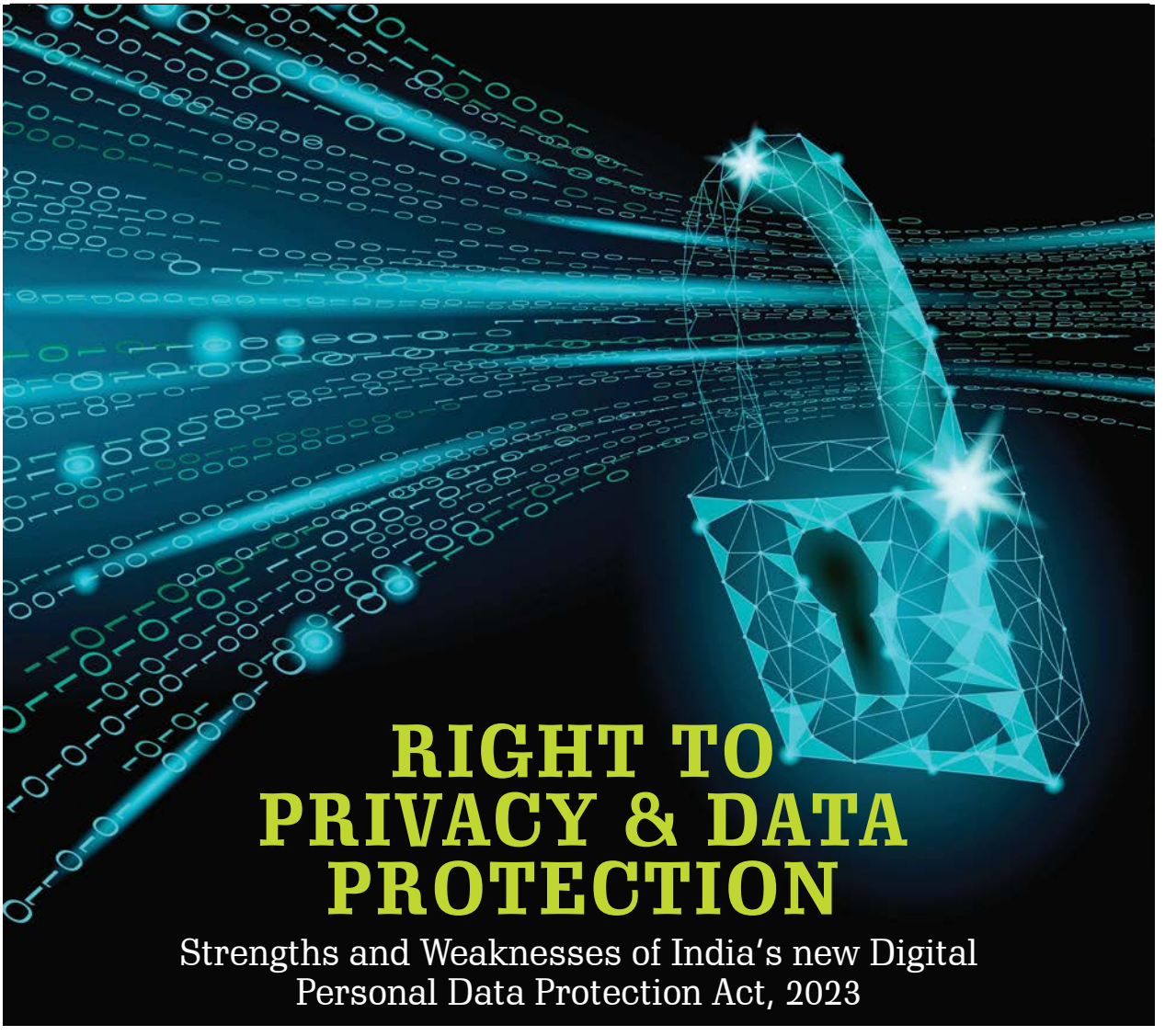
Vol. XLII No. 3 July-September, 2023

COMMON CAUSE

www.commoncause.in

POLICY-ORIENTED JOURNAL SINCE 1982



RIGHT TO PRIVACY & DATA PROTECTION

Strengths and Weaknesses of India's new Digital Personal Data Protection Act, 2023

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

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Technical Terms Explained

We expose our personal data with various stakeholders, for a myriad of reasons throughout our life. The Digital Personal Data Protection Act, 2023 aims to provide a legal framework for the processing of individual's digital personal data in India, and hence, everyone needs to know the basics of the law. For our readers to have a better understanding of the DPDP Act, we are providing a small glossary, defining a few important and technical terms, as per the law:

Appellate Tribunal	The appellate body, to be approached against the decisions of the Data Protection Board of India
Data	A representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means
Processing or Data Processing	A wholly or partly automated operation or set of operations performed on digital personal data. It includes collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction
Person	Person includes an individual, a Hindu Undivided Family, a company, a firm, an association of persons or a body of individuals, the state and every artificial person, any non-human legal entity considered as a person
Personal Data	Any data about an individual who is identifiable by or in relation to such data
Digital Personal Data	Personal Data in digital form
Data Principal	Individual(s) who owns the personal data and in case of a child or person with disability, their parents or lawful guardian
Data Fiduciary	Any person that determines the purpose and means of processing personal data
Data Processor	Any person who processes personal data on behalf of a Data Fiduciary
Notification	A notification published in the Official Gazette. Terms notify and notified to be understood similarly
Personal Data Breach	Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data
Significant Data Fiduciary	A Data Fiduciary or class of Data Fiduciaries that is notified by the Central government. Significant Data Fiduciary is identified on the basis of various factors; such as volume and sensitivity of personal data they process or for the sovereignty and integrity of India, etc.
Data Protection Officer	An individual appointed by the Significant Data Fiduciary to act as a point of contact for grievance redressal
Specified Purpose	The purpose mentioned in the notice given by the Data Fiduciary to the Data Principal for processing their data
The Data Protection Board of India	An adjudicatory body established by the Central Government to determine the non-compliance with provisions of DPDP Act, 2023 and impose penalty as per the provisions of the Act

A COMPLEX BUT VITAL LAW

Can the DPDP Act Secure our Data

In a cursory reading, the Digital Personal Data Protection (DPDP) Act comes across as complicated. Its clauses, technical terms, and add-ons can be boring and convoluted. But be cautioned: we shall ignore this vital Act at our own peril. Sooner or later, all of us will have to know – or suffer – its consequences. That is why it is a good time to start making sense of it.

This special issue of your journal tries to discuss the Act in its overall context. The idea is to appreciate the value of our data and begin to think about its full protection individually as well as collectively. We have tried to explain the provisions of the Act in simple terms through FAQs and focused articles. A glossary of technical terms is given on the preceding page while a timeline follows on the next page.

As we know, our daily activities create digital footprints that can be accessed, stored or shared by multiple agencies. We generate personal data virtually all the time: when we follow a digital map, order things online, share a joke or a selfie, make a payment, or just phone a friend. Even while we sleep, our smart watch records our heartbeats and sleep patterns. CCTV cameras do the same when we take a walk in the park. All such data is of enormous value for multiple players like governments, businesses, scammers, political parties, or entities based overseas.

Some of this data keeps slipping out of our hands with or without our knowledge. When we use an app, or when we make a UPI payment, we give our consent to third parties to process that data, presumably for lawful purposes. Often, we do not even know if and when such consent was given. This is where a data protection law steps in. The DPDP Act aims to protect the privacy and personal data of individuals. The Indian law draws on the European General Data Protection Regulation (GDPR) but many feel that it falls short of its stated objectives.

The DPDP Act applies to all personal data collected online or digitised from offline sources. It grants an individual the right to obtain information regarding personal data, seek corrections, and ensure redress of grievances. The objective is to ensure that data is maintained accurately, stored securely, and erased when its purpose has been met. The law permits the transfer of data overseas with certain conditions. It has a compliance and oversight mechanism for organisations and companies with provisions for penalties through a proposed Data Protection Board.

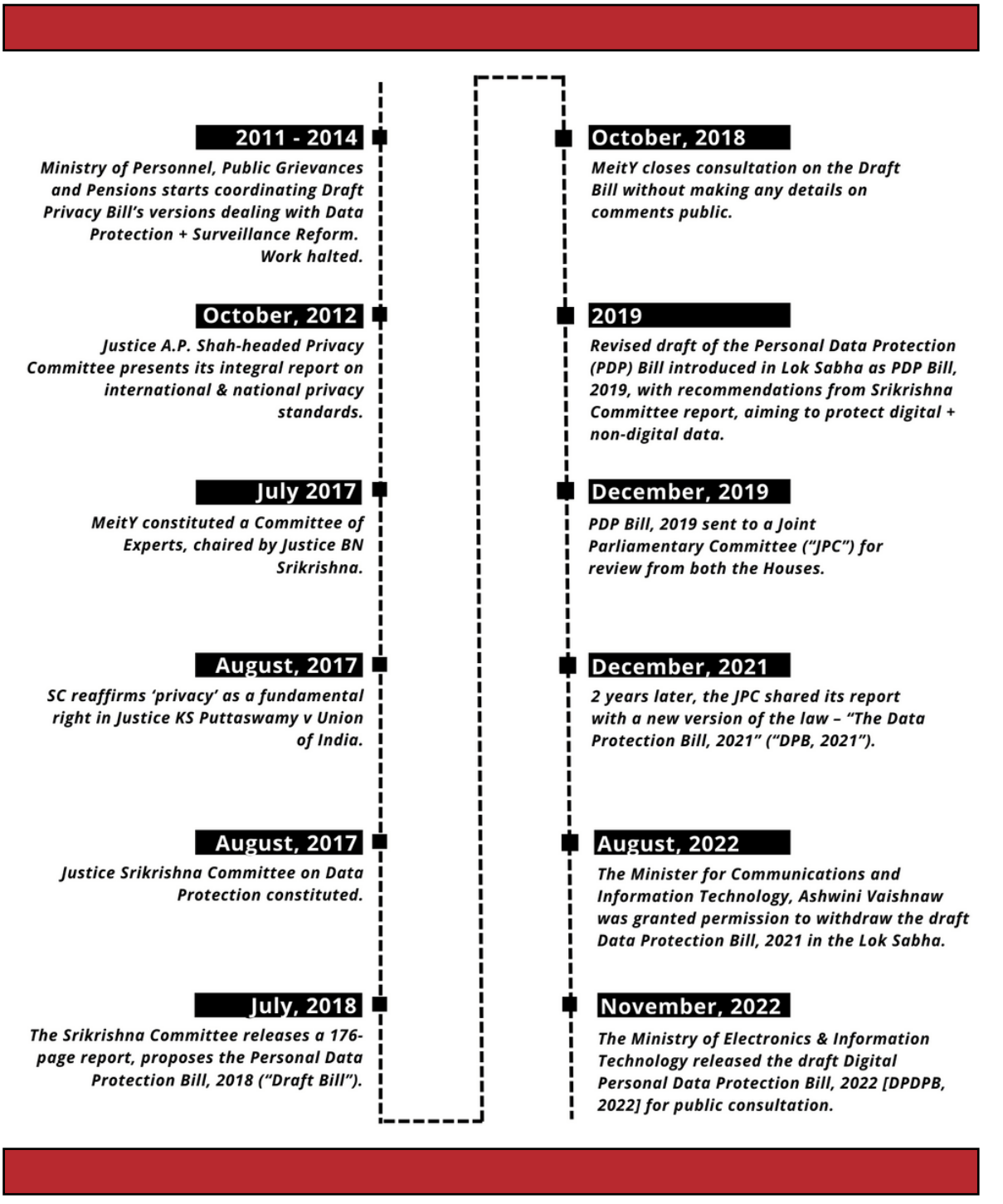
The main criticism of the DPDP Act comes from the sweeping exceptions it provides to the state and its agencies. This is also a point of departure from the European GDPR which puts the autonomy of the individual at the centre. The DPDP Act overrides consent for certain purposes vaguely defined under the umbrella of national security, public safety, and prevention of offences. It also makes the citizens vulnerable to data breaches and mass surveillance.

For a healthy relationship between technology and democracy, the law has to catch up quickly with the fast-changing digital world. As citizens, we do not tend to protect our general data as keenly as we guard our investments or bank accounts. But a fair and progressive law requires us to be sufficiently aware of all its implications in light of our fundamental right to privacy. This issue is a step in that direction.

As always, your comments are welcome at commoncauseindia@gmail.com.

Vipul Mudgal
Editor

TIMELINE : 2011-2023



Source: Internet Freedom Foundation

WHY IS DATA SO VALUABLE?

The Idea of the New Data Protection Law

Tushar Dhara*

The Digital Personal Data Protection Act, 2023 was passed in August. It was preceded by several years of debates and postponements but the final draft was passed without much deliberation in Parliament. In just over a week, the final draft Bill breezed through the lower and upper Houses of the Parliament and received Presidential assent. The Act (DPDP henceforth) provides a legal framework "for the processing of digital personal data"[i]. India is the last but one country in the G20 to pass a data protection law – which it did while holding the G20 presidency.

Why has data become so valuable? In the early 2000s Clive Humby, a British mathematician coined the phrase "Data is the new oil"[ii] . The statement has proved to be amazingly prescient. Consider the following metric: In 2006, the Financial Times estimated the top ten companies in the world based on market capitalisation (M-cap). ExxonMobil, the American oil and gas giant, was ranked number one at $446 Billion. In all, there were three other fossil fuel companies in the top ten: British Petroleum, Royal Dutch Shell and Gazprom[iii]. In 2023 the top ten list is dominated by tech firms. Apple - valued at around $3 Trillion - leads the list, followed by Microsoft, Alphabet (formerly Google) and Amazon. Meta (formerly Facebook) clocks in at number eight with a capitalisation of $735 Billion. The only energy firm in the top ten today is Saudi Aramco. Markets see more value in companies that have vast pools of data rather than vast reservoirs of oil and gas.

According to an estimate by Forbes magazine, 3.7 billion people worldwide use the internet and produce 2.5 quintillion bytes of data every single day![iv] This estimate was made five years ago. A 2021 report by the Parliamentary committee on the Personal Data Protection said that the size of the internet is 44 zettabytes (one zettabyte is a billion terabytes).[v] The report further notes that India generates 150 exabytes of data annually (an exabyte is a million trillion bytes). India - with an economy of around $3.75 trillion, over 700 million internet users and 600 million active smart phones - is one of the fastest growing data nations in the world.

The increasing digitalisation of life means that every person generates a data footprint that can be collated and used by an entity to create a 360-degree profile: An individual's opinions through her social media posts, favourite cuisine via orders on food delivery apps, places visited from trip data, purchases on e-commerce sites like Amazon or Big Basket, financial data from payment apps, personal details like age,

**Tushar Dhara is the Deputy Editor at Inclusive Media for Change*

sex, mobile numbers and email ids from online forms, and likes from Google searches.

Data has thus become a vital new resource for building the next generation of businesses. By integrating discrete datasets and applying algorithms and machine learning, new insights can be derived. India already has multiple datasets, including Aadhar, passport seva, open data stack (data.gov.in), the MCA21 data dump containing information on Indian corporates, goods and services tax network (GSTN), water resources information system (WRIS) housed within the Department of Water Resources, the Ministry of Rural Development's DISHA and the Indian Space Research Organization's Bhuvan[vi]. In addition, the government is pushing for a national digital public infrastructure under the moniker 'India Stack'[vii]. India Stack is the collective name given to a set of open APIs that operate across identity, payments and data. Application Programming Interfaces - or APIs - are software tools that developers can use to build more complex apps. The bedrock of India Stack is a set of digital products centered around Aadhar, including Aarogya Setu, Unified Payments Interface (UPI) and FASTag.

This burgeoning information economy needed a comprehensive law to protect and regulate personal data.

What are the Main Provisions in DPDP?

The DPDP law borrows from the EU's GDPR approach when defining "personal data" and extends coverage to all entities which process personal data. The law also has significant extraterritorial application. The DPDP has narrowly defined lawful grounds for processing personal data, while at the same time establishes purpose limitation obligations. It also creates a set of rights for individuals whose personal data is processed, including rights to receive notice, access and erasure. Further, it establishes a supervisory authority called the Data Protection Board of India.

At the same time DPDP provides significant exceptions to government bodies, especially law enforcement agencies. Other exemptions include publicly available personal data, processing for research and statistical purposes, and processing the personal data of foreigners by companies in India pursuant a contract with a foreign company (such as outsourcing companies). The Act also empowers the union government to request access to any piece of information from a data processing entity or an intermediary.

The DPDP Act establishes a national framework for processing personal data, replacing the more limited IT Act[viii]. Only digital personal data - or regular personal data that has been subsequently digitised - is covered by the law. *Digital* personal data has been defined as any data that can be used to identify an individual. However, DPDP does not contain increased protection for sensitive data like biometrics, health information, sexual orientation or religious affiliation.

Some Broad Exceptions - Public and Private

The law also includes some broad exceptions for data activities that threaten the "sovereignty and integrity" of India, the security of the state, etc. Justice Srikrishna is critical of such exemptions[xi]. Some targeted exceptions also apply to companies, and are either well defined in the law or left to the government for specification. Under what can be called an "outsourcing exception," the Act exempts companies based in India who process the personal data of people outside of India.

Almost No Restrictions on International Data Transfers

The definition of the "data principal" does not include any conditions related to residence or citizenship, meaning that fiduciaries based in India which process the personal data of foreigners within Indian

territory may be covered by the Act. The Act also applies extraterritorially to processing of digital personal data outside India, if such processing is related to data principals within India. The DPDP does not currently restrict the transfer of personal data outside of India, unless the government specifically restricts transfers to certain countries (blacklisting).

> ***"The DPDP Act requires that consent for processing of personal data be "free, specific, informed, unconditional and unambiguous"***

Consent - the Primary Means for Processing Personal Data

Data fiduciaries need a lawful purpose to process personal data and this can be obtained either through consent by the data principal or for "legitimate use". Based on the wording of the Act, fiduciary obligations to give notice and respond to access, correction and erasure requests are only applicable if the processing is based on consent.

The DPDP Act requires that consent for processing of personal data be "free, specific, informed, unconditional and unambiguous." People whose personal data is processed must freely give their consent, without tying it to other conditions. In order to meet the "informed" criterion, the Act requires that notice be given to principals before or at the time that they are asked to give consent. The notice must include information about the personal data in question, the purpose for processing, the rights of data principals, and how to register a complaint to the Board.

Data principals must be given the option of receiving the information in English or a local language. The DPDP addresses the issue of legacy data, for which companies may have received consent prior to the enactment of the law. Fiduciaries have to provide a new notice to the data principals for the reuse of legacy data as soon as "reasonably practicable." In which case, the data processing may continue till consent is withdrawn. Data fiduciaries can process personal data for the specific purpose provided to the data principal, and must obtain separate consent to process old data for a new purpose.

Data Principals - Rights and Obligations

The DPDP Act provides data principals a set of enumerated rights, which is limited compared to GDPR-style legislation passed by the European Union. The DPDP guarantees right of access, erasure and correction. However, rights to data portability or objecting to processing based on grounds other than consent, and the right not to be subject to automated decision-making are missing. To compensate, DPDP provides for two other rights: grievance redressal and a right to appoint a nominee on behalf of the principal.

Section 15 of DPDP imposes duties on data principals, including an obligation to not impersonate or withhold information while providing personal data for government documents. Register a false or frivolous grievance is punishable. Non-compliance can result in a fine.

Parental Consent for Processing Personal Data of Minors

DPDP creates significant obligations for processing children's personal data, with "children" defined as people under 18 years. Data fiduciaries are forbidden from processing children's data that is "likely to cause any detrimental effect on the well-being of the child". Data fiduciaries need to obtain verifiable parental consent before proceeding with such data. Similarly, consent must be obtained from a lawful

guardian before processing the data of a person with disability. The Act also prohibits data fiduciaries from tracking children, or targeting them with advertisements.

The Act Creates a Data Protection Board to Enforce the Law

The DPDP Act empowers the government to establish a Data Protection Board as an independent overseer. The Board will have a chairperson and government-appointed members. The Board has been vested with the power to receive and investigate complaints, after the principal has exhausted the grievance redress mechanism set up by fiduciaries. While the Board is granted "the same powers as are vested in a civil court", the Act specifically excludes any access to civil courts in the application of its provisions, creating a *de facto* limitation on effective judicial remedy.

How Does The DPDP Act Affect Civil Society and Media?

Civil society, journalism bodies, opposition MPs and privacy rights organisations have raised several objections to the Act.

An analysis by the Internet Freedom Foundation finds that the legislation fails on key parameters of what a good privacy law should strive for[x]. The key principles of privacy are purpose limitation, data minimisation, accuracy and storage limitation. However, The DPDP Act compromises purpose limitation by stating that data can be processed without consent for "certain legitimate uses". On data minimisation and storage limitation, the right to erasure is limited by the need to retain information for "compliance with any law for the time being in force" [Clause 12(3)] - which when combined with various sectoral/ other data retention requirements, may result in heavy dilution of this right. Clause 17(3) gives the government the ability to exempt a data fiduciary, including start-ups, from the requirement on completeness, accuracy and consistency of personal data.

Moreover, several Members of Parliament have raised concerns about the removal of the terms like "privacy", "harm", and "compensation" in the DPDP Bill, 2023[xi]. MPs have also questioned why the right to be forgotten and right to data portability was removed in the Act when it was part of the 2019 draft, and whether the data protection board will be independent. More seriously, there seems to be an absence of surveillance reform and a slew of fresh blocking powers that the Act hands to the government under Clause 37(1). Given the Pegasus spyware issue, the absence of checks on surveillance from a law that purportedly protects personal data raises questions about intent.

Concerns have also been raised by the journalists' fraternity. The Editors Guild of India has expressed concern that the DPDP Act doesn't provide exemptions for journalistic activities. In a statement[xii] it said that, "We are deeply concerned about the lack of exemptions for journalists from certain obligations of the law, where the reporting on certain entities in public interest may conflict with their right to personal data protection. This will lead to a chilling effect on journalistic activity in the country". The Guild also noted that the Act doesn't seem to contain any provisions for surveillance reform, and in fact widened the censorship powers vested in the government.

The Digipub News India Foundation, a body of digital media organisations, has expressed similar concerns. In a statement they noted that DPDP, 2023, could "potentially impinge on citizens' and journalists' rights to privacy, information, and freedom of expression." Digipub has expressed concern about potential censorship and surveillance of journalists, and the lack of exemptions for journalistic activities.

The watering down of the Right to Information by the DPDP Act is a serious concern that has been flagged. Section 44 of the Act introduces amendments to other laws, ostensibly to protect privacy. Subsection 3 inserts the following line in Section 8 of the RTI Act: "information which relates to personal information". Former Central Information Commissioner Sailesh Gandhi explains that this amendment would allow the government to decline any RTI requesting information relating to an individual. In a public petition, Gandhi has urged the Prime Minister to ensure that the change does not override or amend the RTI Act[xiii].

Endnotes

i The Digital Personal Data Protection Act, 2023

ii Viernes, F. A. (2021, September 14). Stop Saying 'Data is the New Oil' | by Francis Adrian Viernes | Geek Culture. Medium. Retrieved August 16, 2023, from https://bit.ly/48Lg4xj

iii Wikipedia. (n.d.). List of public corporations by market capitalization. Wikipedia. Retrieved August 18, 2023, from https://bit.ly/45AralH

iv Marr, B. (2019, March 9). How Much Data Do We Create Every Day? Forbes. Retrieved August 19, 2023, from https://bit.ly/46ynySH

v Loksabha Secretariate. (2021, December). LOK SABHA .REPORT OF THE JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019 SEVENTEENTH LOK SABHA LOK SABHA SECRETARIAT. Parliament Digital Library. Retrieved August 18, 2023, from https://bit.ly/46PNCZd

vi ibid.

vii Pandey, J. (2019, March 9). India Stack: Public-Private Roads to Data Sovereignty. Internet Governance. Retrieved August 16, 2023, from https://bit.ly/3SfxcFJ

viii Supra Note i

ix SAIGAL, S. (2019, March 9). Data Protection Bill | Granting government exemption causes great concern, says Justice Srikrishna. The Hindu. Retrieved August 19, 2023, from https://bit.ly/3LZanSs

x Internet Freedom Foundation. (2023, August 9). DPDPB, 2023 in the Parliament: Dialogue, Drama, and Discord. Internet Freedom Foundation. Retrieved August 13, 2023, from https://bit.ly/48SymN1

xi Supra note xxii

xii Editors Guild of India. (2023, August 6). EGI statement on Digital Personal Data Protection Bill, 2023. Editors Guild of India. Retrieved September 16, 2023, from https://bit.ly/3RZzecU

xiii Gandhi, S. (2023, August 7). Save RTI : Citizen's Empowerment. Change.org. Retrieved September 16, 2023, from https://bit.ly/3Qf0dj3

HOW DOES THE DPDP ACT AFFECT MY LIFE?

Some Frequently Asked Questions

Anshi Beohar*

An individual's personal data is as unique and identifiable as any other biometrics such as the fingerprints or the iris of one's eye. From using one's Aadhar card to filling an application form to making an online purchase or even just browsing the internet, we share a piece of our personality. And it is in this kind of daily activities that our individual identity could be recognised. Often this processing of data helps us, like selecting the right products or services, finding jobs or life-partners, or for setting reminders to pay our bills, but this could also be misused to cheat or mislead us.

On August 11, 2023, the Digital Personal Data Protection Act, 2023 was brought into force to attend to some of these concerns. The law deals with digital personal data and the rights and obligations of the stakeholders as well as with penalties in case of violations. Although several provisions need more specification, that is achievable only when the rules are created by the central government.

Some of the frequently asked questions related to the DPDP Act, 2023 are answered below:

1. What is the DPDP Act, 2023?

The Digital Personal Data Protection Act, 2023 is now the primary law that deals with data protection in India. The Act recognises the individual's right to protect her digital personal data and deals with the need to process such personal data for lawful purposes and for protecting it.

2. When is it applicable?

The personal data of a Data Principal may be processed for lawful purposes and for legitimate uses. The DPDP Act is applicable on:

- The processing of digital personal data within the territory of India where the personal data is collected
  - » in digital form, or
  - » in non-digital form and digitised subsequently
- The processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

3. When is it not applicable?

The DPDP Act is not applicable on:

- Personal data processed by an individual for any personal or domestic purpose, and
- Personal data that is made or caused to be made publicly available by—
  - » the Data Principal to whom such personal data relates, or
  - » any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

4. What are the grounds for processing personal data?

The personal data of a Data Principal may be processed for a lawful purpose - a purpose that is not expressly forbidden by law - only in accordance with the provisions of this Act for which the consent has been given or for certain legitimate uses.

**Anshi Beohar is the Manager (Law and Policy) at Common Cause*

The DPDP Act allows for the following legitimate uses of personal data by Data Fiduciaries:

- where the Data Principal has voluntarily provided her personal data for a specific purpose, and has not indicated that she does not consent to the use of her personal data in that respect.
- where the state or any of its instrumentalities require the personal data for providing any subsidy, benefit, service, certificate, licence or permit to the Data Principal (keeping in mind the policy issued by the central government or any law for the time being in force for governance of personal data), -
  - » she has previously consented to the processing of her personal data by the state or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit, or
  - » the personal data is either digitally available or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the state or any of its instrumentalities and is notified by the central government
- for the performance by the state in the interest of sovereignty and integrity of India or security of the state; for fulfilling legal obligations; for compliance with judgments; during medical emergencies or disasters, etc.

5. What is the mechanism of processing personal data?

In order to process personal data, the Data Fiduciary must issue a request accompanied or preceded by a notice to the Data Principal, with an option to access the contents of the notice. The notice will contain the personal data, the purpose of processing the data, the manner to provide (or withdraw) consent or access grievance redressal as well as the manner to make a complaint to the Board.

6. What are the provisions for consent under the Act?

The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Every request for consent shall be presented to the Data Principal. The contact details of the Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal must be provided as well.

The Data Principal shall have the right to withdraw consent at any time where the personal data is processed on the basis of the consent provided. If the consent is withdrawn by the Data Principal, the Data Fiduciary shall cease and cause its Data Processors to cease processing the personal data of such Data Principal within a reasonable time, unless legally authorised.

7. What are the responsibilities of a data fiduciary?

A Data Fiduciary shall be responsible for complying with the provisions of this law for any processing they undertake even if the Data Principal fails to carry out their duties under this law or any other agreement to the contrary.

Data Fiduciaries are responsible to protect personal data in its possession by taking reasonable security safeguards to prevent personal data breach. Any breach in observing the obligation of Data Fiduciary may lead to a penalty extending up to Rs 250 crore.

Data Fiduciary shall intimate the Board and each affected Data Principal if there is a personal data breach. Any breach, subject to legal provisions, may lead to a penalty extending up to two hundred crore rupees.

In addition to this, unless otherwise directed, Data Fiduciaries must:

(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and

(b) cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for

processing to such Data Processor.

Data fiduciaries have to publish the contact details of the Data Protection Officer or a person who will answer the questions about the processing of personal data. Data fiduciaries will have to establish an effective grievance redressal mechanism.

8. Do additional obligations apply to processing of personal data of children or a person with disability?

The DPDP Act imposes additional obligations on data fiduciaries in relation to processing of personal data of children and persons with disability with legal guardians. The Data Fiduciary is mandated to obtain verifiable consent from the parents or legal guardians before processing personal data of children (individuals below 18 years of age) and persons with disability.

The Act however prohibits processing of children's data that is likely to cause any detrimental effect on the well-being of a child or tracking or behavioural monitoring of children or targeted advertising directed at children, unless otherwise authorised under law.

Any breach in observance of additional obligations under section 9 of the DPDP Act, 2023 may lead to a penalty extending up to Rs 200 crore.

9. Who is a Significant Data Fiduciary and do they have any additional obligations?

Any Data Fiduciary or class of Data Fiduciaries as may be notified by the central government on the basis of an assessment of certain factors such as the volume and sensitivity of personal data processed; risk to the rights of Data Principal; potential impact on the sovereignty and integrity of India; risk to electoral democracy; security of the state; and public order.

In addition to the obligations of the Data Fiduciary, a Significant Data Fiduciary must also abide by the following:

- Appoint a Data Protection Officer (DPO) based in India, to represent them. This DPO must be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary and must act as the point of contact for the grievance redressal mechanism.
- Appoint an independent data auditor to carry out data audit, who shall evaluate compliance on their behalf.
- Conduct periodic Data Protection Impact Assessment, a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed.
- Conduct periodic audits
- Undertake such other measures, consistent with the provisions of this Act, as may be prescribed.

Any breach in observance of additional obligations of Significant Data Fiduciary under section 10 of the DPDP Act, 2023 may lead to a penalty extending up to Rs 150 crore.

10. What are the rights of a data principal?

These are the rights available to a Data Principal under this law:

1. Right to access information about their personal data

If the Data Principal has consented, they have a right to obtain regarding summary of personal data being processed, the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared and any other relevant information, subject to conditions.

2. Right to correction and erasure of personal data

A Data Principal can correct, complete, update and erase personal data for which consent has been given previously, subject to legal restrictions.

3. Right of grievance redressal

A Data Principal must be provided by a Data Fiduciary or Consent Manager, with the means to access grievance redressal mechanisms with respect to any act or omission in relation to their obligations or the exercise of the Data Principal's rights during the handling or processing of their personal data. The Data Fiduciary or Consent Manager shall respond to any grievances within the legally ascertained time period. This right needs to be exercised before approaching the board.

4. Right to nominate

A Data Principal shall have the right to nominate any other individual to exercise their rights in the event of death or incapacity (inability to exercise the rights or unsoundness of mind or infirmity of body) of the Data Principal.

11. What are the duties of a data principal?

This law has assigned the following duties to the Data Principal:

- Compliance with the provisions of all applicable laws while exercising rights under the DPDP Act
- To not impersonate another while providing personal data
- To not suppress any material information while providing personal data
- To not register a false or frivolous grievance or complaint
- To furnish only verifiably authentic information while exercising the right to correction

Any Data Principal found in breach in observance of the duties may face a fine extending up to Rs 10,000.

12. Can data be shared with foreign entities?

The DPDP Act provides that the central government may restrict the transfer of personal data to certain notified countries. If any other law provides for a higher degree of protection or restriction on transfer of personal data by a Data Fiduciary outside India, this Act shall not restrict it.

13. What are the exemptions under DPDP Act?

There are certain circumstances, that are completely exempted from the DPDP Act:

- Where the central government has asked to furnish and process any personal data in the interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order or preventing incitement to any cognisable offence relating to any of these
- Where the personal data is necessary for research, archiving or statistical purposes but the it is not to be used to derive specific decisions
- Certain other circumstance will attract limited exemptions:
- Where processing of personal data is necessary for enforcing any legal right or claim
- Where the personal data is processed by courts, tribunals etc.
- Where the personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law
- Where the personal data is processed pursuant to a contract with any person outside the territory of India by any person based in India
- Where the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction (or division) by way of demerger or otherwise of a company, approved by a court or tribunal or other competent authority
- Where the processing is done to ascertain the financial information and assets and liabilities of any person who has defaulted in payment against a loan or advance taken from a financial institution

In addition to this, the central government may notify and exempt certain Data Fiduciaries.

14. What is the grievance redressal mechanism?

Data fiduciaries have to publish the contact details of the Data Protection Officer or a person who will answer the questions about the processing of personal data. For this, data fiduciaries will have to establish an effective grievance redressal mechanism. Once this measure is exhausted, the Board may be approached to deal with the grievance.

15. What is the Data Protection Board of India?

The DPDP Act proposes to establish the Data Protection Board of India, an adjudicatory body, to regulate protection of digital personal data in India. The central government shall notify, appoint and establish the Data Protection Board of India. The Board shall be a body corporate with perpetual succession, common seal and with the power to acquire, hold and dispose of movable and immovable property. The Board shall also be able to contract, sue or be sued, depending upon the circumstances.

The Board will be headed by the Chairperson along with as many members as per the notification of the central government for a term of two years, with the eligibility to be reappointed. The Chairperson and other Members shall be persons of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the central government may be useful to the Board, with at least one expert in the field of law.

16. What are the powers of the Board under this law?

The Board has the power to inquire as well as direct urgent remedial or mitigation measures and impose penalty, if necessary:

- On receipt of an intimation of personal data breach
- When complaint is made by a Data Principal in respect of a personal data breach etc.
- Against a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to her personal data
- On receipt of an intimation of breach of any condition of registration of a Consent Manager
- On a reference made by the central government in respect of the breach in observing any directions issued by them.

If a person is aggrieved by an order or direction made by the Board, they may appeal before the Appellate Tribunal, the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within a period of sixty days. The TDSAT shall function digitally and will be digital by design for the receipt of appeals, hearings and the pronouncement of decisions.

The Appellate Tribunal shall be vested with the powers of a civil court.

17. What are the penalties for violation of law under the DPDP Act, 2023?

If the Board concludes in an inquiry that a person has breached the provisions of this Act or the rules made thereunder, after giving the person an opportunity of being heard, it may impose monetary penalty as per the Schedule. The Schedule prescribes various penalties for the violation of specific provisions.

Breach of any other provision of this Act or the rules made thereunder may lead to a penalty extending up to Rs 50 crore.

While the Act has not mentioned any criminal charges for the offenders, cognisable offences leading to serious sensitive data breach or cybercrimes will automatically attract criminal prosecution separately.

COMMON CAUSE EVENTS

Mohd. Aasif and Ashok Kumar*

Police Reforms Day, 2023 --- Mumbai, September 22, 2023

Mr Julio F. Rebeiro speaking at the Nehru Center, Mumbai while other speakers look on

On September 22, 2023, Common Cause joined the Indian Police Foundation (IPF) and Public Concern for Governance Trust (PCGT) to observe the Police Reforms Day, 2023 at a well-attended function that was held at the Hall of Culture, Nehru Centre, Mumbai. Hon'ble Justice Gautam Shirish Patel, a Sitting Judge of the Bombay High Court, was the chief guest of the event which was attended by a large number of serving and retired police officers, media persons, lawyers, intellectuals and law students.

One of the highlights of the day was to confer a Lifetime Achievement Honour on a highly decorated former police officer Julio F. Ribeiro. Alumnus of 1953 IPS batch, Mr Ribeiro, 94, served as Mumbai Commissioner of Police and Director General of CRPF. At the height of the extremism in Punjab, he was given the charge of Director General of Police of the state and he later served as an advisor to the Governor of Punjab.

The main speakers of the day, besides Justice Gautam Shirish Patel and Mr Ribeiro, were Mr Prakash Singh, Patron IPF, Mr M L Kumawat, Acting Chairman IPF, Mr N Ramachandran, President IPF, Dr Vipul Mudgal, Director, Common Cause, and Mr Mihir Desai, Senior Advocate. The citation to honour Mr Rebeiro was read by leading industrialist and philanthropist Mr Deepak Parekh, former Chairman of HDFC.

Speaking on the relationship of Police and Politicians Mr Ribeiro candidly spoke in favour of operational independence of the force without undue interference of the political executive. "It means they should manage their own affairs and not look at the politicians to decide who should be appointed at the police stations and who should be arrested or not arrested", he added.

Justice Patel underlined the significance of the rule of law in his keynote address. He cited the 2006

** Mohd Aasif is a Research Executive at Common Cause and Ashok Kumar is an assistant editor at Inclusive Media for Change (im4change.org)*

Director Common Cause speaking at the Police Reforms Day

judgement of the Supreme Court in Prakash Singh & Ors v. Union of India regarding police reforms and called it a "missed opportunity" with a "narrow approach". "Striving for an impartial and independent police force is a real struggle," he added. Pointing to the impatient behaviour of the general public towards justice, he said, "there is no substitute for this system". He also criticised the Bollywood movies that project police absurdly and added "films like Singham send very harmful message where a hero cop delivers justice single-handedly."

Introducing the police reforms programme of Common Cause to the audience, Dr Mudgal explained the idea behind the Status of Policing in India Reports (SPIRs). He said the civil society is not looking for effective police alone but both effective and accountable police. "We want democratic and people-centric police whose balance is not tilted in favour of the rich and the powerful. Their real obligation, therefore, is not only to control crime and maintain peace but to do so while treating people with dignity and respect" he said.

16th National Conference on Of The Association for Democratic Reforms --- Pune, July 15-16, 2023

The Association for Democratic Reforms (ADR) and the Maharashtra Election Watch (MEW) organised the 16th Annual National Conference at the Gokhale Institute of Politics and Economics (GIPE), Pune, on July 15 and 16, 2023. State Election Watch coordinators from all the states in India participated on the first day of the event, along with members from civil society groups, activists, journalists, retired bureaucrats, judges, advocates, political party representatives, academics and students.

Released at the event were the report on 'Analysis of Sitting MLAs from 28 State Assemblies and 2 Union Territories of India 2023' and the ADR's Annual Report for FY 2022-23. The two-day event started with

Release of the ADR Reports on Crime Records at the ADR National Conference in Pune

a focus on the urgent requirement of addressing the most pressing problems in the electoral and political arena. The first day of the conference consisted of panel discussions on various important issues related to electoral and political reforms like 'The Continuing Trend of Money Power and Criminality in Indian Politics: What is the way forward?', 'Decoding the Controversial Electoral Bonds Scheme: How long for Supreme Court to adjudicate?', 'Bringing Political Parties under RTI: Fostering inner-party democracy', and 'Local and Urban Governance'.

In his keynote address, the former Chief Election Commissioner, Dr Nasim Zaidi, talked about the necessity of clean politics, in view of the rise in criminal records of elected representatives from 22 percent to 43 percent. He also raised concerns about the impact of fake news, hate speech, divisive politics and the role of digital media in exacerbating these. Dr Zaidi lauded the efforts of ADR and National Election Watch (NEW) for their work on electoral and political reforms. He emphasised the need for a constitutional review of the first-past-the-post (FPTP) voting system.

Justice (Retd.) Narendra Chapalgaonkar, former Judge of Bombay High Court spoke on the challenges before Indian democracy and pointed out the role of religion and caste in electoral politics and their implications. Highlighting the issue of the election expenditure, he emphasised on the need for the declaration of wealth before and after elections.

Dr Vipul Mudgal, Director Common Cause and Trustee, ADR and NEW, participated in a panel discussion on decoding the controversial electoral bonds scheme. The discussion was chaired by Prof. Jagdeep Chhokar, founder member and trustee, ADR and NEW. The discussion was focused on institutional paralysis caused by electoral bonds and shed light on the judicial intervention and the continual acceptance of electoral bonds by opposing parties. Common Cause and ADR have challenged the constitutionality of the electoral bonds in a joint PIL. Dr Mudgal also chaired a panel discussion on "Bringing Political Parties under RTI: Fostering Inner-Party Democracy". The discussion was focused on political parties' refusal to come under the purview of RTI, absence of legal oversight or public scrutiny over the function of political parties, and transparency in ticket distribution, among other things.

India Justice Report by Citizens' Forum India --- September 16, 2023

The Citizens' Forum India organised a virtual discussion on India Justice Report (IJR) and invited two of its authors, Radhika Jha of Common Cause and Nayanika Singhal of India Justice Report to speak.

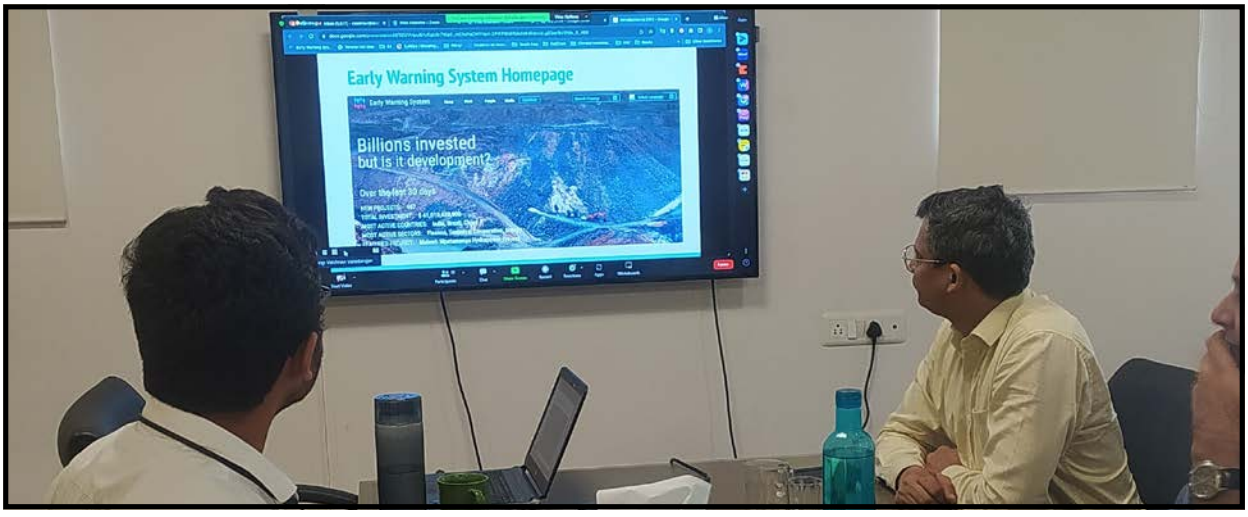
Ms Singhal explained the methodology adopted for the ranking system of the states for the four pillars of the Indian Justice System i.e. the police, judiciary, prisons and legal aid. Explaining the ranking system of IJR, she said that report looked into the representation of SC, ST, OBC and women, expenditure on training, disposal of cases, occupancy of prisons with undertrials and convicts; and accessing justice through the State Human Rights Commissions among other things. While talking about a few findings, she pointed out that money equivalent to six veg burgers is spent annually on legal aid per person.

Ms Radhika Jha elaborated on the role of the police, one of the four pillars of the justice system. She spoke about the expenditure on police training, filling of vacancies, police diversity and other indicators used in the report. "Every state has statutorily mandated quotas for SC, ST and OBC in the police but only Karnataka has been able to fulfil these reserved quotas", she added. Responding to one of the queries on pending cases in the courts, she said, vacancies of the judges and magistrates is one of the major reasons for the pendency of cases.

Meeting with Mineral Inheritors Rights Association (MIRA) --- August 28, 2023

Common Cause team participated in a meeting of the Mineral Inheritors Rights Association (MIRA) on August 28, 2023. The meeting started with a session where various stakeholders from the mining-affected regions raised issues they were facing and MIRA members provided suggestions to deal with their issues. Following this, Vaishnavi Varadarajan of International Accountability Project (IAP) delivered a talk on the Early Warning System (EWS). The EWS is an initiative that ensures local communities and the organisations that support them, to have verified information about projects being proposed at major development finance institutions.

The Early Warning System includes the first web-based tool to organise, summarise and standardise



The Zoom Meeting Underway

projects at 13 development finance institutions. The growing database is updated daily and holds more than 7,000 projects proposed since 2016. While the database itself is an important resource, the EWS team also focuses on outreach for getting this information and extending support to those affected by the proposed project who needed it the most.

Lecture on Indian Legal System and Access to Justice --- August 29, 2023

Radhika Jha, Lead (Rule of Law) at Common Cause was invited to deliver a guest lecture to the law students from the National Law School of India University (NLSIU), Bangalore on Police violence and discrimination in India on August 29, 2023. The lecture focused on findings of the SPIR series that highlighted the systemic biases within the police in India. Simultaneously, the students were introduced to survey methodology as a research tool for studying the Indian criminal justice system. It was part of an elective course titled 'Indian Legal System and Access to Justice'.

Release of SafetyNiti 2023 --- August 11, 2023

Safe in India, an organisation working towards the safety of workers at automobile factories, released its annual report 'SafetyNiti 2023, three years of tracking India's top 10 auto sector brands' OSH Policies for their supply chain: Gaps, Opportunities, Best Practices, Solutions,' on August 11, 2023.

Common Cause team attended the virtual panel discussion on the topic 'Will ESG reporting deliver supply chain sustainability in the auto sector supply chain? Does it measure and report on the real changes on the ground that must follow an improvement in policies on paper?'. Dr Garima Dadhich, Associate Professor, Indian Institute of Corporate Affairs; Mr. Gorakh G Velapurkar, VP (Materials), Bajaj Auto; and Dr Dev Nathan, Professor, Institute for Human Development were on the panel discussion. Sandeep Sachdeva, Co-Founder and CEO, Safe in India moderated the event.

During the event, one of the injured workers associated with Safe in India, Ram Singh Parihar, expressed dismay over the sloppy approach towards the safety. He said, "There is no timely maintenance of machines in our factory. Neither the maintenance staff is available on time. They don't carry out maintenance task even when we inform that the machine is out of order."

The findings of the latest report show that there has been a slow but steady improvement in the brands' occupational safety and health policies since SafetyNiti 2021, with Bajaj and Honda having improved the most on several parameters, while TVS and Ashok Leyland continue to remain at the bottom. As an impact of the past reports, eight of the top 10 auto sector companies have now declared their OSH policies in the public domain, four auto sector companies have their Human Rights policy in the public domain and categorically cover non-permanent workers and/or deeper supply chain and six of them now have Supplier Code of Conduct in the public domain.

WHAT ABOUT ACCOUNTABILITY?

Unfulfilled Expectations from the DPDP Act, 2023

Swapna Jha*

On August 24, 2017 the Supreme Court of India gave a ruling that laid the foundation for the 'Right to Privacy' jurisprudence in the country. In KS Puttaswamy v Union of India the court held that the right to privacy is a fundamental right under Article 21 of the Constitution of India, thus recognising privacy as intrinsic to the right to life and liberty. The ruling of the nine-judge bench set the stage for the enactment of a single-statute legislation by the government for the protection and regulation of personal data.

A Timeline from PDPB to DPB to DPDP

A month before the judgment, the Ministry of Electronics and Information Technology (MeitY) had constituted an expert committee under the chairmanship of Justice B.N. Srikrishna to examine the issues related to data protection. In July 2018, the committee released a 176-page report which, among other things, laid out the first draft of a data protection act. The Personal Data Protection Bill, 2018 (PDPB, 2018) proposed that certain types of compliance were required to be made for the use of all forms of personal data. While broadening the rights given to individuals and proposing data localisation for certain forms of sensitive data, it imposed major financial penalties in case of non-compliance. Further, the Bill suggested the creation of an independent regulatory body called the Data Protection Authority for the enforcement of the legal framework.

The government revised the Srikrishna draft and introduced it in the Lok Sabha as the Personal Data Protection Bill, 2019 (PDPB, 2019). In December of that year the Bill was sent to a Joint Parliamentary Committee (JPC) for review by members of both houses.

The JPC submitted its report in December, 2021, along with a new iteration of the Bill called the Data Protection Bill, 2021 (DPB, 2021). However, in August 2022 the government withdrew the Bill citing the "extensive changes" that the JPC had made to the 2019 Bill. MeitY released yet another version in November - The Digital Personal Data Protection Bill, 2022 (DPDP, 2022) – and sought comments from the public.

In 2023, after years of reiterations and an alphabet soup of shorthand, India finally has its data protection law, the Digital Personal Data Protection Act, 2023 (henceforth the Act), which received the assent of the President on August 12, 2023.

> ***"In KS Puttaswamy v Union of India the court held that the right to privacy is a fundamental right under Article 21 of the Constitution of India, thus recognising privacy as intrinsic to the right to life and liberty.***

Oh, those Exemptions

However, the wide powers given to data fiduciaries need to be critically analysed. Section 7 of the Act allows a fiduciary to process data for "certain legitimate uses". This is the second way through which personal data can be processed, in addition to the "voluntary" provision given by a data principal. A close reading suggests that the said section has narrowed the consent process down to 'certain legitimate uses' which includes the use of personal data for specified purposes, for the state and any of its agencies, as well as for any of the

*Swapna Jha is a Senior Legal Consultant at Common Cause

legitimate uses as specified under Section 17.

Section 17, however, exempts the state and its agencies from some of the provisions in the Act when it comes to processing data. Some exemptions are vague and arbitrary. For instance, "in the interests of sovereignty and integrity of India, security of the state, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognisable offence relating to any of these, and the processing by the central government of any personal data that such instrumentality may furnish to it". Further, "The central government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification."

"A blanket exemption will give unregulated powers to the government, which may adversely affect privacy of citizens and lead to the creation of a "mass surveillance state".

The Act also exempts from its scope the processing of personal data of principals located outside the territory of India by an entity based in India.

Moreover, the government has been given powers to exempt some fiduciaries, including startups, from certain provisions of the Act, based on the volume and nature of the personal data they process. Most arbitrary is the power given to the government to exempt "notified state entities" from the Act entirely in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, and maintenance of public order.

The union and states governments will be among the largest data fiduciaries, since they will be in possession of the personal data of 1.4 billion citizens. The loopholes that grant exemptions to government agencies give the state unfettered power over data without the necessary safeguards in place[1]. Moreover, the legal text outlining the exceptions is vague and broadly framed.

The blanket exemptions instead should have been replaced with exemptions for specific purpose, thus avoiding arbitrariness. A blanket exemption will give unregulated powers to the government, which may adversely affect privacy of citizens and lead to the creation of a "mass surveillance state". While the Act allows the state to override consent from the data principal for the purpose of providing subsidies and benefits, it does not provide for purpose limitation, which is defined as using data only for the specified purpose. This provision would be open to misuse by the state or its agencies. The Act has also, unfortunately, removed the public interest exception to disclosure of personal information under the Right to Information Act, thereby diluting accountability and transparency in the functioning of government officials.

Section 9 of the Act provides protection for children's data, but sub-section 9(4) allows the government to exempt fiduciaries from general restrictions in processing children's personal data, subject to some conditions. Similarly, sub-section 9(5), exempts the need to seek parental consent for processing personal data of specific age groups of children.

Section 37 of the Act allows the government to block public access to certain fiduciaries in consultation with the Data Protection Board. This could potentially enable the government to completely shut down a service provider in India. The board can recommend blocking of access if a platform or internet service provider has been penalised twice, or if it finds that there is the need to protect the "interests of the general public". A moot point, however, is that content blocking, which is becoming almost a norm in India, may not

necessarily be in public interest.

While the basic structure of the law is similar to the European Union's General Data Protection Regime (GDPR), India's approach has the distinction of shielding the biggest fiduciary i.e. the state from data transparency and accountability. The DPDP Act, 2023 has more limited scope for data processing because it grants wide exemptions to government agencies, and hands over regulatory powers to the government. Furthermore, there are no special provisions to process or protect sensitive personal data, and the government has the power to access information from fiduciaries, the board and intermediaries.

The omission of critical elements such as the absence of a definition of "reasonable security safeguards," lack of provisions for compensation indicate the failure by the legislative branch in creating a comprehensive legislation that makes citizens' privacy its cornerstone.

The right to privacy imposes on the state a duty to protect the privacy of an individual. The failure to do so should incur a corresponding liability on the state. The right to life and individual liberty are inalienable to human existence and not a matter of largesse granted by the state. And that is why it is imperative to acknowledge that the right to privacy is a fundamental right. Any violation by the state of this right must pass the test of being fair, just and reasonable under Article 21 and, equally, it must satisfy the test laid down in the *Puttaswamy* judgment. It is here that India's DPDP Act 2023 may fall short of its stated purpose and also may fail to ensure that the state will not infringe on the right to privacy as guaranteed by the Constitution.

European Union's GDPR vis-à-vis DPDPA

The GDPR is a comprehensive data privacy law that sets guidelines for the collection, processing, storage, and transfer of personal data. It is one of the most significant data protection laws in the world and has set the tone for other countries to follow suit. The GDPR applies to all organisations that process personal data of EU citizens, regardless of location. These regulations seek to protect the privacy rights of individuals and ensure that their personal data is processed in a transparent and secure manner. It came into force on May 25, 2018.

Unlike DPDPA, there is no vested right under GDPR to process the data for lawful purposes except for the purpose of protection of rights of natural persons.

The GDPR classifies personal data into two categories:

a. regular personal data and

b. special categories of personal data.

The latter category includes personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, genetic or biometric data processed for the purpose of identification, sex life, and sexual orientation. Special categories of personal data are subject to distinct compliance requirements, especially the legal basis that can be adopted for the processing of such personal data.

On the other hand, the DPDPA applies to a broader set of personal data without further categorising it into sensitive or critical personal data. Given that there is no such classification or further categorisation of personal data, there is no statutory requirement to implement separate compliance standards for different kinds of personal data collected.

The GDPR does not distinguish between classes of data controllers while prescribing compliances and obligations. However, the DPDPA intends to classify certain data fiduciaries as 'significant data fiduciaries' with increased compliance obligations, such as the appointment of a data protection officer responsible for grievance redressal, the appointment of an independent data auditor, conducting Data Protection Impact Assessments and such other compliances as may be prescribed. The classification will be based on factors like the volume and sensitivity of personal data collected, the risk of harm to data principals, the potential impact on India's sovereignty and integrity, etc. Further, the DPDPA empowers the government to notify certain data fiduciaries or class of data fiduciaries to whom compliances will not apply regarding consent obligations, the obligation to ensure accuracy of personal data collected, data retention obligations, enhanced compliances while collecting children's personal data, and the obligation to give effect to data principal's requests in relation to their personal data.

Both the GDPR and the DPDPA recognise consent of individuals as one of the legal bases for processing personal data. However, the DPDPA has introduced the novel concept of 'consent managers'. Consent managers are data fiduciaries who may, on behalf of the data principals, collect and manage consent provided by them. Consent managers will enable data principals to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform. Every consent manager will be required to be registered with the Data Protection Board ('the Board') in such manner and subject to such technical, operational, financial, and other conditions as may be prescribed.

Unlike the GDPR, the DPDPA does not provide the right of data portability in favour of data principals. While such a right was incorporated in the Personal Data Protection Bill, 2019, it has not been incorporated in the final DPDPA.

The DPDPA sets out certain duties for data principals. Pursuant to the same, data principals have been directed to refrain from instituting any false or frivolous complaints or grievances against data fiduciaries. They have also been directed to submit verifiably authentic information. Any non-compliance with these duties will attract imposition of financial penalties. On the other hand, there is no such corresponding provision under the GDPR.

While the GDPR and the DPDPA have a lot in common, the approach and means taken by both legislations are different, as outlined above. The GDPR is, comparatively, more prescriptive whereas the DPDPA appears to tilt the balance in favour of the state and its agencies as it lays down certain fundamental ideas and leaves many implementation-related aspects to subordinate legislations, rules, and regulations to follow.

Endnotes

1 Chandran, R. (2022, January 19). In India's surveillance hotspot, facial recognition taken to court | Context. Context News. Retrieved September 12, 2023, from https://bit.ly/3RVtMrd

Guest Column

SHROUDED IN SECRECY

Dangers in the DPDP Act

Amrita Johri & Anjali Bhardwaj*

The Digital Personal Data Protection (DPDP) Act, 2023 was passed in Parliament in the Monsoon session. The deliberative process around the legislation remained shrouded in secrecy and seemed largely focussed on the concerns of industry. Just prior to the bill being brought to Parliament, opposition members walked out of a meeting of the Parliamentary Standing Committee and submitted dissent notes, objecting to the adoption of a report on the issue of Data Protection — claiming that the proposed bill was neither shown to the members nor formally referred to the committee.

The DPDP Act continues to suffer from the problems pointed out by civil society including the National Campaign for Peoples' Right to Information (NCPRI) in the earlier drafts including weakening of the RTI Act through amendments and lack of independence and autonomy of the oversight body- the Data Protection Board.

Blow To Right To Know And Accountability

The Data Protection Act includes a provision to amend the Right to Information (RTI) Act, which has empowered millions of Indian citizens since its enactment in 2005. To effectively hold their governments accountable in a democracy, people need access to information, including various categories of personal data. For example, the Supreme Court of India has held that citizens have a right to know the names of wilful defaulters and details of the Non-Performing Assets (NPAs) of public sector banks. Democracies routinely ensure public disclosure of voters' lists with names, addresses and other personal data to enable public scrutiny and prevent electoral fraud.

Experience of the use of the RTI Act in India has shown that if people, especially the poor and marginalised, are to have any hope of obtaining the benefits of government schemes and welfare programmes, they must have access to relevant, granular information. For instance, the Public Distribution System (PDS) Control Order recognises the need for putting out the details of ration card holders and records of ration shops in the public domain to enable public scrutiny and social audits of the PDS.

** Amrita Johri and Anjali Bhardwaj are associated with the National Campaign for Peoples' Right to Information (NCPRI) and Satark Nagrik Sangathan (SNS) and Bhardwaj is also a member of Common Cause Governing Council*

The RTI Act includes a provision to harmonise peoples' right to information with their right to privacy through an exemption clause under Section 8(1)(j). Personal information is exempt from disclosure if it has no relationship to any public activity; or has no relationship to any public interest; or if information sought is such that it would cause unwarranted invasion of privacy and the information officer is satisfied that there is no larger public interest that justifies disclosure.

The enactment of a data protection law, therefore, should not require any amendment to the existing RTI law — this is also noted by the Justice AP Shah Report on Privacy. The DPDP Act, however, makes amendments to Section 8(1)(j) to expand its purview and exempt all personal information from disclosure. This threatens the very foundations of the transparency and accountability regime in the country.

Wide Discretion to Government

A primary objective of any data protection law is to curtail the misuse of personal data, including for financial fraud. Given that the government is the biggest data repository, a robust data protection law must not give wide discretionary powers to the government. The DPDP Act, unfortunately, empowers the executive to draft rules and notifications on a vast range of issues. For instance, the central government can exempt any government or even private sector entity from the application of provisions of the law by merely issuing a notification. This potentially allows the government to arbitrarily exempt its cronies and government bodies such as the Unique Identification Authority of India (UIDAI), resulting in immense violations of citizens' privacy. On the other hand, small non-governmental organisations, research organisations, associations of persons and opposition parties, that the government chooses not to include in the notification, would have to set up systems to comply with the stringent obligations of a data fiduciary.

Caged Parrot by Design

Further, to meet its objective of protecting personal data, it is critical that the oversight body set up under a good legislation be adequately independent to act on violations of the law by government entities. The Act does not even make a pretence of ensuring autonomy of the Data Protection Board — the institution responsible for enforcement of provisions of the law. The central government has several powers including appointing the Chairperson and members and deciding the strength of the Board.

The creation of a totally government-controlled Data Protection Board, empowered to impose fines upto Rs.500 crore, is bound to raise serious apprehensions of it becoming another caged parrot — open to misuse by the executive to target the political opposition and those critical of its policies.

The failure to address these concerns in the DPDP Act means the citizens of the country have ended up with a law that empowers the central government while taking away peoples' democratic right to seek information and use it to hold the powerful to account.

PRIVACY, SURVEILLANCE AND THE PUBLIC

Evidence from SPIR 2023

Radhika Jha*

Even as the pros and cons of the Digital Personal Data Protection (DPDP) Act 2023 continue to be debated, some important questions to be asked are—how does the Act tie in with the larger public's awareness, opinions and expectations from the government on the right to privacy? Are these opinions and perceptions of the public founded on informed knowledge about the nuances of these debates? These are some of the issues that this article delves into, using data from the recently published 'Status of Policing in India Report (SPIR) 2023: Surveillance and the Question of Privacy.'

The study, the fifth in the SPIR series of reports on policing in India, is brought out by Common Cause in collaboration with the Lokniti team of the Centre for Study of Developing Societies (CSDS). It includes, among other things, data from a survey of just under 10,000 people across 12 Indian states and UTs.

This article primarily relies on findings from the survey to bring out people's lack of awareness on issues related to the right to privacy, coupled with some disturbing perceptions of the larger public on freedom of speech and right to dissent, to finally argue that the worst-affected when it comes to the violation of privacy are the already-vulnerable groups, particularly in the context of mass surveillance by the government.

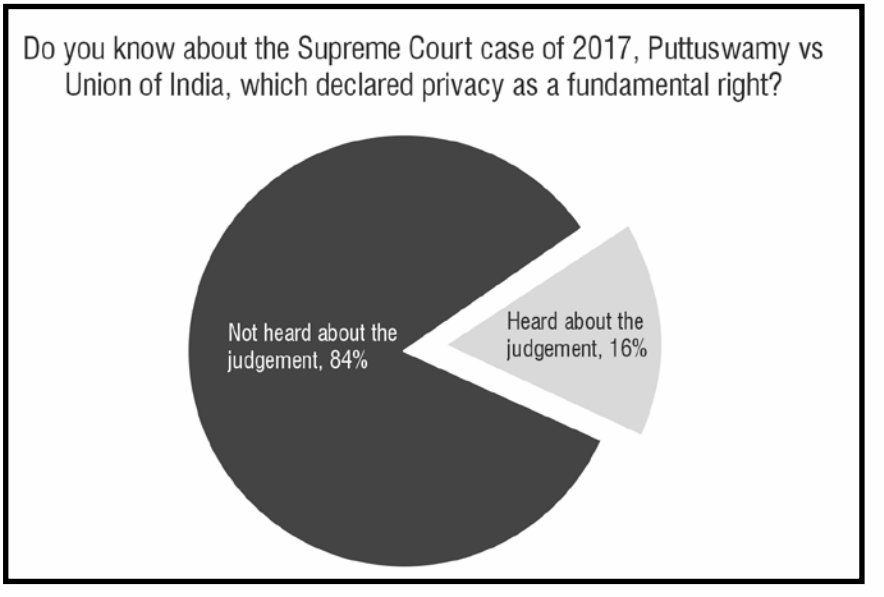
One major criticism of the DPDP Act is regarding the wide exemptions granted to the state and its agencies for data collection and surveillance. Seen in this context, it can be argued that these exemptions can possibly exacerbate state surveillance of already marginalised groups, thus increasing their sense of vulnerability.

People's Awareness Of Issues Related To Privacy

Even with a new legislation in place, the discourse around the right to privacy and data protection appears to have failed to permeate to the granular level of the common Indian person. There is not only a limited vocabulary to both comprehend and formulate the right to privacy at an individual, common person's level on the one hand, but also an extremely limited level of awareness of national, and political debates related to these issues.

This lack of awareness, at least insofar as it relates to some current political events and debates on the

Figure 1: Eighty-four percent of the general public have not heard about the Puttaswamy judgement on the right to privacy

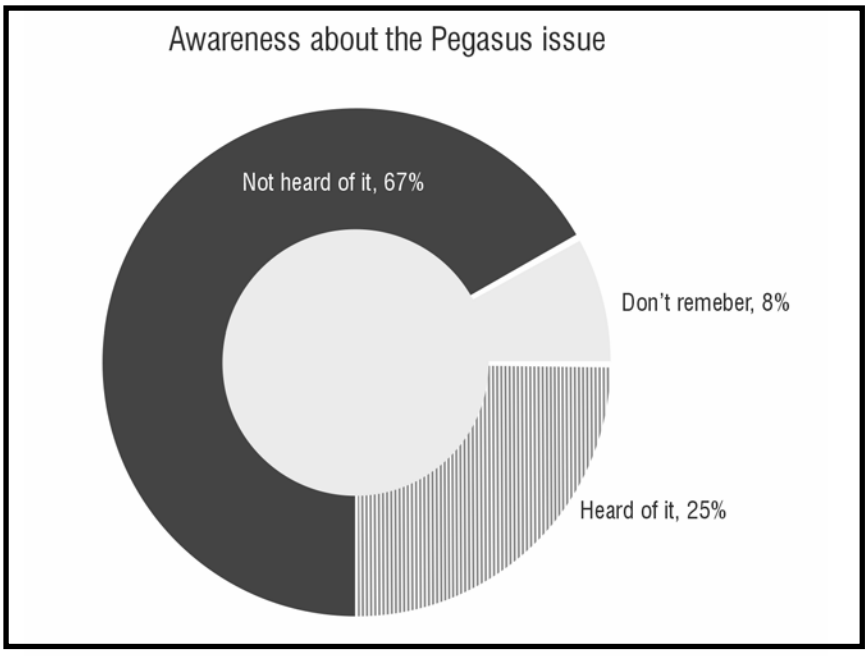


Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy

* *Radhika Jha is Lead Researcher, Status of Policing in India Report (SPIR) series and Project Lead (Rule of Law) at Common Cause.*

right to privacy, is evident from some of the survey findings of SPIR 2023. In 2017, the Supreme Court passed the landmark judgement on the right to privacy, declaring it a fundamental right for the people of India in *Puttaswamy and Anr. v. Union of India and Ors*. However, just a fraction of the 9,779 respondents, 16 percent, were aware of this judgement or had heard of it, while a staggering majority—eighty-four percent – were not aware of it.

Figure 2: More than two out of three people have not heard of the Pegasus issue



Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy

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?"

In July 2021, the International Consortium of Investigative Journalism (Pegasus project) revealed that about 50,000 phone numbers and linked devices across the globe were infected by the Pegasus spyware. It was alleged that several countries, including India, purchased the spyware from an Israeli company, the NSO Group, as part of their defence deals. In India, this spyware was allegedly used to target more than 300 people ranging from serving ministers and judges to journalists, activists and businesspersons (Shekar & Mehta, 2022).

This news, which led to a Supreme Court-appointed enquiry into the matter, created outrage amongst not just the political opposition but also in the media and amongst those advocating for free speech and the right to privacy. In this context, the general public was asked in the survey if they had heard of the Pegasus spyware issue. Again, a large majority—more than two out of three respondents (67%)—had not heard of the Pegasus scandal, while just one-fourth of the respondents (25%) had heard of it.

The low levels of awareness of the general public regarding issues such as the Pegasus scandal or the right to privacy judgment are coupled with dangerous opinions on the extent to which the government should carry out surveillance. While 43 percent of the respondents fully supported the use of such spyware by the government against suspected criminals, another 27 percent also fully supported its use against elected representatives such as MPs and MLAs, while 19 percent fully supported its use against journalists.

Whether or not these disturbing opinions are caused by the lack of awareness around the issue is debatable, but such opinions are completely contrary to the opinions of domain experts, some of whom were interviewed using a Focused Group Discussion (FGD) for the study. A group of 13 key informants, including former police officers, journalists, academics and civil society activists were interviewed using the FGD method. All of the FGD respondents were unanimous in their opinion that surveillance by the state can be used as an excuse to suppress dissent and silent opposition. While some FGD respondents

Table 1: More than a quarter of the respondents fully support the surveillance of MPs/MLAs and other politicians using spywares

Support for the targeted surveillance of the following groups using spywares such as Pegasus (%)				
	Fully support	Support in some cases	Oppose	Don't know
Suspected criminals	43	21	15	21
MP/MLA	27	24	26	23
Other politician	27	25	25	23
Bureaucrat	20	24	32	24
Lawyer	18	23	36	23
Judge	16	24	37	23

Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy

Question asked: "Should the government use Pegasus or similar software for phone hacking, location tracking etc. of these people, even if there is no criminal case against them?

a. Journalist
b. Judge
c. Lawyer
d. MP/MLA
e. Other politicians
f. Suspected criminals
g. Ordinary citizens
h. Businessman
i. Bureaucrat
j. NGO/social worker"

Table 2: Majority of the respondents feel that government surveillance by CCTVs, drones, FRT, etc. to curb protests and political movements is justified

Use of mass surveillance technology by the government to curb protests and political movements					
Type of surveillance technology	Level of support (%)				
	To a great extent	To some extent	Very little	Not at all	Can't say
CCTV cameras	52	25	6	7	10
Drones	30	29	13	12	16
Mobile Surveillance	27	30	15	14	14
FRT	25	26	14	13	22
Voice recognition technique	24	26	16	15	19

Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy

Question asked: "To what extent do you think it's justified for the government to use the following technologies to curb political movements or protests against policies & laws enforced by the government – to a great extent, to some extent, very little or not at all?"

made the distinction between patently illegal activities such as hacking (under which spyware such as Pegasus would fall), and surveillance, they pointed out that targeted surveillance by the state can have a chilling effect on freedom of speech.

Freedom Of Speech And Right To Dissent

Regardless of whether the ignorance and lack of proper public discourse around the issues are directly related to some of the opinions on privacy, surveillance and freedom of speech, the final picture that emerges from people's perceptions is that of support for undemocratic, even illegal forms of surveillance that go against Constitutional values as well

as judicial precedents on these matters. Thus, it may be argued, that there is little critical analysis of the new Act by the larger public, or enquiry into how the Act will play out in people's daily lives and affect various sections of society.

Some of the starkest examples of the support for extreme forms of surveillance, essentially gagging right to protest and freedom of speech, are given here using the survey findings. For instance, large sections feel that government surveillance by CCTVs (52%), drones (30%) and facial recognition technology (FRT- 25%) to curb protests and political movements is justified to a great extent.

Similarly, 61 percent of the respondents support the use of FRT to identify those protesting against the government or its laws/policies. Even as leading international human rights organisations warn against the usage of technology to hinder peaceful protests and target protestors (OHCHR, 25th June 2020), there have been increasing reports of the use of such technologies to identify and target protestors (Reuters, February 17th, 2020). That such acts largely go unquestioned is explained by people's support for such targeting, as revealed through this survey.

Another finding that attests to people's lack of support for freedom of speech is that one out of five people believe that

Table 3: More than 60 percent support the use of FRT to identify protestors

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 crime	39	44	17

Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy

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 little or not at all? (List of circumstances mentioned in the left column of the table)."

Note: The categories "to a great extent" and "to some extent" were clubbed together to make 'support' and 'very little and not at all' were clubbed to make 'against' for a better contrast. All figures are in percentages.

Table 4: One out of five people believe that it is right for the government to monitor people's social media posts

	Government's action is …? (%)			
	Right	Right, but in some cases	Wrong	Can't say
Monitoring what is posted on social media or the internet	21	30	36	13
Tracking online/ phone activities and accessing contents	12	24	50	14
Imposing restrictions on social media content	12	28	45	15
Location tracking	12	28	47	13
Creating social and financial profiles by collecting information from different sources	11	20	52	17
Tracking call histories	10	24	56	10

Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy
Question asked: "Do you think it would be right or wrong for the government to do these things? List of questions is mentioned in the first column of this table."

it is right for the government to monitor people's social media posts, while another 30 percent feel that it is right only in some cases.

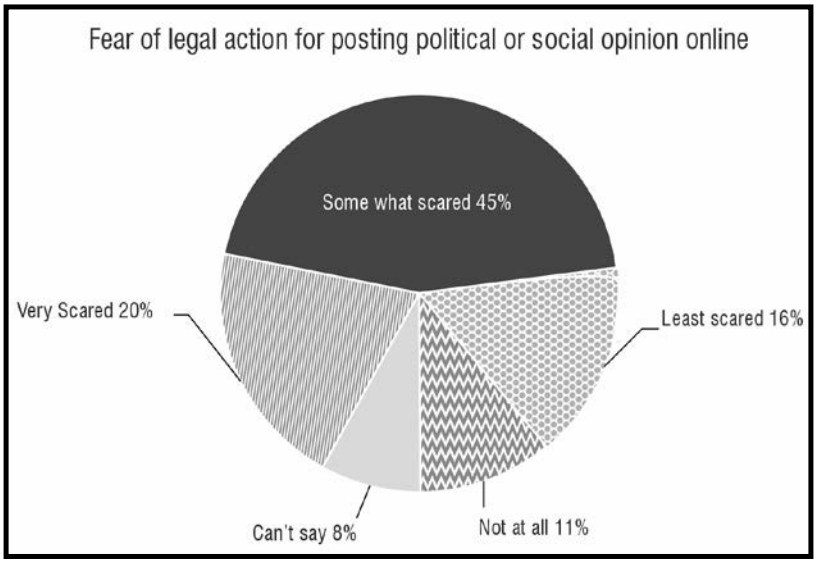
Impact on Vulnerable Groups

Even as the people, at least through their opinions and attitudes, grant license to the government to use surveillance technology to monitor and curb protests and dissenting opinions, they are also simultaneously afraid of voicing their own political and social opinions because of the fear of legal action. While 20 percent of people reported being very scared, another 45 percent were somewhat scared of legal action for posting their political or social opinion online.

Even as a large proportion of the overall population is scared of voicing their political and social opinions online, across these survey questions it emerges that the most vulnerable groups are also those who are most sceptical of state surveillance.

For instance, Adivasis and Muslims, both groups that are majorly over-represented in the undertrial prisoner population, are least likely to support the police collecting biometric details of all suspects. This finding is worrying in the context of the historic over-incarceration of these groups, coupled with the passing of the passing of the Criminal Procedure

Figure 3: Nearly two out of three respondents are scared to post their political or social opinions online for fear of legal action



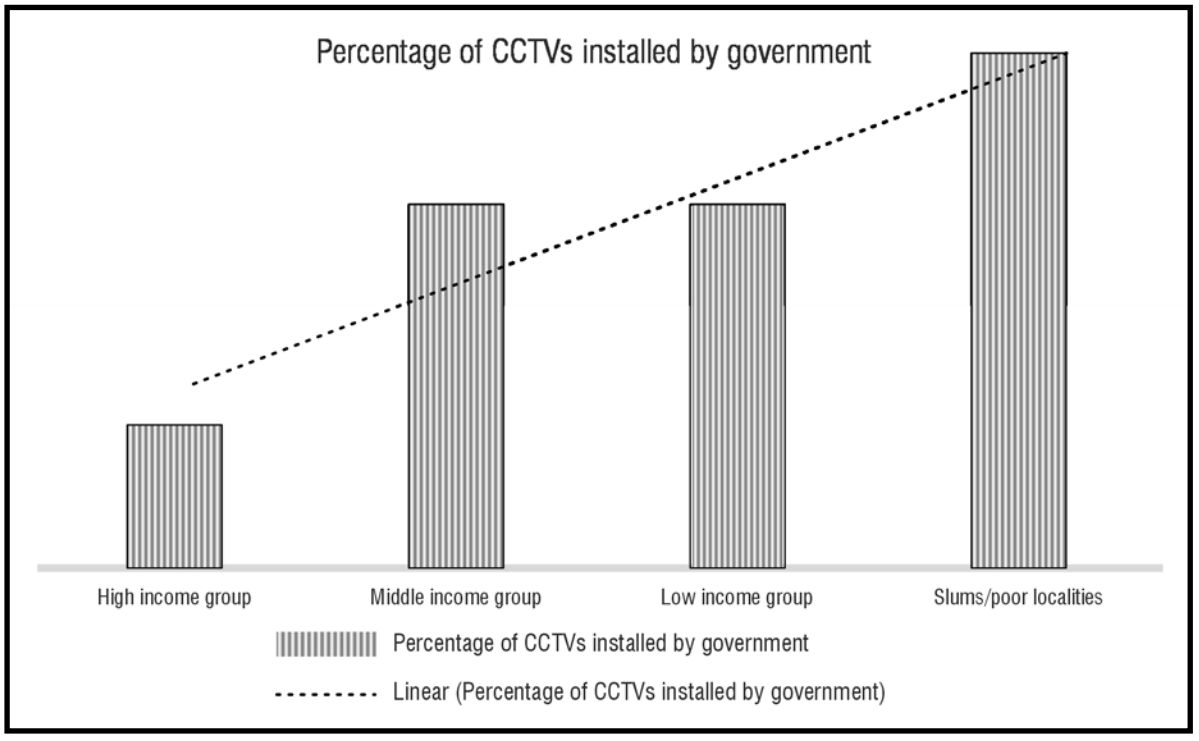
Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy
Question asked: "How scared do you feel that if you post your opinions about a political or social issue on social media, and if it hurts the sentiments of certain groups, there might be legal action against you – very scared, somewhat scared, least scared or not at all scared?"

Table 5: Adivasis and Muslims are the most critical of the police collecting biometric details of all suspects

Caste/religious groups	Police should be able to collect biometric details (%)	
	Support	Against
Dalits	42	34
Adivasis	39	44
Other backward castes	50	31
General	50	28
Hindu	50	30
Muslims	39	32
Christians	44	36
Sikhs	43	34
Other religious minorities	47	32

Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy
Question asked: "Do you think police should be able to collect the biometric details (such as fingerprint, footprint, iris, retina scan, facial recognition, etc.) of all suspects, including those who haven't been declared guilty by the court?"
Note: Rest did not respond.

Figure 4: The government is three times more likely to install CCTV cameras in slums/poor localities, compared to higher-income localities



Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy
Note: All figures are in percentages. Data of only those respondents who reported having CCTV cameras in their households/ residential areas.
Question asked: "Were CCTVs installed by you or some other authority?"

Table 6: Poor least likely to support regular drone surveillance of the public by the police/government

Class	How justified is the usage of drones for regular surveillance by the police and government? (%)	
	Fully Justified	Not at all justified
Poor	39	11
Lower	40	9
Middle	44	9
Rich	50	11

Source: Status of Policing in India Report 2023- Surveillance and the Question of Privacy
Note: All figures are in percentages. Extreme polarities were taken into consideration rather than moderate categories on either side while analysing to give a clear distinction of choices.
Question asked: "In your opinion, to what extent is the use of drones justified for regular surveillance of the public by the government or police?"

(Identification) Act, 2022 which authorises police to collect biometric details of all persons who have been apprehended by them, whether as an accused, convict or otherwise.

Another example of the differential impact on vulnerable sections of society emerges from the finding that although the poorest are least likely to support the installation of CCTV at any location, the government is three times more likely to install CCTV cameras in slums/poor localities, compared to high-income localities.

Similarly, respondents from the poor and lower class are also least likely to support the use of technologies such as drones by the police and government for regular surveillance. While 50 percent of the rich respondents said that the use of drones by the government and police for regular surveillance of the public was fully justified, notably lower 39 and 40 percent of the poor and lower-class respondents respectively agreed.

Conclusion

The above are only some of the findings that point to the differential impact of state surveillance on marginalised groups, and the increased sense of vulnerability amongst these sections of the society. Even as there is a limited understanding of the nuances of surveillance technology, state surveillance and issues related to data protection and the right to privacy, there is an apparent distrust and wariness amongst the already vulnerable groups of such surveillance by the state.

Some of the findings of the latest SPIR provide an insight into why there is little public engagement and debate on not just the new legislation, but issues surrounding the right to privacy and data protection in general. While on the one hand there is a lack of awareness about some of the current political happenings in the context of privacy and surveillance and India, on the other, people in general tend to hold strong opinions supporting the use of surveillance to curb protest and dissent, which often run contrary to democratic values on the freedom of speech and expression. However, when the responses of the public on these issues are sliced across religious, caste and class lines it emerges that it is the marginalised groups who are most critical of such surveillance by the government.

In this context, the exemptions under the Act, which allow the state to collect data under broad conditions, such as security of the state, preservation of public order, prevention of offences and incitement to commit offences, provide wide discretion to the state and can potentially increase the sense of vulnerability and fear amongst the marginalised groups, defeating the purpose of "protection" under the new Data Protection Act.

References

Office of the High Commissioner for Human Rights (OHCHR) (25th June 2020). New Technologies Must Serve, Not Hinder, Right to Peaceful Protest, Bachelet Tells States. Geneva. Retrieved from: https://bit.ly/3rH9bM

Shekar, K., & Mehta, S. (17th February 2022). The State of Surveillance in India: National Security at the Cost of Privacy? Observer Research Foundation. Retrieved from: https://bit.ly/3txdUkR

Siddiqui, Z. & Ulmer, A. (17th February 2020). India's Use of Facial Recognition Tech During Protests Causes Stir. Mumbai/New Delhi, India. Reuters. Retrieved from: https://bit.ly/3ZSLIoq

COMMON CAUSE CASE UPDATES

Supreme Court Cases

Miscellaneous Application (M.A. No. 1756 of 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 Justices BR Gavai and 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 the concerned matters 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. The court concluded the hearing and on May 8, 2023 judgment was reserved.

On July 11, 2023 the SC disposed the batch of writ petitions as well as the MA and ruled that the central government extending the tenure of the director of the Enforcement Directorate (ED) is invalid and directed Sanjay Kumar Mishra, who is presently the director, to vacate the office by July 31, 2023.

The court however upheld the validity of amendments to the Central Vigilance Commission Act conferring power on the central government to extend the tenure of ED director.

Petition Challenging Constitutional Validity of Sedition: Sedition, a colonial law, used to suppress dissent by the British in India, continues to be heavily abused by the law enforcement authorities against citizens for exercising their freedom of speech and expression.

Common Cause filed a petition in 2021, challenging the constitutional validity of sedition under Section 124A of the Indian Penal Code, 1860, as being violative of Articles 14, 19(1)(a), & 21 of the Constitution of India.

In Kedar Nath Singh v State of Bihar, the constitutionality of this section was tested and upheld. The offence of sedition was presumed to be complete if the activities tended to create public disorder or disturbance of law and order or public peace.

In its welcome order on May 11, 2022, the Supreme Court granted interim stay on the use of the provision by governments. It suspended pending criminal trials and court proceedings under Section 124A (sedition) and allowed the Union of India to reconsider the law of the colonial times.

The order stated that the Union of India had agreed with the prima facie opinion expressed by Supreme Court, that the rigors of Section 124A of IPC are not in tune with the current social milieu. Rather, the section was from a time when India was colonised. The Union of India, in its May 9, 2022 affidavit, had agreed to re-examine and re-consider the provision of section 124A of the Indian Penal Code before the Competent Forum. The court adjudicated that it would be appropriate not to continue the usage of the aforesaid provision of law by the government. In addition, it said that the persons accused in fresh cases were free to approach courts for relief, which were asked to examine these cases, considering the present order passed as well as the clear stand taken by the Union of India.

The matter was taken up on May 1, 2023 when the Attorney General for India, stated that, in pursuance of the order dated May 11, 2022, the government has initiated the process of re-examining the provisions of Section 124A of the Indian Penal Code 1860 and the consultations are at a substantially advanced stage. On September 12, 2023 the Supreme Court declined to entertain request of the Attorney General and Solicitor General appearing for the Union of India to defer considering whether a reference should be made to a larger bench, since parliament is in the process of re-enacting the provisions of the penal code and the bill have been placed before a standing committee. The court in its order mentioned, "We are not inclined to accept the request for deferring the consideration of the 5 constitutional challenge in this batch of matters. The provisions of Section 124A of the IPC continue to remain on the statute book. Even if the new law which is proposed to be placed by the government before the legislature results in a modification of the existing provision of Section 124A, there is a presumption that a penal statute would have prospective and not retrospective effect." Existing prosecutions under Section 124A will likely be governed by that provision. Consequently, the validity of the prosecutions which have been launched or would be launched so long as Section 124A continues to remain on the statute would have to be assessed under it. The issue of the validity of the provision for the period that it continues to operate would, therefore, need to be determined. Referring to the judgment in Kedar Nath Singh it was submitted by the petitioners that the observations in that case did not make a distinction between the state which falls within the ambit of Article 19(2) of the Constitution and the government, which does not. At the point in time when the Constitution Bench ruled on the validity of the provision, the challenge on the ground that Section 124A violated Article 19(1) (a) of the Constitution was tested only on the anvil of that article. This must be read in the backdrop of the constitutional position as laid down by this court at the relevant time, which was that a challenge to the validity of a statutory provision on the ground that it violated a specific article in Part III, say Article 19(1)(a), would have to be adjudged on the basis of whether the law was sustainable with reference to Article 19(2) of the Constitution. There was no challenge on the ground that

Section 124A violated Article 14 nor did the Constitution Bench have occasion to consider the validity of the provision against a constitutional challenge on the basis of Article 14. The position as it has evolved in constitutional jurisprudence is that the fundamental rights do not exist *in silos*. There is, in other words, a coalescence of several of the rights protected by Part III. Article 14, which presents an overarching principle of reasonableness permeates Articles 19 and 21 as well. Hence the court directed that the matter be placed before the CJI, who may if so considered appropriate, pass orders for the batch of cases to be heard by a bench of five or more Judges, since the decision in Kedar Nath Singh's case was rendered by a Constitution Bench.

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 BCI prayed for yet further time to complete all his instructions as also to advice appropriately. On April 17, 2023 the Chairman, BCI, informed the court that further process was actively being taken up as regards the framing of rules. He also indicated that in another matter involving akin issues, order has been reserved in another bench. On May 8, 2023, the Chairman BCI submitted that further steps have been taken for amending the rules as submitted before the court on the last few occasions and in that regard, meeting of the representatives of all the state bar councils have also taken place. The court took note of the submission that pursuant to the decision taken in these meetings, the BCI is actively considering the necessary amendment to the rules. The matter was listed on July 17, 2023.

Illegal Mining in Odisha: On July 10, 2023, a bench comprising of the Chief Justice and Justice Pamidighantam Sri Narasimha directed IA No. 42571 of 2023 to be listed on August 11, 2023.

On August 14, 2023, the three-judge bench of Chief Justice with Justices J.B. Pardiwala and Manoj Misra heard the matter. Earlier, on May 1, 2023, the bench comprising of Justice KM Joseph and Justice BV Nagarathna heard the counsel for the state of Odisha in this matter. The state had filed an IA to rectify errors in the previous submissions. The IA for rectification provided that of the total amount of compensation, i.e., Rs. 3308.05 crore, only a sum of Rs. 305.32 crore, have been recovered from the defaulters. Although the court allowed the IA for rectification, they also asked the state to indicate reasons for delay in recovery and to present steps taken for speedy recovery of the amount.

Answering the court, Mr Rakesh Dwivedi, senior counsel appearing on behalf of the state of Odisha made the following statements:

(i) At present, an amount of Rs 2,622 crores, excluding interest, is due and outstanding on account of illegal mining, out of which an amount of Rs 2,215 crores is recoverable from five lessees;

(ii) The leases of the defaulters have either expired or, as the case may be, have been terminated and they are not operating any lease or allowed to participate in tenders; and

(iii) Proceedings for termination of the leases are pending against some of the defaulters who shall have small some amounts comparatively due and outstanding.

The bench issued the following directions:

(a) The state government shall take expeditious steps to pursue the recovery proceedings in accordance with law and shall take necessary steps by attaching the assets of the defaulting entities; and

(b) Hereafter, the terms and conditions of tender shall expressly clarify that no tender shall be entertained at the behest of an entity against which outstandings are due or companies in which the same promoters are interested.

During the hearing, Mr Bhushan highlighted that there is a need to impose a cap on mining in the state of Odisha and presented the states of Karnataka and Goa as examples. The records indicate that yearly mining permissions cover 58 leases with permissible excavation to the extent of 227.13 million tonnes. Mr Bhushan's note has provided that considering the total reserves are 4748.52 million tonnes, the reserves would come to an end within twenty years.

In this regard, the state of Odisha countered that the estimate of iron ore reserves on the geologically explored strata at present is 9220 million tonnes and there is a likelihood of this increasing in future.

Ms Aishwarya Bhati, Additional Solicitor General on behalf of the union of India stated that the union of India shall consider the position and file its affidavit within eight weeks. They will be examining the states of Karnataka and Goa to identify whether a cap on mining is necessitated in the case of state of Odisha.

The amicus curiae, Mr A D N Rao opined that the Central Empowered Committee (CEC) may be tasked with submitting recommendations on the capping of mining. The CEC has functioned as a fact-finding body in this case and provided its report to the Supreme Court. The court shall also examine this after union of India's response is filed.

The next listing of the application is on October 20, 2023.

Petition to Restrain the use of Public Funds for Political Campaigning through Government Advertisements: Presently, the matter is pending before the Registrar H. Shashidhara Shetty. Previously, on September 26, 2022, Justice DY Chandrachud and Justice Hima Kohli heard the petition to restrain the use of public funds for political campaigning through advertisements and issued notice to the respondents. As the service has been completed, the Registrar recorded the activities with respect to the filings of various respondents on August 10, 2023 and on July 7, 2023:

1. The states of Arunachal Pradesh, Himachal Pradesh, Rajasthan and Sikkim have submitted the counter affidavit.

2. Union of India and the states of Chhattisgarh, Goa, Karnataka, Nagaland, Uttarakhand and West Bengal were granted four weeks as final opportunity for filing the counter affidavit.

3. The representatives of the states of Haryana and Meghalaya had requested more time for filing vakalatnama and counter affidavit and were given four weeks as final opportunity.

4. Rest of the respondents (Andhra Pradesh, Assam, Bihar, Gujarat, Jharkhand, Kerala, Manipur, Mizoram, Odisha, Punjab, Tamil Nadu, Telangana, Tripura, Uttar Pradesh and Jammu & Kashmir) have not entered appearance

Common Cause filed a petition to restrain the unnecessary use of public funds on government advertisements in ways that are completely malafide and arbitrary and amount to breach of trust, abuse of office, violation of the directions/guidelines issued by this court and violation of fundamental rights of citizens. Noticing the unnecessary expenditure on advertising campaigns outside the territory of their respective states with no benefit to the target audience or prime beneficiaries of that government's achievements, policies and welfare measures, six specific issues were pointed out in the petition:

- Publication of advertisements by state governments outside the territorial limits of their respective states
- Publication of government advertisements in the form of 'advertorials'
- Publication of government advertisements during/prior to the elections
- Issues concerning the 'Committee on Content Regulation of Government Advertisements' (CCRGA)
- Publication of photographs of functionaries on government advertisements
- Advertisements in the name of awareness campaigns

The Supreme Court in its judgment dated 13-05-2015 in Common Cause v Union of India (2015) 7 SCC 1, had issued several guidelines aimed at regulating government advertisements in order to check the misuse of public funds by central and state governments. The five principles of those guidelines were as follows:

1. Advertising campaigns are to be related to government responsibilities,

2. Materials should be presented in an objective, fair and accessible manner and designed to meet objectives of the campaign,

3. Not directed at promoting political interests of a Party,

4. Campaigns must be justified and undertaken in an efficient and cost-effective manner; and

5. Advertisements must comply with legal requirements and financial regulations and procedures

The objectives behind rolling out these guidelines, as pointed out in the judgment dated 13-05-2015, were as follows:

a. To prevent arbitrary use of public funds for advertising by public authorities to project particular personalities, parties or governments without any attendant public interest

b. Neither to belittle the need nor to deny the authority of the union and state governments and its agencies to disseminate information necessary for public to know on the policies and programmes of government but only to exclude the possibility of any misuse of public funds on advertisement campaigns in order to gain political mileage by the political establishment;

c. To address the gap in the existing DAVP Guidelines which only deal with the eligibility and empanelment of newspapers/journals or other media, their rates of payment, and such like matters and not on how to regulate the content of government advertisements;

d. To ensure that "all government activities satisfy the test of reasonableness and public interest, particularly while dealing with public funds and property";

e. To ensure that government messaging is well co-ordinated, effectively managed in the best democratic traditions and is responsive to the diverse information needs of the public.

Notice was issued on September 26, 2022, by Justice DY Chandrachud and Justice Hima Kohli. On August 10, 2023 the respondents were given four weeks' time to file their counter affidavits. During the record of proceedings on September 21, 2023, the court of the Registrar declined the opportunity to the respondent states who had failed to file the counters and directed the matter to be listed on November 6, 2023.

Petition Challenging the Appointment of Interim Director, CBI: Common Cause had filed a PIL on March 2, 2021, challenging the appointment of an interim/acting CBI director. It also sought the appointment of a regular director, as per procedure established by law. As per the Delhi Special Police Establishment (DSPE) Act, 1946, the appointment of director, CBI is to be made by the High-Powered Committee comprising the Prime Minister, Chief Justice of India (or any judge of Supreme Court nominated by the CJI) and leader of opposition in the Lok Sabha.

The petition prayed for a direction to the executive to initiate the process of selecting a regular director forthwith. The petition also sought a direction to the centre to initiate and complete the process of selection of the CBI director well in advance. The selection process should be completed well before the date on which the vacancy to the post is about to occur.

Previously, in another petition in 2019, Common Cause had challenged the appointment of M Nageshwar Rao as interim director, CBI on similar grounds. On February 19, 2019, while declaring the decision of the case, the court indicated that if due process is not followed in appointments, it is always open to any incumbency and the said appointments could be questioned in accordance with the law.

After holding a few hearings in 2021, where the court expressed its displeasure on the interim appointment, the appointments committee of the cabinet, based on the panel recommended by the High Powered Committee, approved the appointment of Subodh Kumar Jaiswal as the new director of CBI on May 25, 2021. On October 20, 2021, the court asked the government to continue with the incumbent director till next director was appointed in accordance with the provisions of the law in force. On November 14, 2021, an ordinance extending the tenure of the director CBI by up to five years from a fixed tenure of two years was brought in force.

The matter was disposed on August 7, 2023 when Justices Sanjiv Khanna and SVN Bhatti held that:

"In view of the fact that the substantive prayer made in the writ petition has become infructuous, we are not inclined to continue further with the present writ petition and hence, the same is disposed of. However, it will be open to the petitioner(s) to file a fresh petition in case of a change in circumstances or need arising with regard to other prayers made in the present writ petition."

As per news reports, the Union government is mulling over the idea of creating a new post of chief investigation officer of India (CIO) to whom will report the chiefs of the Central Bureau of Investigation (CBI) and Enforcement Directorate (ED).

Petition Seeking Cancellation of the Entire Allocation of Coal Blocks to Private Companies between 1993 - 2012 and a Court Monitored Investigation of the said Allocation: On July 24, 2023, the Chief Justice, Justice JB Pardiwala and Justice Manoj Misra heard and allowed transfer of the seven investigating officers of ED in the normal course and disposed of the concerned IA. On August 14, 2023, the three-judge bench of Chief Justice, Justice JB Pardiwala and Justice Manoj Misra heard the matter. The CBI placed on the record a "Note on Administrative Issues" indicating the present status of the investigation and prosecution in the coal block allocation cases. Pursuing this, permission was granted to relieve certain officials from their present charge. Previously, the Supreme Court had said that that no officials who were investigating the coal block allocation cases could be moved out without its prior permission. The matter is likely to be listed on October 17, 2023.

FUNDAMENTAL RIGHTS AND DUTIES

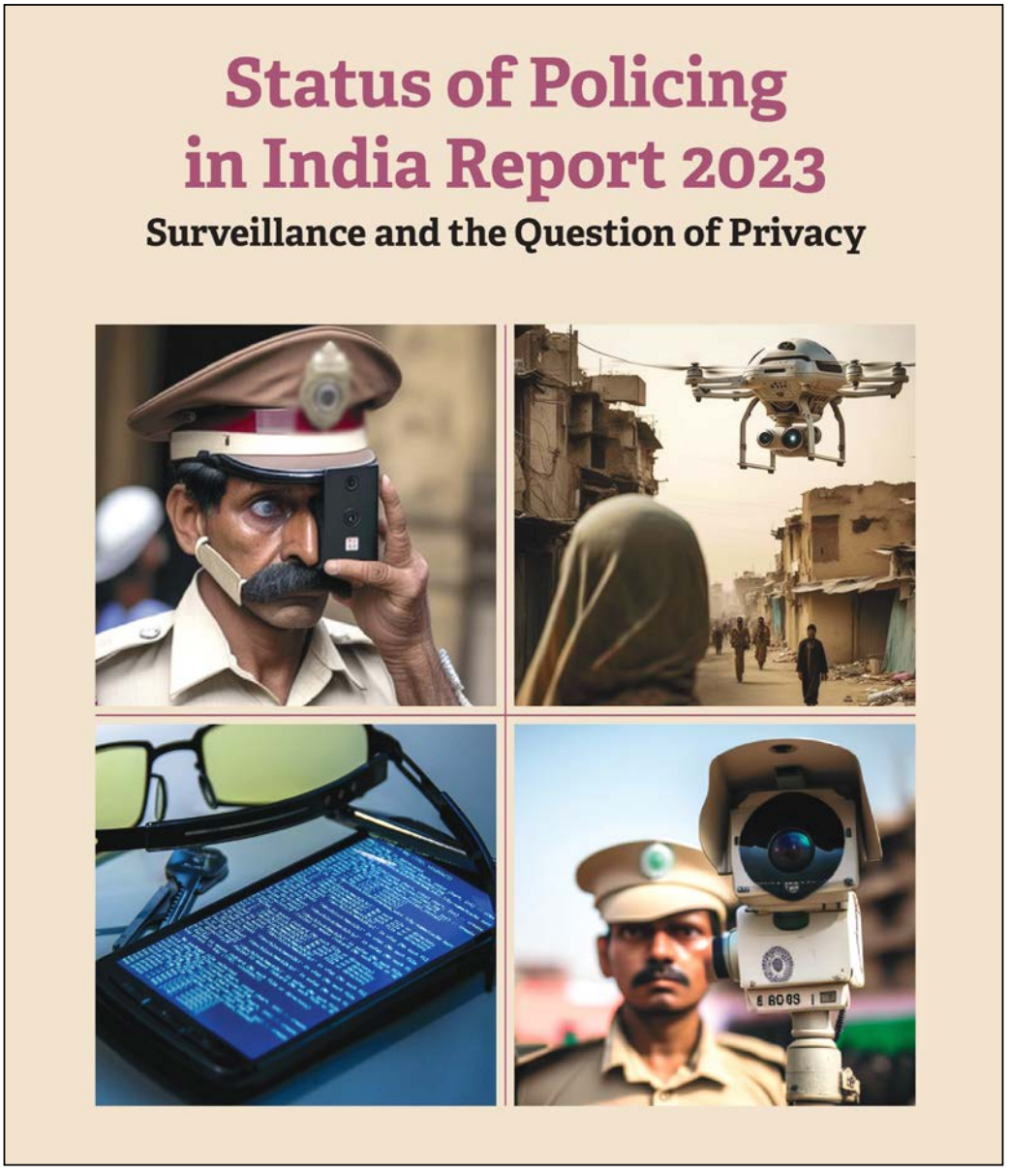
Rights beget empowerment for citizens. They enable them to participate in public affairs and to lead a life of dignity. Rights are also the bedrock of the citizens' legitimate entitlements from the State, their freedom and personhood. Every great nation is defined by the rights of their citizens. In 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;

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

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