.

- Two out of five people are anxious about hackers accessing the information on their phones without their consent or knowledge.
- Three out of four people are anxious about an unknown person/company accessing their email accounts.
- Seven percent people report having their personal photos or videos shared online without their permission
- Nearly one out of three people do not use any form of digital banking such as United Payments Interface (UPI), digital wallets, debit/credit cards or net banking. Older respondents are least likely to use payment wallets or feel comfortable with such apps.
- Scheduled Caste respondents were least likely to use digital banking while upper caste respondents were most likely to.
- Twelve percent of the respondents reported that they have been victims of online financial fraud.

Analysis of Media Content on Surveillance

In order to gain insights into the media coverage of surveillance the research team conducted an analysis of relevant news stories over a period of a year from July 1, 2021, to June 30, 2022. A total of 1,113 news stories from six media outlets (three Hindi and three English) were coded and analysed to identify broader trends such as the type of stories, their slant and sources used.

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

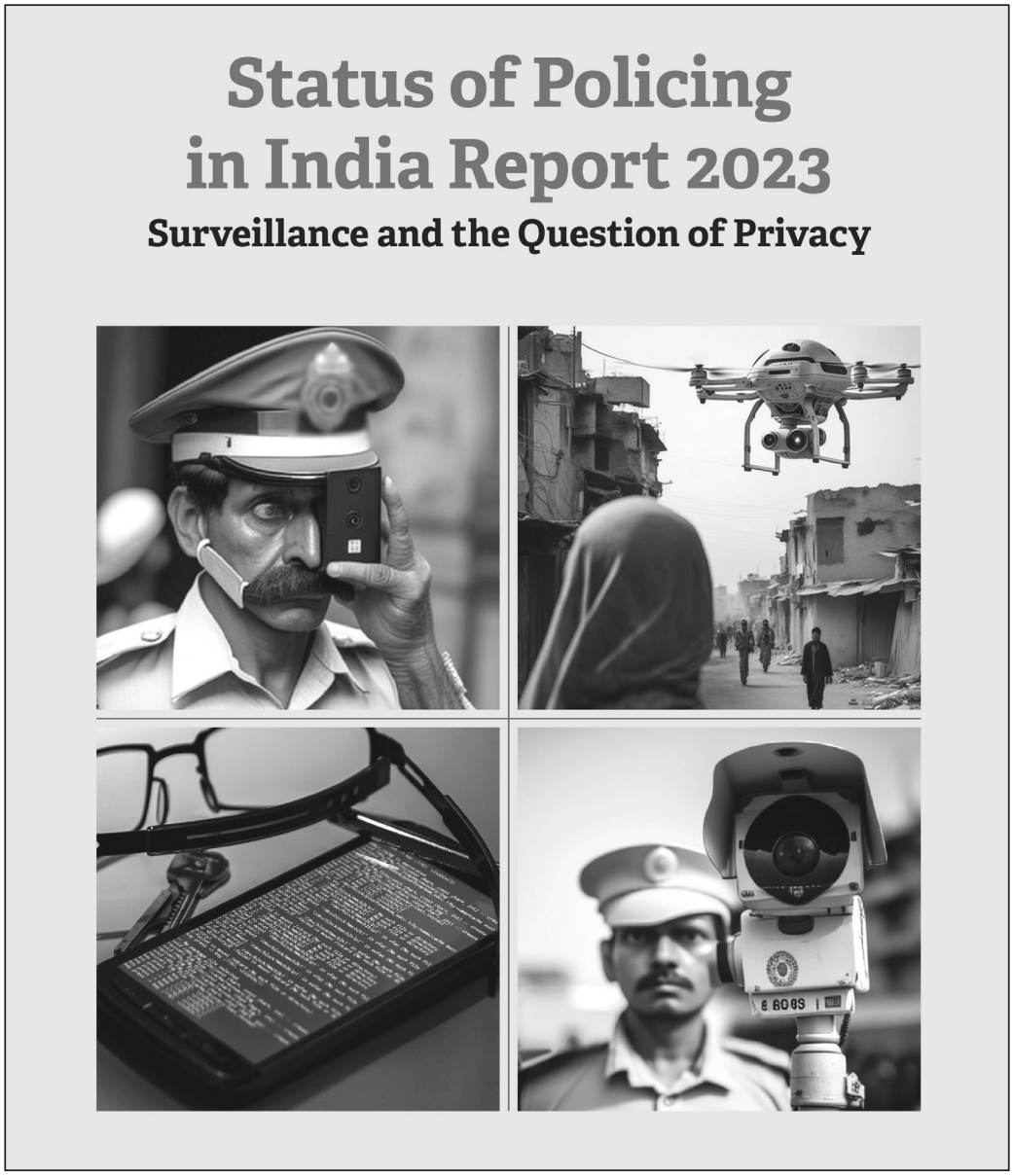
Note: All figures are in percentages and are rounded off.

Frame	No of stories	Percent
Human Rights	297	27
National Security	92	8
Public Safety	696	63
Technology	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.

- Nearly three out of four news items rely on government agencies as their primary source.
- One in four stories has a pro-surveillance approach.
- Times of India and Dainik Jagran were most likely to have a pro-government slant on surveillance, while The Wire was most critical of the government. Over half of Times of India stories are pro-surveillance.
- Nearly two of three news items are on the use of surveillance technology for public safety and order. Only a quarter of the news stories focus on human rights.
- Stories on CCTVs and drones are least likely to include debates around their legality or right to privacy.
- Of the total sampled stories, less than 14 percent mention right to privacy or the legality of the surveillance.

Please email us at commoncauseindia@gmail.com if you want a soft copy of the report.



Jointly prepared by Common Cause and its academic partner, Centre for the Study of Developing Societies (CSDS), the Status of Policing in India Report 2023: Surveillance and the Question of Privacy, is a study of public perceptions and experiences regarding digital surveillance in India .

SPIR 2023 analyses data collected from face-to-face surveys conducted with about 10,000 individuals from Tier I, II and III cities of 12 Indian states and UTs to understand perceptions around digital surveillance. The study also involved a Focused Group Discussion (FGD) with domain experts, in-depth interviews with serving police officials, and an analysis of media coverage of surveillance-related issues.

Please email us at commoncauseindia@gmail.com if you want a soft copy of the report. It can also be downloaded from commoncause.in

SPIR LAUNCH EVENT 2023

Followed by a Lively Panel Discussion and Keynote Address

Common Cause released the Status of Policing in India Report 2023: Surveillance and the Question of Privacy (SPIR 2023) on 31 March, 2023. The report is a first of its kind, in-depth study of surveillance in India.

The report was released at a well-attended function at the India Habitat Centre in New Delhi. SPIR 2023 is the fifth consecutive annual report on policing by Common Cause, in collaboration with the Lokniti Programme at the Centre for the Study of Developing Societies (CSDS).

Radhika Jha, the lead researcher of SPIR, kicked off the launch with a brief introduction of the survey that undergirds the project. Next up Dr. Sanjay Kumar, Co-Director of Lokniti, which conducts the survey, provided an overview of SPIR Reports since their inception. He said that every report, going back to 2018, had broken new ground in our understanding of Indian policing. The first four reports were based primarily on surveys, but SPIR 2023 has supplemented that with interviews with police officials, focus group discussions with experts and official policing data.

Dr. Vipul Mudgal, the Director of Common Cause, made a power point presentation about SPIR 2023. Dr. Mudgal said that while the SPIR documents aimed to capture public opinions about policing, SPIR 2023 tried to fathom what people felt about surveillance and privacy and the deployment of surveillance technologies by police and the government. He also expounded on the key findings of SPIR 2023.

Justice Jasti Chelameswar, former Judge, Supreme Court of India and former Chief Justice, Kerala and Gauhati High Courts, gave the Keynote Address. Justice Chelameswar was part of the nine-judge bench that recognised the right to privacy as a fundamental right and a separate bench that affirmed in 2015 that citizens cannot be denied government services for lacking an Aadhaar number. Justice Chelameswar made a strong pitch for enacting a law to regulate data collection. Without such a law, it would be difficult to determine if citizen's data was being scooped up for welfare or to serve the whims of the political masters, he said.

The release of the report was followed by a panel discussion on rethinking surveillance. The discussion was moderated by transparency and accountability activist Ms Anjali Bhardwaj. The speakers were Mr Prakash Singh, former DGP of Uttar Pradesh, Assam and the Border Security Force and Chairman, Indian Police Foundation, Prof. Ruchi Sinha, Associate Professor of Criminology at the Tata Institute of Social Sciences, Mumbai, and Mr Apar Gupta, Executive Director, Internet Freedom Foundation.

The programme ended with the speakers answering a round of questions from the audience that included lawyers, academics, activists, retired and serving police officers and students. The event was live-streamed on YouTube and can be accessed at: https://bit.ly/40vOcrI

Image Courtesy: Ghazala Ahmad

The unveiling of the Status of Policing in India Report 2023

Mr Sanjay Kumar, Co-Director, Lokniti, CSDS gave a snapshot of the SPIR series

Ms Anjali Bhardwaj moderated the Panel Discussion on Rethinking Surveillance: How Much is Too Much

Dr Vipul Mudgal, Director and Chief Executive, Common Cause gave a presentation on the findings of SPIR 2023

Ms Radhika Jha steered the event

Mr Kamal Kant Jaswal, President, Common Cause, among the audience

A scene from the Panel Discussion

KEYNOTE ADDRESS BY JUSTICE JASTI CHELAMESWAR

Edited Excerpts from SPIR 2023 Launch by Former Supreme Court Judge and Former Chief Justice, Kerala High Court and Gauhati High Court

I don't know how many of you remember when the Aadhar scheme was challenged. *Puttaswamy* judgement and the question of whether there is a fundamental right to privacy under the Constitution arose in the context of a challenge to the Aadhar scheme, which was a non-statutory scheme to start with, propounded by the previous political dispensation. The matter was lingering in the court for a few years and eventually, it was heard by a bench of nine judges of which I was a part.

At an earlier stage, when the matter was heard by a Bench presided over by me, a very vehement submission was made by the then Attorney General, saying that there is no fundamental right to privacy under the Indian constitution as per an old, 1964 judgement. In support of the submission, a stray sentence from this eight-judge bench judgement was picked up, which did say that there is no fundamental right to privacy in the Indian Constitution. The Supreme Court very rarely sat in the last 75 years in benches of even numbers (barring two judges); the rest of them were odd, the highest being 13 so far in the *Kesavananda Bharati* case. Vehement submissions were made and the matter got referred to a larger bench. When the argument was going on, a lot of public opinion was generated by the previous political regime, which had originally propounded the scheme, bitterly opposing it later. Finally, when the Supreme Court declared in a unanimous judgement by nine judges that there is a fundamental right to privacy under the Constitution, both the political parties and their respective spokespersons claimed vindication as they supported the citizens' right to privacy. Everybody wants to take advantage of the public opinion and ride the crest of popularity.

On Surveillance

As Mr Prakash Singh pointed out, surveillance and data collection have existed from the time of Chanakya. Citing the Ramayana, he said that the episode of Sita's exile was based on information gathered by Rama. Not only in India, but anywhere in the world where there is an organised state.

There are justifications for this too. Human beings are not angels barring a few great souls, and 99 percent of us are personifications of rascality in

different degrees. Therefore, there is a need for an organised state. The minute we have an organised state it has its own compulsions. If you can recollect, during 26/11 at Taj Hotel, Mumbai, a lot of criticism said that there was a total intelligence failure. If you are talking about intelligence failure, you're tacitly approving that data collection for intelligence is necessary for the country. This has always been an aspect of the state administration.

I'm sure some of you would have certainly read this book titled '21 Lessons for the 21st Century' by Yuval Noah Harari. He said it will be simply impossible for us to imagine how this world is going to be in 2050. He says that the rapid progress that is being made in artificial intelligence and biotechnology are the factors which are going to change this world beyond all recognition.

With this kind of state of affairs and the progress of technology, the problem of surveillance becomes more and more intense. It is possible because all of us voluntarily contribute data to the state. The minute we have a smartphone, the minute you operate a computer or iPad or a tablet, a lot of your information goes on onto the net and any individual can access it. This is inevitable.

On State and Surveillance

State also has its own reasons to collect data and it has reasons to keep surveillance on certain classes of individuals or groups, depending upon the situation. Notwithstanding the fact that the Supreme Court declared privacy to be a fundamental right, one basic principle of jurisprudence is that no right in law is absolute. Every right comes with a corresponding obligation which imposes limitations on the rights. So is the right of privacy. When the state is collecting for whatever reasons and justifications, is there an amount of transparency in that process? Is the data being collected in a manner which can be examined and assessed? Whether the data is meant really for the welfare of the people? Whether a particular activity of the state like surveillance or data collection is meant for the security of the nation? Ultimately, any act of the state is required to be meant for the welfare of people. Depending on the nature of the right, there are different tests and parameters as well as limitations like national security, decency, etc. in the Constitution.

Whether this collection of information or surveillance on certain individuals or organisations is really meant for the welfare of the country as a whole or the security of the state honestly is the question. Such an assessment is only possible if we have a proper system and a law which regulates the surveillance and collection of data by the state. Only then would we be able to make an assessment of whether all this exercise is genuinely done for the benefit of the people or to just suit the political needs of those in power.

Perhaps, in a good number of cases, the information is collected, not perhaps in the larger interests of the society but to suit the political convenience of those in power. It is nothing new. I don't know how many of the younger generation are aware of the Watergate scandal. President Nixon authorised the surveillance of his opponents. This is a practice which went on and on in human history and it will continue to go on.

Are we, the people of India, in a position to bring the necessary democratic pressure on the governments? When I talk about the government, I don't talk about any particular political party. Whichever political party is in power, the only change is in the hardware, the software remains the same and everybody follows the same practices. Of late, we hear a lot of complaints about the abuse of government agencies, particularly the CBI. The political party which is shouting hoarse about the misuse of CBI, managed this country for over 40 years before and yet they never bothered to make CBI any more stable, statutory and rational. Today they find the present dispensation is abusing it. If only we had a rational law dealing with CBI and the specific, defined areas where it could intervene.

On Citizens, Surveillance and Privacy

The question is - Can we, as a society, put democratic pressure on the lawmakers of this country, the parliament or the state legislatures to rationalise these practices and these institutions?

What is your right to privacy? Broadly speaking, talking about data collection, CCTV cameras, surveillance in public places, etc is a very very minor aspect of the right of privacy. Because the right to privacy is concerned with something that is personal. The minute we enter a public space, we are no more in a private area and our right to privacy becomes very limited.

As for the need of the state to collect information, what is the policeman doing on a railway platform? They are keeping surveillance on the events happening there and we accept their presence without any question. Be it a railway station, bus stand or a business centre, they keep a watch. Since the last 200 years or so, it has been a part of the system and we accept it. Now, technology is trying to slowly replace that physical supervision by the police constantly through CCTV cameras. It has very little to do with your right to privacy.

In law, there are three elements which describe or constitute privacy - Sanctuary, Repose and Intimate Decisions. Sanctuary means your own home, where you are absolutely free, subject of course to indulging in hazardous and nefarious activities. Intimate decision-making process is another aspect which revolves around what I eat, how I dress up, whom I marry or whom I don't want to interact with. But the minute I go out, what I am doing in public is open to the public gaze. CCTV cameras are installed by the state. If I do not and cannot have an objection with going out in front of thousands of people watching me, I don't know why there should be any objection for a CCTV camera in a public place.

On the other hand, the state may have justifications to install those too. One of the findings is that the installation of CCTV cameras did not result in reduced crime. The problem is not with the camera but with the way data was utilised by the investigating agencies. If the investigating agencies did not make proper use of the data collected through the CCTV cameras, if they were not efficient enough to utilise the data then naturally the crime rate would not come down. The other thing is personal data through tapping of telephones or installing electronic equipment in offices, etc. I will not refer to the names but I remember, a decade back, a senior cabinet minister complained that his office was bugged and had an unseemly quarrel with another senior minister.

These things are objectionable unless established that they are absolutely in the larger public interest. The establishment of such a fact that this activity is required in the larger public interest depends on the existence of verifiable data and recorded material by persons who are resorting to this kind of surveillance. The requirement is to create a legal regime around it. Unfortunately, the old Telegraph Act is being amended and only the title is changing, the content doesn't change.

I was joking with my friend here that this is the progress that we have made on the *Amrita Mahotsava* of Azadi. You have changed the names but not the content, from 1875 to 2023, in roughly 150 years or so. I think the requirement is more to exert democratic pressure on the lawmakers to create more rational legal systems that regulates such activities for the time being.

I thank the organisers for giving me the honour of releasing this report.

RETHINKING SURVEILLANCE: HOW MUCH IS TOO MUCH?

Edited Excerpts from Panel Discussion, SPIR 2023 Launch

Mr. Prakash Singh, Former DGP (UP, Assam and BSF) and Chairman, Indian Police Foundation

We are talking today on a very sensitive subject, which concerns our privacy, our fundamental rights. But let us be very clear about certain things. Surveillance has always been an essential or even an integral part of a state craft from the very beginning of history. Every king, every ruling party has employed the techniques of surveillance.

Historically, Chanakya's Arthashastra contains very detailed instructions on surveillance. It talks of surveillance not only of people who are enemies of the state, it talks even of surveillance over officials of the government. I will just read out just two-three lines about what he says about the high officials. The king shall select from among the roving spies those who are diligent, can disguise themselves credibly conforming to different regions and know various languages and professions to spy on the activities of high officials within the country. They shall serve the king with devotion and to the best of their ability. So, every segment is to be kept under surveillance according to Kautilya. He talks of spies in the guise of ascetics, spies in the guise of householders, spies from amongst merchants, spies from amongst thieves. He also talks of those who are visiting drinking houses and spending more than their means. It's a very comprehensive system of surveillance chalked out by Kautilya as far back as the Mauryan times.

As I said, surveillance is an integral part of a government. No ruling party or government or King can rule without surveillance. In India, once established, Britishers also felt the need for surveillance. In 1885, they formulated the Telegraph Act. Interestingly, it is somehow invoked even today and is used by the government. Apart from the Telegraph act, we have the Information Technology Act of 2000. These are the two main laws which govern and regulate surveillance in India.

On Challenges around Surveillance

The famous instances when surveillance went berserk. One

of the two was the Neera Radia case. The conversations which that lady had with industrialists, journalists, businessmen and politicians were leaked out. It caused huge embarrassment to a lot of people. The other one was the biggest case that Mr Mudgal referred to. The data from 300 people's accounts was stolen without their consent in India.

Surveillance does create problems. These problems have become very aggravated in the present context for the simple reason that technology is galloping. It's not advancing, it's galloping. Technology has placed intrusive and formidable tools in the hands of the governments with which anybody can be put under surveillance, without knowing about it. Today's challenge is not only your privacy. The democratic institutions can be threatened and subverted with such instruments. So, it's a very powerful instrument and therefore a very powerful threat also.

On Lack of Accountability and Oversight

In the absence of any law, the Supreme Court has been intervening from time to time to ensure that surveillance is kept within limits. The first important case on this issue was the 1996 *PUCL* case. The Supreme Court laid down certain procedural safeguards concerning surveillance. The other important case you would hear from the learned judge present here was the *Puttaswamy* case. Here, it was conceded that the right to privacy is a fundamental right guaranteed under the Constitution. So, the Supreme Court said that any order for surveillance has to be reasonable and *bonafide*.

In India, there are currently 10 agencies which have been authorised to intercept and monitor your communication. The Intelligence Bureau, the CBI, the Enforcement Directorate, the Narcotic Control Bureau, and some others are among the ten. These are the agencies which have the authority to put you under surveillance. But the sanction must come from the Secretary of the Home Department, Government of India. At present, about one lakh monitoring or surveillance orders are sanctioned every year. It works out to about 250 per day. If 250 cases are sanctioned per day for monitoring and surveillance, can there be judicious application of mind? It's not possible. The concerned officer would be just signing in a routine manner. They have no time to see who is going to be put under surveillance and whether they deserve to be placed under surveillance.

Who is going to be accountable if a wrong order is passed? There is no system of accountability. The officer concerned gets away with it. There's no liability provision. If somebody files petitions and it is found that the surveillance was not correct, at the most the surveillance order would be quashed and the monitored and intercepted communication might be destroyed. That's about all. Now, accountability is a huge problem. An officer who sanctions monitoring and interception of communication has to take the responsibility that it was required under the circumstances and that due application of mind has occurred before exercising their powers.

Since this is not happening today, there is a huge accountability gap. As a former law enforcement official, I can say that in a lot of cases, surveillance is ordered for extraneous reasons. Not because you are indulging in international activities, not because you have links with some foreign agency, but because government probably wants to fix you. So, they put you under surveillance.

This amounts to abuse of certain powers. These cases are objectionable. But this is not common only in India, rather it is common across the world. Everybody is not able to exercise a certain power given to them judiciously and within the limits prescribed by the law. As I have already said, there's no accountability and the existing procedural safeguards are inadequate. What is needed is a comprehensive legislation covering every aspect of surveillance. For instance, under what circumstances would surveillance be ordered? What

will be the mechanism? Who will be the sanctioning authority and for what duration? It's not that if you are put under surveillance it can go on year after year and people forget. It's like a billboard which somebody puts up and then forgets even after the function is over. The billboard is still there. There are serious problems in surveillance today and these need to be taken care of.

On the Implications of Surveillance in India

I just want to make pretty brief comments about some of the findings. I find it very encouraging that there's a high level of public support for surveillance. There is support for CCTV; support for drones, not 100 percent, but there is sizable support for drones, facial recognition systems and biometrics. But, I would say not many people who are giving their consent to or conveying their approval for these tools of surveillance are fully aware of the possibilities of misuse and abuse. They have given their consent in a general way. Because they find that there are a lot of lawless elements around here. There are a lot of communal elements here. There are subversive and separatist elements are there.

Indian society is very complex. Whatever comparative studies, I have done, I find it more complex and more problematic than societies in any other part of the world. As I have said, more than once, you think of any problem in any part of the world and I will show you a reflection of that in India. So, we such a plethora of problems. It's unimaginable for the common man. You travel from one part of the country. You have a separatist problem in Kashmir. In Punjab, you're seeing the Khalistan problem. You come to central India, you have Maoist problem. You go to Northeast, you have insurgencies, multiple insurgencies by Manipuri and Naga groups. It is in this context that people say that government needs surveillance. Government needs monitoring and interception in a general way. But as I said, the sensitivities of the exercise, the criticalities of how it could be misused or reviewed, that probably not many people are aware of.

One thing that is very encouraging is that there's a huge degree of support for the surveillance of MPs and MLAs. It is also mentioned in the report. I found it very interesting and I think it's absolutely called for. Especially when you have almost 43 percent people of questionable backgrounds in the parliament, as per the Association of Democratic Reforms. So, if people have supported their surveillance, I'm not surprised. It's a good preference they have indicated.

On Surveillance by Social Media Giants

Another area which is also a huge cause for concern but has not been highlighted to that extent, is the surveillance by social media giants. They have all the information about the Indian educated class today. I was shocked when I get a Facebook (now Meta) notification that we can prepare an album for you. I said okay, let me have it and I found the complete album of my activities for two years. I just switched off Facebook. I said I refuse to be part of such social media where it is almost tracking me and has got my album year by year, more organised than I do.

Of course, there was another reason for quitting Facebook. I found that they were promoting soft porn, very discreetly, very quietly and I wrote a nasty post about it and then quit. But the social media giants have all the information about the Indian educated class today. Every time you find a long page that these are the terms and conditions, you feel like, *Oh! Yeh bhi kaun padhega yaar? Dastakhat maro, click karo, aage badho*. (Who will read this? Just sign, click and move to the next item). That is the temptation. All the information about you is there with the social media giants based in USA and we have willingly parted with it. Can you get it back? You can't. So that is another huge area of concern but I think it has not been highlighted that much in the report.

So, I would say that surveillance is a useful tool for any state. It's a useful tool but it has to

be used discreetly. It has to be used judiciously and there has to be an accountability mechanism for it. All that could be achieved if we have proper regulatory authority. The Indian government has been working on it and their data protection bill is yet to be finalised. It has gone to the Joint Parliamentary Committee and it is yet to be passed by the parliament. But once it is finalised, the Bill has to be checked if it is weighted in favour of the government or does it take care individuals' privacy concerns. Whether it takes care of all the areas which could create problems for an individual. That still remains to be seen. I would conclude by saying that we need to strike a balance between privacy and the need for security. It won't be easy. But if you can strike a balance, surveillance would be a useful tool for the government. But if you don't strike a balance and we give overarching authority to the state, then we are heading for trouble.

Prof Ruchi Sinha, Tata Institute of Social Sciences

Before I begin it would be interesting to know that the context has been set. We are okay with staying in gated localities, yet we do not have a problem with being digitally exposed. This dichotomy is the underlying problem with surveillance and privacy. I want my privacy physically, but I don't mind being put under surveillance if it is based upon a digital community.

This context is the problem which has actually polarised all of us. Should we have it? Should we not have it? Is it good? Is it bad? These questions are so typical of what I call a stochastic experience. That is, it comes up. Snowden happened. Everybody was absolutely shaken. Oh my God! This can happen! But when Pegasus happened nobody was shocked. They're like *hota hai* (it happens). The way we have a reduced reaction than what we should have to this privacy being removed, has slowly been blunted by technology. That is where the problem is. That is what we need to understand.

On the Permeance of Technology and the Surveillance that Follows

I think that comes from the fact that our understanding of surveillance and privacy is variably different. When we talk about it, we tend to talk about it in homogeneous terms. We assume that the other is talking about or thinking about it in the same context but it's not. It's different. It is these layers of difference between surveillance and privacy that give the leeway to the power holder whether it's the state or the corporation to be able to permeate our lives. That is why we need to address that as well.

Interestingly, the neighbourhood

watch scheme is the best surveillance tool that Delhi police used before CCTV cameras came. That was something that everybody was happy about without realising that you can put anyone under surveillance. So, the neighbourhood auntie, uncle and child, everybody was supposed to be saying *kya sahi hai, kya galat hai* (what is right and what is wrong). That kind of surveillance is acceptable, but CCTV camera surveillance is not acceptable! When did CCTV cameras become so important? Everybody is now busy with their gadgets. You don't know who's travelling with you on the train, or the metro or who's walking next to you. In fact, many a times people don't even remember which bag they were carrying. They themselves don't know that. When you have blunted your understanding and awareness to this level, you have given the right to CCTV cameras to enter into your lives. Now, the logical permeance of technology in our lives has given apparently the rationale to have surveillance in place.

Jeremy Bentham is said to have made prison humane. He actually didn't make it humane. Actually, he said that the best way to have surveillance in prison is to have the panopticon. This technology is all about the panopticon. It's basically saying that I can see you, you can't see me. It is this invisibility that has made people absolutely immune to the idea of surveillance.

This invisibility is what most activists and advocates of privacy and surveillance keep trying to highlight. Every time you download an app it asks you to give access to your phonebook, the right to make calls and to read the SMS. You're saying *"okay kar dete hain"* (let's do it). Once you've done that can you imagine what all you've given away? But I don't have any problem with Google and Apple. When the *policewala* is doing it away from me, I have a problem. This difference is then used by the state *"usse problem nahi hai toh isse problem kyun hai?"* (if you don't have problem with that, then why does this bother you?) Now this is physical and that is metaphysical apparently.

On Invisible Gaze and Disciplinary Power of Surveillance

The power that is largely being circulated around is known as disciplinary power that Foucault talked about. Foucault talked about three powers. For instance, absolutist power, which was used by the monarchy. The juridical power, which Justice Chelameswar will be talking about. I'm going to be talking about the disciplinary power. Technology is using that disciplinary power. If Zomato is telling you which food to order and when, Croma is going to tell you that it's time to replace your AC, or if XYZ is saying, now it's time to do this, that's surveillance. That is surveillance of your most private desires that we are letting be but we don't react. If you're not reacting to it, I think that's a huge problem.

This invisible gaze of digital hits is something that needs to be regulated now. That is where accountability comes in. That accountability will not come from the powers up there, the corporation. It will come from us. How will it come from us? Stop downloading apps. Stop making your life so easy. Start working hard because the lesser you have to use your mental faculties the more will be the surveillance in your lives.

The surveillance is normally seen as being top-down. But many a times surveillance is also bottoms-up. There are people below you who are keeping tabs on you. That bottom-up surveillance is also a minefield of information. We completely negate it because it's bottom up. Surveillance from the power holder is credible but surveillance from the bottom is not so credible.

Horizontality of Surveillance and the Way Out

We are victims of is horizontal surveillance. That horizontality which is cutting across all of us is technology. That's another reason to understand that surveillance is not homogeneous. I would basically try to bring about the understanding that contemporary surveillance is asymmetrical. It's a place

where you are seen but I do not see who's seeing me. The data capture that I'm giving to them is giving permission for the corporations to use with the power holder. In 2001, this is where she was and today in 2023 this is what she's doing and there is a data footprint showing that she was about to do this.

Data footprint, as has already been pointed out, is the bias of the person who has done the coding. Is there any guideline that people who are doing the coding, have human rights training, have social sensitivity training, and are diversity congruent? Do we know about that? No. So, we probably need to get down to all those data centres. We need to get down to all the computer scientists educational places and say that they need to start doing that. If we don't do that it's just a reaction to an action that has taken place. There will be no solution to what we are doing.

If you don't have a problem with data misused by the corporations, the state will definitely turn around and ask why you have a problem with me if I'm doing it in the name of security. Now, security is the biggest consumable that everyone will take over. Whatever surveillance is happening is happening in the name of security. Which security are we talking about? My personal security or national security? You are not clarifying that. If you are not clarifying and crime rates are escalating, despite your CCTV cameras with security, then why should I agree or understand that your surveillance is further safeguarding me? It gives me a tool as a citizen to ask whoever is doing the surveillance, should give me a guarantee. Do we ask for guarantees? We don't. So we are laid back and we need to now stand up for our rights.

I would say that Google's Brillo, Apple's home kit, smart watches, if you are raring to be the "in person", you're also raring to give permission to someone to do your surveillance. You decide what you want to be: the in-person, the cool person or the safe person. Finally, I would say it's frightening that everything is being controlled. This control is pervasive and imposing. Unfortunately, we are only stuck with the absolutist power that is against the state but not against the others. We need to put checks for everyone.

Apar Gupta, Executive Director, Internet Freedom Foundation

I think such long-term research is incredibly important. Even when it does show findings that a large number of Indians may not be predisposed towards certain forms of privacy protections, or may support surveillance. I think it's literacy which needs to be done in terms of the social attitudes. I believe people are not a product of some biological creation solely but nurtured as per the environment which is around them.

I'd also like to thank CSDS-Lokniti for providing the methodology behind it. I really follow your work very closely around all the election-based surveys which are done. It imparts a great degree of objectivity to my own political biases. Of course, Lal Family Foundation for supporting this. This is critical work which requires to be done. It fills in gaps which are not exposed either by technology or by policy and legal analysis. This is work which needs to be done multi-year.

One thing I'd like to point out just picking up from where the last speaker left off was that we need to understand surveillance as a relationship of power. Which also explains the survey findings as they have come about. For instance, they do show that even today there's a very low deployment despite clear code directions for the installation of CCTVs in police stations by itself. This was also there in the India Justice Report.

Delhi police doesn't have audio recording. Why is that? Because it will place a system or provide information of accountability to the police forces by itself. I think this also is a realisation which comes from the repeated non-compliance with the creation of police accountability committees

which comes from Prakash Singh sir's case itself.

On Misplaced Faith in Technology for Policing

When you understand surveillance as a system of power, we can also understand some of the other findings which come through the survey. For instance, it does show that people who are lower on the socio-economic rung seem to instinctively not like surveillance. This is not born out of suspicion. It is born out of the actual experience. For instance, if you look at a report which is released about two years ago by the Criminal Justice Accountability Project. On the basis of surveys and interviews they did with tribal communities in Madhya Pradesh, they call the deployment of new technologies in violation of safeguards under criminal law and police practices, which are fairly casteist in nature. Technology is a veneer for an institutionalised system of deprivation of rights. So, it does not matter if it is AI, big data or facial recognition. It is the same police system by itself which at its underlying basis may require reform. I think our belief in technology today needs to be a little more critical. We ourselves are seeing new stories and the media ecology is flooded with statements about the potential of artificial intelligence and this fits within what is called sometimes a Gartner's Hype Cycle. In this, we expect technology to be a panacea for all our social problems, but ultimately it turns out to be a weak medicine. Here, I'd like to say that our institutionalised attitudes towards technology in policing have been there for a long period of time. Why have they come about? They have come about because there have been genuine problems in terms of resource allocation in our criminal justice system.

Let us take the Justice Malimath Committee Report on Criminal Justice Reforms, 2003. There's a conspicuous section within it. With respect to the use of technology to help solve crimes because the number of police officials per person is low but also develop and share intelligence tools and databases. We must remember, this is in 2003, when internet penetration may be 0.01 percent and computer desktop ownership would be 0.03 percent. Crimes are increasing especially with changes in technology.

A few years later the Madhava Menon's Committee on Draft National Policy and Criminal Justice had a complete chapter on electronic surveillance and use of scientific evidence. I'm not dealing with scientific evidence but there's substantial writing which is coming out that sometimes pseudo-science by itself may give the presumption of possibly evidentiary disclosure which may not be completely solving the crime but confirming an investigator's bias. I would urge people here to read Jinee Lokaneeta's book called the Truth Machines. I am trying to say in the first place that sometimes the faith we are placing in technology may not actually be met with evidence.

Let me substantiate it with a much more recent example. There was lawlessness that occurred in northeast Delhi which has a very high density of CCTV cameras. Our Chief

Minister boasts that it leads even other cities such as Tokyo, Paris and London. It also has the highest tele-density all over this country. In fact, there are about 2.4 to 2.7 active internet connections per person. RTI data suggests that between February 23 and 26, 2020 there was violence which resulted in 53 deaths, 581 injuries, 754 FIRs and 1369 arrests.

The Union Home Minister in response to this violence, on the floor of the house, as per parliamentary record, on March 11, 2020 spoke about face identification software, "It starts the process of recognising all the faces. The software does not recognise religion and attire. We have put voter ID cards, driving licenses and government data inside this software. Through it, more than 1,100 people have been arrested out of which 300 are from Uttar Pradesh." Again, there is a form of technology-determinism. Secondly, it leads to real consequences for people in terms of denial of their liberty. This statement is substantiated by the Delhi Police's Annual Report in 2020. Interestingly, you can't find it on their website any longer and also has about four pages which go on to state how the violence in Northeast Delhi was solved to a large extent with the use of CCTV footage, with data tools, with the use of the Vaahan database etc.

What is the result of all this evidence which has been gathered and all the cases which have been filed under the IPC and the UAPA? Technology is supposed to solve crimes. Technology is supposed to make these evidentiary processes better. Of course, there is a video of a person but that video is of a person at a place without indulging in violence. Sometimes, that video is of a person who's wearing a specific colour of shirt or a jacket and they have arrested another person. This is as per analysis which has been conducted by Millennium Post, which reviewed about 100 bail orders out of a total of 3500 bail orders granted so far. The police had cited CCTV and video footage in at least 44 cases to back the allegations against the accused out of which in 32, the video footage did not stand up to basic judicial scrutiny and the accused were granted bail.

Another article, if you do not like Millennium Post, is in Article-14. It states in a series of recent cases, various Delhi district courts, have granted bail while holding the police responsible for vague evidence and general allegations. Words like 'shoddy probe', 'absolutely evasive', 'vague', 'lackadaisical', 'callous', 'casual', 'farcical' and 'poor' were quoted in judicial orders.

On Budgetary Vested Interest for Surveillance

Finally, I'd like to come to why I think this is happening. I think this does not happen only because we have structurally and institutionally accepted that technology is how we will solve our policing problem. I believe there is a very important role being played by the private sector here. This is illustrated in Manisha Sethi's book Kafkaland. This is in 2008, contemporaneous with the Mumbai terror attacks, where there were CCTV vendors interacting with police departments offering modern technologies. These are budgetary processes of allocation which deprive police forces of more manpower. It is my firm belief that money is being diverted towards technologies which do not serve public purpose. In fact, it takes this money away from police itself towards their own benefit of being a better police force.

I will end by stating a FICCI and Ernest and Young report for the foundation of smart and safe cities which is claimed by cities in Punjab. I'm not drawing reference. Punjab claims that its smart cities have the capacity of real-time monitoring. This is a report which was authored by in fact Rajiv Chandrashekhar when he was the FICCI chairperson and it states, "totalising surveillance technology including centralised data system GIS which means geography-based analysis and reporting and ubiquitous CCTV cameras are the way to prevent law enforcement and national security issues."

With this, I'll end my prepared remarks and respond to certain comments which have been made earlier by panellists. I say this with a very high degree of respect as much as there is substantial agreement and some difference as well.

On Surveillance and Lack of Transparency

The first, I filed the RTI about four years ago asking for statistical information only, statistical information, numbers of the number of requests which are made, then granted, then reviewed of telephone-based interceptions in this country. There has been no data. It has been denied. It was first denied on grounds of national security thereafter it was revised and claimed that this data has been destroyed. We do not even maintain it. This matter is pending determination before the High Court of Delhi. Hence, we do not even have data. That is the level of opacity of the number of surveillance orders issued in this country today. Hence, we do not even know today if the home secretary any longer applies their mind or even has the physical capacity to affix their own signature on them.

The second is, there is a large amount of pending legal proposals which are in motion with respect to how our data is captured and how the governance frameworks are being set. However, they again represent the same view of a post-colonial state which is still aspiring to be a democracy but is not confident to give rights to ordinary Indians. The Digital Data Protection Bill is limited to data protection which means consensual sharing of data. I agree, I have knowledge, I have noticed but even there are large exemptions. This is a structural choice adopted from the time of the Sri Krishna Committee where surveillance was kept out. Hence, there is no regulation of surveillance within the digital data protection bill. It is not a comprehensive privacy bill.

Secondly, the Telegraph Act which is being proposed to be amended and as per a ministerial statement will be introduced in the monsoon session of parliament is calling it the Telecommunications Bill. But if you look at the sections of surveillance which is only a direct copy of Section 5(2) of the older Telegraph Act. In fact, it contains a provision which is titled as exclusive privilege of the central government. I will end here by stating that exclusive privilege is a phrase used by monarchs and colonies. It is not used in a democratic country. The power with the central government may be the power to license and regulate.

COMMON CAUSE UPDATES

Illegal Mining in Odisha: The matter was listed several times in 2023, where interlocutory applications filed by interested parties were disposed of and directions issued on penalties to be paid. In two related WPs, the Apex Court had raised the mining limits as well as allowed parties to lessen their contribution towards Special Purpose Vehicle formed.

On February 23, 2023 Common Cause filed an IA focussed on directing the Union of India and State of Odisha to impose limit on extraction of minerals and on constituting a committee of two or three independent experts to suggest and recommend such limit to be imposed on the extraction of iron ore in the State of Odisha and submit its report in a time-bound matter. The IA also asked for a status report with regard to amount of penalty deposited by the lessees till date (as well as the amount that is yet to be recovered) as directed in judgment dated 02.08.2017 as well as lease-wise details of the ore reserve, extraction permitted, current status of mining lease and also total iron ore reserves and total permitted extraction in the State.

Other than this, the IA seeks complete details of the work done for the benefits of tribal community in the affected districts and other area development works. As it involves public money in such a large quantity, the Special Purpose Vehicle (SPV) must fall under the purview of the Comptroller and Auditor General of India and the audit accounts of the receipts and expenditure of the SPV must be provided to the Apex Court. The matter was taken up on February 27, 2023, where the Court directed the service of IA to the standing counsel for the Union of India. Subsequently the matter was listed on March 17 and April 6, 2023 when the Court heard the IAs filed by the parties. The matter is likely to be listed on May 1, 2023.

Miscellaneous Application (MA No 1756/2022) by the Union of India seeking modification of the Supreme Court order in the Common Cause petition challenging re-appointment of the Director, ED: The Union of India (Respondent No.1) filed a Miscellaneous Application in the Common Cause petition, WP(C) 1374 of 2020, challenging the re-appointment of the ED Director, for modifying the judgment of the Supreme Court, dated September 8, 2021. By the way of the instant modification application, they have sought the deletion of the following from the judgment:

"We make it clear that no further extension shall be granted to the second respondent"

The Union of India has claimed that on the basis of the 5th proviso to Fundamental Rule 56(d) and Section 25(d) of the Central Vigilance Act, 2003 as well as various pending petitions challenging the extension of the incumbent ED Director's tenure, the above statement must be deleted from the judgment of the petition challenging the re-appointment of the ED Director.

This application has been filed as a Miscellaneous Application, disguising the review petition. Several precedents have established that the Supreme Court disapproves the practice of filing such Miscellaneous Applications seeking "modification" or "recall" or "clarification" in an attempt to bypass Order XL of the Supreme Court Rules, 1966. In addition to this, the Supreme Court has also upheld that change in law or subsequent decisions by itself could not be grounds for review and such petitions shall be accordingly dismissed. The matter was taken up on January 30, 2023, when the SC gave the Centre three weeks to respond to the petition filed by Dr. Jaya Thakur questioning the third extension given to director of the Enforcement Directorate

(ED) Sanjay Kumar Mishra, while also indicating that it will not entertain any review of its September 2021 judgment that directed against further extension to Mishra based on the law being subsequently changed. "Subsequent legislative change cannot be a ground to review our earlier order (passed on September 8, 2021)," the bench of Justice BR Gavai and Justice Vikram Nath said.

The Solicitor General stated that the petitioner was extensively relying on the September 2021 judgment where the Centre moved an application seeking clarification/modification (MA) and requested for tagging these matters together. The Bench refusing to entertain the MA said, "We will not entertain such an application. It amounts to review of our order."

The Court ordered that WP 1106/2022, 456/2022, 204/2022 and MA be tagged together and posted the matter for hearing on February 27, 2023. The Court heard the counsels on March 21 and 23 2023 and directed that it be listed at number 1 as part heard case on April 20, 2023.

Petition to Completely Ban Export of Iron Ore: Common Cause filed a writ petition in April 2021, to completely ban the export of iron ore (whether in the form of pellets or otherwise). Alternatively, it sought the levy of export duty of 30%, on the export of iron ore in all forms, including pellets (except pellets manufactured and exported by KIOCL, formerly known as Kudremukh Iron Ore Company Limited). The petition also prayed to initiate proceedings under Section 11 of the Foreign Trade (Development & Regulation) Act, 1992 and Section 135(1) of the Customs Act, 1962. In addition, it sought the levy of appropriate penalty as per law against mining companies exporting iron ore pellets in contravention of the provisions of India's export policy. By exporting iron ore pellets, they have been evading the duty chargeable on the commodity. In addition, the petition prayed for a thorough and independent investigation into the role of public officials in allowing the same. Notice was issued on September 24, 2021, directing the respondents to file their response within four weeks from the date of the order. The UOI filed its response on November 11, 2021, which was taken on record by the Court. The Union of India was directed to provide a copy of the counter affidavit to the counsel for the petitioner. Rejoinder affidavit, if any, was directed to be filed, in the meantime. The matter was taken up on February 18, 2022 when upon hearing the counsel, the Court ordered the matter to be listed on March 9, 2022 for final disposal. Further date was granted in the matter on March 22, 2022.

However, on May 21, 2022 the government increased the export duty from 0% to 45% on iron ore pellets. Recently, the export duties on certain steel products and iron ore imposed in late-May were removed and the duty on iron ore pellets has been reduced to nil again. The matter was taken up on January 17, 2023 and after hearing the counsels, the Court directed the matter to be listed for March 29, 2023. On the said date the Court heard the IAs filed by the parties and directed the matter to be listed for May 9, 2023.

Miscellaneous Application in Right to Living Will (MA No 1699/2019): On November 23, 2022, Justices KM Joseph, Ajay Rastogi, Aniruddha Bose, Hrishikesh Roy and CT Ravikumar heard SG Tushar Mehta, Mr Bhushan, Mr Datar and Dr RR Kishore. It was brought to the Court's notice that efforts have been undertaken to engage the attention of the Ministry of Health, Union of India and the efforts may have to be made to arrive at suitable draft guidelines which can be placed before the Court for consideration.

On January 17, 2023 the Constitution Bench led by Justice KM Joseph heard the application to modify the SC's 2018 Judgment which recognised the right to die with dignity and provided guidelines for terminally ill patients to refuse further treatment. The 2018 judgment also recognised the validity of 'Advance Directives', allowing individuals to provide instructions on how to proceed

if they become terminally ill, unable to communicate their wishes and seek to refuse treatment.

The Indian Society for Critical Care Medicine (ISCCM) had filed a Miscellaneous Application in July 2019 claiming the SC's guidelines were cumbersome and very few Advance Directives (ADs) were accepted and implemented. The Court directed the counsels to prepare a chart comparing the SC's 2018 guidelines along with the changes suggested by the parties for the hearing on January 18, 2023.

On January 18, 2023, the counsel for the petitioner attempted to convince the Bench to include persons in a 'permanent vegetative state' who are not at risk of death but have no hope of recovery and no ability to communicate their wishes. This was not accepted by the Bench. It was suggested that instead of requiring the Judicial Magistrate to sign the AD, it can simply be attested by a notary public. The Bench appeared to be more amenable to this suggestion, although Justice Joseph suggested that someone should keep a copy of the AD for counterchecking purposes. The counsel provided a possible solution referring to the government portal maintained by the National Digital Health Commission. It was suggested that individuals could upload their ADs to the portal and it could be made available to doctors in the hospital where they eventually sought treatment. Removing the requirement for a second medical board to review the decision of the primary medical board, as well as limiting the number of members to three was also suggested. It was claimed that this would make the process more efficient. The Bench mandated a four-member board comprising the treating physician and three 'subject-experts'.

On January 19, 2023, the Bench directed the parties to submit a joint proposal by January 24, 2023. On January 24, 2023, the Bench orally delivered the order and accepted the joint proposal submitted by ISCC and the Union of India, subject to the minor changes proposed by the Bench during the hearings. The order contains a table of all the changes. Before concluding the proceedings, Sr. Adv. Datar gave the Bench a parting gift. Each judge received a signed copy of Arun Shourie's book 'Preparing: For Death'.

Contempt Petition against Lawyers Strike: The contempt petition filed by Common Cause against the strike of lawyers in Delhi High Court and all district courts of Delhi on the issue of conflict over pecuniary jurisdiction was eventually taken up on November 2, 2022, where the Court asked for short notes on the proposed submissions and the propositions by the parties within four weeks. The matter was listed next on December 6, 2022, when on behalf of the petitioner, advocate Prashant Bhushan told the Bench that the Bar Council of India (BCI) had not suspended those who went on strike. "We expect a serious response from you," the Bench told advocate Ardhendumauli Kumar Prasad, who represented the BCI. Noting that suspension was not sufficient, the Supreme Court said major steps were needed against striking lawyers. "BCI is the apex body and should act like one. What are the preventive measures being taken? This can never acquire the proportions of adversarial litigation," a Bench led by Dinesh Maheshwari said while hearing the contempt petition. The matter was taken up on January 24, 2023 when the counsel appearing for the Bar Council of India prayed for yet further time to complete all his instructions as also to advice appropriately. On March 28, 2023 the Court taking note of the submissions made by learned counsel, appearing for the Bar Council of India in their affidavit dated 13.03.2023 and providing them time to take the contemplated processes to finality, deferred consideration of the matters to April 17, 2023. On April 17, 2023 the Chairman, Bar Council of India, informed the Court that further process was actively being taken up as regards the framing of Rules. He has also indicated that in another matter involving akin issues, order has been reserved in. Taking note of the submissions the Court listed the matter for

May 8,.2023, as prayed.

Introduction of Electoral Bonds Challenged: On March 21, 2023, the Supreme Court said it would consider whether the pleas challenging the validity of the electoral bond scheme for political funding of parties could be referred to a Constitutional Bench for an "authoritative pronouncement". Looking at the current data, Electoral bonds have legitimised unaccounted-for money to the tune of more than Rs 12,000 crores in our electoral and political process, where the citizens do not know the names of the donors. Under the circumstances, the Court's observations to decide whether the pleas could be referred to a Constitution Bench assume great significance.

Common Cause and the Association for Democratic Reforms (ADR) challenged the introduction of Electoral Bonds, which was introduced by amending Finance Act 2017. These bonds have not only made electoral funding of political parties more opaque, but also legitimised high-level corruption at an unprecedented scale by removing funding limits for big corporates and opening the route of electoral funding for foreign lobbyists. The PIL sought direction from the Supreme Court to strike down the amendments brought in illegally as a "Money Bill" in order to bypass the Rajya Sabha.

On November 22, 2022, a new petition challenging the government notification allowing the sale of electoral bonds for an additional 15 days in Assembly election years was tagged with our case. This petition filed by Dr Jaya Thakur sought the quashing of the November 7, 2022 notification issued by the Finance Ministry amending the electoral bonds scheme. "An additional period of 15 days shall be specified by the central government in the year of general elections to the legislative assembly of states and Union territories with the legislature," the gazette notification had said. Earlier, a 30-day extra period for sale was allowed only in Lok Sabha election year.

On March 21, 2023, the Court granted three weeks' time to the Union of India to file its counter affidavit. It also appointed two lawyers from both the petitioner as well as respondents' side to act as nodal counsel for ensuring a smooth hearing of the PILs, and directed them to prepare a common compilation containing the written submissions, copies of judgments and any other material that the parties seek to rely upon at the time of the hearing. However, the matter could not be taken up on April 11, 2023 as dictated by the SC and is likely to be taken up on April 25, 2023.

Writ for Supreme Court Directions on Police Reforms: The battle for police reforms has been going on for the last 26 years. The Supreme Court took 10 years to give a historic judgment in 2006, in the petition filed by Prakash Singh, Common Cause and NK Singh. Since then, it has been a struggle to get the Court's directions implemented. On July 3, 2018, responding to an interlocutory application filed by the Ministry of Home Affairs regarding the appointment of acting Director General of Police (DGP) in the states, the Supreme Court gave a slew of directions to ensure that there were no distortions in such appointments. It laid down that the states shall send their proposals to the UPSC three months prior to the retirement of the incumbent DGP. The UPSC shall then prepare a panel of three officers so that the state can appoint one of them as DGP. In October 2022 and December 2022, the Court entertained applications filed by the State of Nagaland and the UPSC to finalise the names of DGP for the state. The matter is directed to be listed for January 9, 2023. In January 2023, the matter was listed twice, when the Court decided on the IA filed by the State of Nagaland on appointment of DGP.

FUNDAMENTAL RIGHTS AND DUTIES

Rights beget empowerment for citizens. They enable them to participate in public affairs and to lead a life of dignity. Rights are also the bedrock of the citizens' legitimate entitlements from the State, their freedom and personhood. Every great nation is defined by the rights of their citizens. In most modern liberal democracies, citizens are meant to be sovereign, equal before the law, and morally autonomous beings, free to pursue their enlightened self-interest.

However, it is equally true that citizenship comes not only with Fundamental Rights but also with Fundamental Duties. After all great power comes with great responsibility. Those who make demands on the system for their Fundamental Rights must give back to the system by fulfilling their responsibilities as citizens. These duties should not be taken lightly, for they are just as important to our national identity as our Fundamental Rights. The notion of Fundamental Duties does not run counter to our freedoms, but rather the two occur in harmony, for a country is run for its citizen and by its citizens, and as citizens we cannot simply take without giving back.

It is perhaps in this spirit that Article 51(a) of the Constitution of India enlists the Fundamental Duties that cast upon the citizens a moral obligation to:

1. To abide by the Constitution and respect its ideas and institutions, the National Flag and the NationalAnthem;
2. To cherish and follow the noble ideals which inspired our national struggle for freedom;
3. To uphold and protect the sovereignty, unity and integrity of India;
4. To defend the country and render national service when called upon to do so;
5. To promote harmony and spirit of common brotherhood among all the people of India, transcending religious, linguistic, regional or sectional diversities, to renounce practices derogatory to the dignity of women;
6. To value and preserve the rich heritage of our composite culture;
7. To protect and improve the natural environment including forests, lakes, river, and wildlife and to have compassion for living creatures;
8. To develop the scientific temper, humanism and spirit of inquiry and reform;
9. To safeguard public property and to abjure violence;
10. To strive towards excellence in all spheres of individual and collective activities so that the nation constantly rises to higher levels of endeavor and achievement;
11. To provide opportunities for education to his child or, as the case may be, ward between age of 6 and 14 years;

Printed & Published by Vipul Mudgal on behalf of Common Cause, 5 Institutional Area, Nelson Mandela Road, Vasant Kunj, New Delhi 110070, Printed at PRINTWORKS, C-94, Okhla Industrial Area, Phase - 1, New Delhi - 110020
Editor-Vipul Mudgal Tel No. 26131313, 45152796, email: commoncauseindia@gmail.com, website:www.commoncause.in