SAVE OUR PRIVACY

Indian Privacy Code 2018: Summary

This code is an output of the public initiative #SaveOurPrivacy, which aims to put forth a model draft law on privacy, data protection, interception and surveillance. The initiative intends to generate awareness, knowledge and discussion on these issues, to ensure that India gets a data protection law that protects the fundamental Right to Privacy of an individual.

With the rising number of debates on Aadhar, Cambridge Analytica and the Right to Privacy in recent Parliamentary sessions and heightened global awareness about privacy and data protection - the need for a user rights focused data protection law has reached its crescendo.

To endorse this public initiative, citizens can pledge their support for the Code and/or add their own comments and feedback to the Code.

An effort has been made to propose a law which is comprehensive and will ensure complete protection of an individual's data. It finds its core values in 7 key principles, that were developed after rigour, debate and adapting the best global practices to India. What follows is an explanation of the provisions of the Code, through the lens of the key principles it is based upon.

Key Principles

Individual Rights are at the Centre of Privacy and Data Protection

The law on privacy must empower an individual and advance their right to privacy, as an individual and her rights are primary. The Code furthers this principle in the following ways:

- The Code builds on the basis that privacy is a fundamental right and that personal data should be handled fairly and lawfully.
- It looks at innovation from the perspective of user trust where it will grow in a sustainable manner by creating frameworks for data collectors and processors to handle resident's data.
- The Code provides individuals with certain Rights with respect to their Data:
    - Right to Access - An individual has the right to access information on what data of theirs has been collected, and how it has been handled.
    - Right to Rectification - Individuals can correct and change data collected about them.
    - Right to Erasure And Destruction of Personal Data - Individuals can request their personal data to be erased at any time.
    - Right to Restriction Of Processing - An individual can stop their data from being processed further.
    - Right to Object - Individuals can object to the processing of their data in a particular way.
    - Right to Portability of Personal Data - Individuals can ask to receive their personal data or for it to be transferred to another data collector.
    - Right to Seek Exemption from Automated Decision-Making - Individuals can opt-out from machine made decisions taken based on their data, like profiling.
- If an individual's privacy is compromised and if this Act, which protects privacy is not adhered to, the offender is

liable to face punitive action taken by Privacy Commissions and Surveillance Tribunals created through this Act. These penalties can go up to fines of ₹10 crore and a five year jail term - for committing a cognizable and non-bailable offence.

Icons made by Gregor Cresnar from www.flaticon.com

A Data Privacy Law must be Based on Privacy Principles

User rights as identified by the report of the Justice A.P. Shah Committee of Experts are essential to a data protection law. To protect user rights and in keeping with global data protection best practices, the following provisions have been made in the Code:

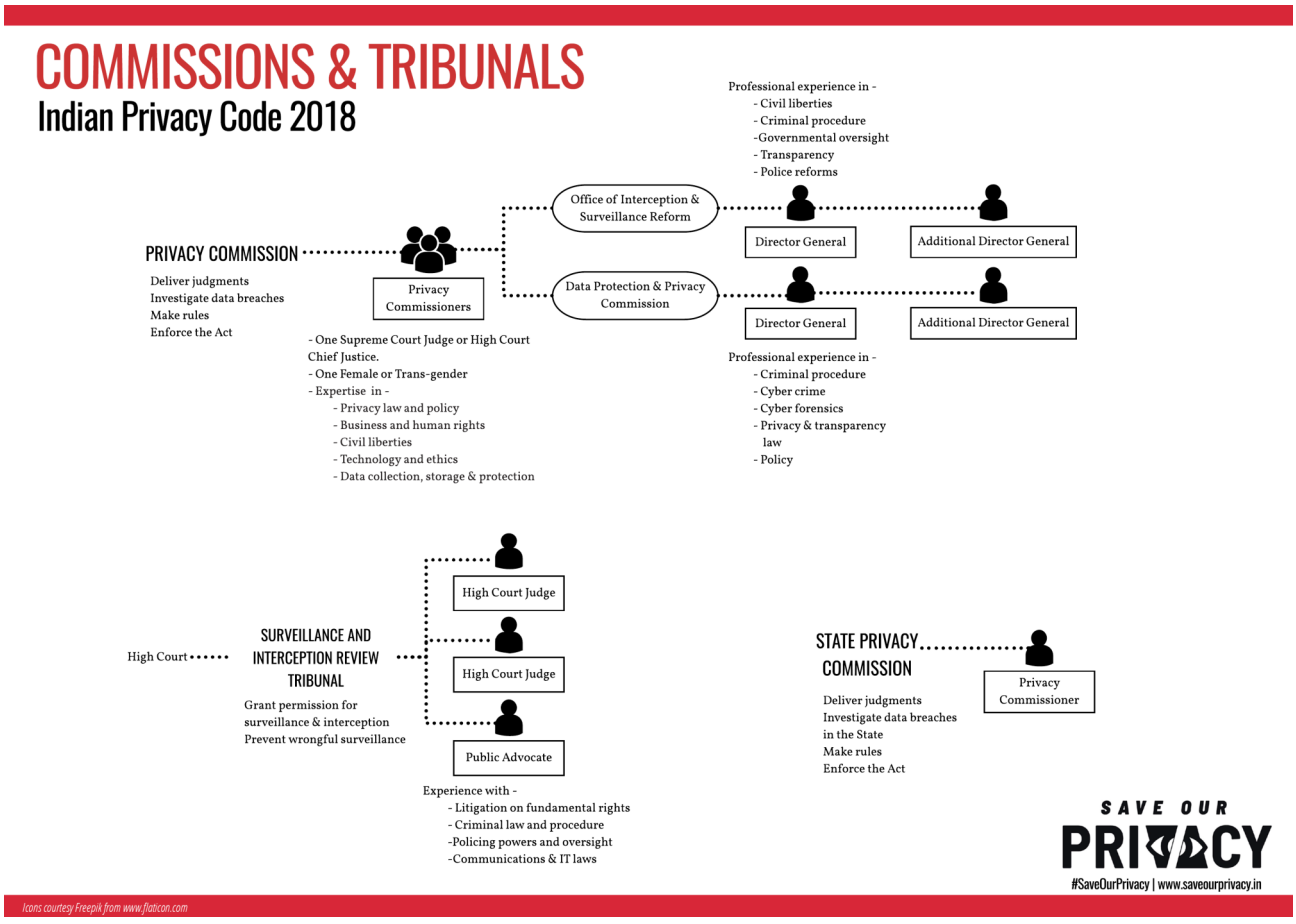
- No individual's data can be collected without intelligible consent and without providing free of cost information on:
  - When the data will be collected.
  - The purpose of collection.
  - It's use.
  - Who it will be shared with.
  - How long it will be stored for and the practices and privacy policies that will protect it.
  - The procedure that will be used to destroy the data and the safeguards available to the citizen.
- Only providers of emergency medical services can use an individual's data without consent, to provide this medical service. Exceptions to the consent rule cannot become the rule.
- All data collected prior to this Code coming into force, will be destroyed within 2 years if consent as mandated by this Code is not obtained.
- An individual's data can only be used to fulfill the purpose it has been shared for. After fulfilling this purpose, an individual's data must be destroyed or anonymized.

- Sensitive data like biometric data, DNA data, sexual preferences, medical history and health information, political affiliation, financial/ credit data and membership of political, cultural, social organisations, can't be collected or disclosed without consent or kept for longer than necessary.

A Strong Privacy Commission Must be Created to Enforce the Privacy Principles

To ensure that the data protection rights provided are kept intact, the Code provides for the formation of a Privacy Commission, which will uphold the rights of users and make regulations, to keep this Code current and timely with the evolution of technology. The key provisions of the Privacy Commission are:

- The Privacy Commission is an autonomous body that can protect an individual's privacy by delivering judgements and investigating data and privacy breaches.
- Its powers will be the same as those conferred upon a Civil Court. The Commission can levy fines and carry out punitive action, to ensure the effective implementation of this Act.
- The Commission can create new rules and regulations for data protection, after consulting with experts and the general public.
- There will be a Central Privacy Commission and a Privacy Commission for each State. While the Central Privacy Commission will deal with disputes between two State Privacy Commissions, and cross border data flows, the State Privacy Commission will take action on complaints of misuse of data within the State.
- The functioning of the Privacy Commission will be reviewed by an ad-hoc committee of Parliament.



The Government Should Respect User Privacy

As the body with the most power and information on the people of India, the Government must protect an individual's privacy. To this extent, the Code provides:

- Essential services like Public Distribution System entitlements, provision of medical care, social security benefits, employment under MNREGA or any other service provided by the Government, cannot be denied if an individual does not consent to the use of their data for identification, or to avail the service and the service provider will at all

times accept any alternate ID.
- Any individual who is denied a service is entitled to damages. If an alternate means of identification is available, and services are still denied - then an individual will receive exemplary damages.
- The Code calls for an absolute bar on mass surveillance by an organisation or Government, since mass surveillance is not necessary to ensure the distribution of welfare schemes or the maintaining public order and security of the state.

A Complete Privacy Code Comes With Surveillance Reform

Indiscriminate surveillance and interception requires to obey the rule of law. To prevent and regulate surveillance and interception, the Code suggests:

- No private entity can engage in surveillance, beyond surveillance of their own property.
- The Code provides for the creation of a Surveillance and Interception Review Tribunal. This tribunal will comprise of 2 or more sitting High Court Judges of each State. This Tribunal will also appoint a public advocate to represent individuals who have been wrongfully surveilled or intercepted.
- After this Code is enacted, irrespective of any other law in force, no surveillance or interception can be conducted by an authority without the written permission of the Surveillance and Interception Review Tribunal.
- Any surveillance conducted without permission will not be considered as evidence in a Court of law.
- No order for surveillance or interception will be valid for more than 60 days (but can be extended if circumstances require), all data collected during surveillance must be deleted 180 days after the surveillance expires, until and unless it is required to be used as evidence in a court of law or presents a threat to the country.
- An individual will be informed of surveillance conducted against them, if the Authorities cannot prove to the Tribunal why this information should not be shared after surveillance is completed.

The Right To Information Needs to be Strengthened and Protected

The protection of an individual's privacy is in no way a conflict with the Right To Information Act, which brings accountability in Government functioning. Privacy protections which already exist under the Right to Information Act need to be preserved. The Code makes the following safeguards for the Right to Information:

- The right to privacy shall not be used to restrain the provisions of the Right to Information Act.
- The proceedings of selection committees for State and Central Privacy Commissions will be disclosed widely under the mandate of proactive disclosure of the Right to Information Act.
- Nothing in the Indian Privacy Code can override provisions of the Right to Information Act.

International Protections and Harmonisation to Protect the Open Internet Use Must Be Incorporated

This Code in no way seeks to prevent the usage of the internet by but seeks to draw a balance to protect users in India whose data is gathered by many global platforms who target services in India. While seeking to preserve the global character of the internet it also looks to ensure data security for Indian users. To this effect, this Code puts forth the following provisions:

- Data can be transferred outside India, if the Central Government and Central Privacy Commission decide that the outside country where data is being collected or stored has adequate data protection norms to meet Indian standards.

SAVE OUR PRIVACY

www.saveourprivacy.in | #SaveOurPrivacy | contact@saveourprivacy.in