

India's proposed Data Protection Bill fosters state surveillance; fails to protect privacy of children

The Indian government should amend its proposed data protection law to protect people's privacy instead of enabling unchecked state surveillance, Human Rights Watch said.



Source: [Pxabay](#)

The government has submitted the draft Digital Personal Data Protection Bill, 2022, for public consultation before introducing the measure in parliament and should incorporate feedback from civil society groups and digital rights experts.

The Digital Personal Data Protection Bill is the latest attempt by the Bharatiya Janata Party (BJP)-led central government to enact India's first data privacy law, after a previous version, introduced in parliament in December 2019, was dropped in August 2022.

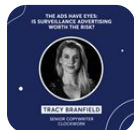
Opposition law-makers, technology companies, and advocacy groups criticised the earlier data protection bill, but the current draft also fails to address their key concerns, including not providing adequate protections for children.

"India's proposed data protection law undermines everyone's, including children's, fundamental rights to privacy and security by enhancing the power of the state to conduct surveillance," said Meenakshi Ganguly, South Asia director at Human Rights Watch. "With more and more data becoming available on digital platforms, the Indian government needs to make protecting people's privacy and security a priority."

Lack of specificity

The current bill, like the 2019 draft, would grant sweeping powers to the government beyond reasonable exceptions to exempt itself from compliance with the bill's data protection provisions for vague and overbroad reasons. These include the "interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, [or] maintenance of public order".

The bill does not elaborate on its interpretations of security and public order, terms that the government has long abused to violate freedom of expression and due process rights of critics of the government. Nor does it define standards for sovereignty, integrity, or friendly relations with foreign states.



The ads have eyes - is surveillance advertising worth the risk?

TracyBranfield, Clockwork 30 Mar 2022



This lack of specificity does not meet the standard for invasions of the right to privacy under the 2017 Supreme Court ruling in *Puttaswamy v. Union of India*, Human Rights Watch said. It is also inconsistent with international human rights law, which requires any privacy restrictions to be necessary and proportional to address a legitimate aim.

The data protection bill does not provide for safeguards or independent oversight of these government powers, and instead proposes a Data Protection Board whose members would be appointed and removed, and whose terms and conditions of service would be prescribed, by the government.

This absence of checks would facilitate surveillance and possible mass violations of people's privacy. The BJP government has already been unwilling to respond to allegations over the use of the Israeli-produced spyware Pegasus to target journalists and activists. It also did not co-operate with the committee set up by the Supreme Court to investigate the use of Pegasus spyware on Indian citizens.

Crackdown on freedom of speech

The surveillance concerns come amid the BJP government's intensifying crackdown on freedom of speech and peaceful assembly, and its enforcement of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules allow greater governmental control over online content, threaten to weaken encryption, and would seriously undermine rights to privacy and freedom of expression online.

The authorities have increasingly arrested and prosecuted human rights defenders, peaceful protesters, and members of religious minorities in politically motivated cases, including under counter-terrorism, sedition, and national security laws. There is evidence that the phone numbers of several activists currently in jail on terrorism charges were on the leaked Pegasus spyware target list. In some cases, their lawyers, relatives, and friends were also on the list.

In India, surveillance is governed by the 1885 Telegraph Act, along with the 2000 Information Technology Act. Even though the Supreme Court has twice stated, in 1997 and in 2017, that an order of surveillance can be passed only when strictly necessary and if there is no alternative, the lack of independent scrutiny and effective reporting mechanisms results in a lack of accountability.

The proposed data protection law will fail to safeguard the rights of users unless it ensures oversight of government agencies responsible for carrying out surveillance. A rights-affirming data protection law should provide independent scrutiny of government surveillance to ensure any interference with the right to privacy is necessary and proportionate, Human Rights Watch said.

The draft law also fails to protect children online, and would further expose them to known and emerging risks facilitated by technology. The bill would delete all previous references to protecting a child's best interests when online, proposing instead to protect children from overly narrow definitions of "harm," such as physical harm.

While the bill would prohibit behavioral advertising toward children, it does not protect children from the many forms of exploitation that they may face through the misuse of their data, such as discrimination, mental injury, or economic or sexual exploitation. Nor does it provide specific legal remedies for children seeking justice and redress for the violation of their rights in the digital environment.

The government should take special care to protect children in contexts in which they, or their guardians, cannot meaningfully consent to how their data privacy is handled.



Cyber savvy parents keep kids safer online

Dan Thornton 22 Aug 2022



In a global investigation of the online learning products endorsed by 49 governments during the Covid-19 pandemic, Human Rights Watch examined Diksha, an app built and used by the Indian education ministry as its primary means of delivering online education to students in Grades 1 to 12. To drive adoption, some state education ministries set quotas for government teachers to compel their students to download the app.

Human Rights Watch found that Diksha had the capacity to collect children's precise location data, including the date and time of their current location and their last known location. Diksha was also found collecting and transmitting children's personal data to Google through a tracker designed for advertising uses.

Nothing in the bill would prevent such violations of children's rights in the future, Human Rights Watch said. The proposed law would fail to protect children in physical and online classrooms alike, as students cannot realistically refuse or protect themselves against such data surveillance without jeopardising their education.

Children's legal protections

Protecting a child's best interests encompasses more than protecting them from harm. Consistent with the United Nations Convention on the Rights of the Child, children are entitled to special safeguards and care, including legal protections, at all stages of their lives. The government should recognise and protect children's data and their use of technology to empower children to realize the full range of their rights, including those to privacy, expression, thought, association, and access to information.

The government should amend the bill to require that all actors apply the highest levels of privacy protections to children's data. The government should also require any processing of children's data to meet strict requirements of necessity and proportionality, regardless of consent.

Digital surveillance or automated processing of children's data should not be routine, indiscriminate, or without the child's knowledge or right to refuse. The law should also establish effective remedial judicial and non-judicial mechanisms specifically for the violations of children's rights relating to the digital environment.

"India's first data protection law should respect people's rights, not become a tool for further invasion of their privacy," Ganguly said. "The government should also carry out surveillance reform that ensures independent oversight and judicial authorisation while providing for effective remedies."

For more, visit: <https://www.bizcommunity.com>