Privacy in India: Overview

by Supratim Chakraborty, Khaitan & Co., with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 22-Dec-2020 | India

A Q&A guide to privacy in India.

The Q&A guide gives a high-level overview of privacy rules and principles, including what national laws regulate the right to respect for private and family life and freedom of expression, to whom the rules apply, and what privacy rights are granted and imposed. It also covers the jurisdictional scope of the privacy law rules and the remedies available to redress infringement.

To compare answers across multiple jurisdictions, visit the Privacy Country Q&A tool.

Legislation

1. What national laws (if any) regulate the right to respect for private and family life and freedom of expression?

The Constitution of India (Constitution) protects the life and personal liberty of persons in India (Article 21, Constitution). Indian courts have recognized that the right to privacy is part of the right to life and personal liberty, and in 2017, the Supreme Court of India recognized the right to privacy as a fundamental right under the Constitution (*Justice K.S.Puttaswamy (Retd.) v Union of India* [Writ Petition No. 494/ 2012]). The Supreme Court of India concluded in its decision that "privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone."

The Constitution guarantees citizens the fundamental right to free expression. This right is not absolute and is subject to certain reasonable restrictions, including in relation to:

- The sovereignty and integrity of India.
- The security of the state.
- Friendly relations with foreign states.
- Public order.
- Decency or morality.

- Contempt of court, defamation, or incitement to an offense.

(Article 19, Constitution.)

Presently, Indian laws relating to data privacy and data protection are still evolving. Although there is no dedicated legislation in India addressing data privacy and data protection on a sector neutral basis, the Information Technology Act 2000 as amended (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Act Rules) implementing the IT Act are the primary Indian legal authorities that address these issues in a focused manner.

However, India's government is actively considering adoption of a new, comprehensive data protection law that would significantly change its privacy framework (see Lok Sabha: Personal Data Protection Bill, 2019 (No. 373 of 2019) (introduced November 12, 2019)). For more on legislative developments, see Lok Sabha: Bills Pending.

Various sectoral laws also impose confidentiality obligations or limit personal data transfers, including laws governing banking, telecommunications, healthcare, and securities.

For more on these laws, see Country Q&A, Data Protection in India: Overview.

2. Who can commence proceedings to protect privacy?

Under the Constitution of India (Constitution), any person may assert claims based on harm caused by a breach of fundamental rights to life and personal liberty and free expression, which includes the right to privacy. In the public interest litigation context, any person whose fundamental rights have been violated may petition the Supreme Court of India or other High Courts. For these purposes, standing is not limited to the aggrieved person (*Bodhisattwa Gautam v Subhra Chakraborty* [1995] ICHRL 69). Additionally, the Court can itself take notice of the matter and proceed *suo motu*.

Fundamental rights such as the right to life and personal liberty enshrined under the Constitution are enforceable against both:

- The State and its instrumentalities.
- Private parties performing state functions.

(*Federal Bank Ltd. V Sagar Thomas*, AIR 2003 SC 4325 (interpreting "other authorities within the territory of India" under Article 12 to include private parties); see also *Consumer Education & Research Centre v Union of India*, [1995] AIR 922 ("in an appropriate case, the Court would give appropriate directions to the employer, be it the State or its undertaking or private employer to make the right to life meaningful").)

To determine whether an entity is discharging a state function, the claimant must establish that both:

- The entity performed the function to achieve some collective benefit for the public or a portion of the public.

- The public accepts that the entity has the authority to perform the function.

The Information Technology Act 2000 as amended (IT Act) allows individuals to sue an organization for damages caused by its negligence in implementing and maintaining "reasonable security practices and procedures" to secure sensitive personal data or information (Section 43-A, (IT Act)). The IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Act Rules) define sensitive personal data or information as personal information relating to:

- Passwords.
- Financial information, such as bank account or credit card details or other payment details.
- Physical, physiological, and mental health condition.
- Sexual orientation.
- Medical records and history.
- Biometric information.

(Rule 3, IT Act Rules.)

Sensitive personal data or information does not include information that is:

- Freely available.
- Publicly accessible.
- Furnished under the Right to Information Act 2005 or other applicable law.

3. What privacy rights are granted and imposed?

The Constitution of India provides the right to:

- Privacy in their life and personal liberty to all persons (Article 21, Constitution).
- Free expression to all citizens (Article 19, Constitution).

The Information Technology Act 2000 as amended (IT Act) provides broader protection for certain wrongful personal information disclosures under its enforcement provision, which applies to all personal information (Section 72-A, IT Act). Although Section 72-A of the IT Act does not provide a definition of personal information, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Act Rules) has defined it as any information that relates to a natural person which, either

directly or indirectly, in combination with other information available or likely to be available to a body corporate, is capable of identifying such a person (Rule 2(i), IT Act Rules).

Under the enforcement provision, any person or organization, including an intermediary, who wrongfully discloses personal information, without consent, in violation of the terms of service contract or intending, or knowing that it is likely, to cause harm, shall be imprisoned for up to three years, fined INR500,000, or both (Section 72-A, IT Act).

The IT Act grants individuals certain privacy rights in personal data and sensitive personal data or information. While the IT Act provisions governing personal data are fairly general, the IT ACT provisions and IT Act Rules governing sensitive personal data or information are more stringent and set out granular requirements, including requiring covered organizations to use reasonable security practices and procedures to protect individuals' sensitive personal data or information from unauthorized disclosure, disclosure in breach of contract, or negligence (Rule 3, IT Act Rules.)

4. What is the jurisdictional scope of the privacy law rules?

The Information Technology Act 2000 as amended (IT Act) applies to any person or organization in or outside of India that commits an offense or contravention if the computer, computer system, or computer network involved in the offense or contravention is located in India (Sections 1(2) and 75, IT Act).

Any organization that processes within India the personal data of individuals located outside India is not covered by the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Act Rules) impose restrictions on transferring sensitive personal data or information outside India. To learn more about India's cross-border transfer requirements, see Country Q&A, Data Protection in India: Overview: 20. What rules regulate the transfer of data outside your jurisdiction?

5. What remedies are available to redress the infringement of those privacy rights?

Any Indian citizen may petition the Supreme Court or other high courts in the case of a breach of a fundamental right under the Constitution of India (Constitution) through a writ or public interest litigation (see *Bodhisattwa Gautam v Subhra Chakraborty* [1995] ICHRL 69). Petitioners can file appropriate proceedings with the Supreme Court of India to enforce rights, issue directions, or order a writ, including a writ that:

- Commands the authorities to produce an imprisoned individual and show a valid reason for detention (known as *habeas corpus*).
- Commands a court or government entity to take some action (known as *mandamus*).

- Requires a person or government entity to stop doing something (known as *prohibition*).
- Commands a person or government entity to show by what authority they are exercising some right or power, including but not limited to holding a public office (known as *quo warranto*).
- Requires judicial review of a judicial or administrative decision (known as *certiorari*).

Organizations or persons that violate the Information Technology Act 2000 as amended (IT Act) face the following penalties:

- Damages to compensate an affected individual for an organization's negligence in implementing and maintaining "reasonable security practices and procedures" to secure sensitive personal data or information (Section 43-A, IT Act). There is no damages cap and damages are determined on a case-by-case basis. To recover damages above INR 50 million, a claimant must file a complaint with a competent civil court. Damages below that amount may be decided by an Adjudicating Officer designated under the IT Act.
- Imprisonment for not more than three years, a INR500,000 fine, or both, for disclosing a person's personal information without their consent and in breach of the terms of service contract intending, or knowing that it is likely, to cause harm (Section 72-A, IT Act). A claimant makes a complaint to the designated Adjudicating Officer in a specified format (see Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003).

The IT Act authorizes police officers at the Inspector rank or above to investigate IT Act offenses (Section 78, IT Act).

Indian law also permits individuals to bring civil actions for injunctions and damages for confidentiality breaches (*Diljeet Titus v Alfred A. Adebare*, 7477 of 2004 in CS (OS) No. 1257 of 2004)

6. Are there any other ways in which privacy rights can be enforced?

Indian general laws such as the Indian Penal Code, 1860 (Penal Code) also regulate some aspects of personal data collection and use. For example, Section 403 of the Penal Code imposes penal consequences for dishonest misappropriation of movable property. While the definition of movable property does not expressly include data, data theft may be tried under this provision. Individuals may also file a complaint under the Penal Code for breach of trust (Section 405, Penal Code), although the law is not well developed on this issue.

END OF DOCUMENT