India Orders a Tracking App to Be Installed in All Smartphones

FROM FIRST BUSINESS PAGE

phone manufacturers, including Apple, Samsung and Xiaomi, would be responsible for ensuring that the app's "functionalities are not disabled."

There are more than one billion phones active in India, and cybercrime is proliferating. The government counted 2.3 million "cybersecurity incidents" last year, more than double the number two years before. Fraud, committed on a mass scale and often from superclusters in rural areas, is the biggest part of the problem. In 2024, a government portal tracked $2.6 billion in losses.

Mr. Pahwa noted that the Sanchar Saathi app, installed at the operating-system layer of a phone, can in principle do much more than track locations. "There's nothing to suggest this app cannot be used to pull out data," including messages, sound and images, he said.

Since the government exempted itself from India's Digital Personal Data Protection Act in 2023, there is no clear legal basis to prevent it from gathering individuals' information.

"When the government forces a special app, with special powers, onto every new phone, it is effectively putting its own lock inside your house," said Apar Gupta, a lawyer and a founder of the Internet Freedom Foundation.

"You lock your front door because you are entitled to safety and privacy," he added. "The same logic applies to digital life. Asking for safeguards and limits is about making sure state power is accountable."

Russia recently started preloading a state-owned messaging app onto its citizens' phones. The Russian government called it a measure to combat fraud, as India has done with Sanchar Saathi.

Apple and other phone manufacturers may resist pressure to ship its products with the app preinstalled. Apple has tangled with Mr. Modi's government over privacy issues before, like when the company sent an alert to some iPhone users in the opposition that their phones may have been subjected to "state-sponsored" surveillance.

ANINDITO MUKHERJEE FOR THE NEW YORK TIMES

An app blurs the line between preventing fraud and monitoring citizens.

Those alerts were prompted when several governments, including India's, bought access to Pegasus, a spyware program developed by an Israeli company, to monitor private citizens.

A list of hundreds of Pegasus targets within India was leaked to a nonprofit in 2021. It included politicians in Congress, journalists, Tibetans, human-rights activists and ministers from Mr. Modi's own party. The government denied having used it, but a committee formed by India's Supreme Court to investigate the matter was forced to disband in 2022, because "the government of India has not cooperated," said N.V. Ramana, the chief justice at the time.

Mr. Pahwa, the digital policy analyst, noted that "apps for cybersecurity can also become apps for cybervulnerability." Connecting every Indian's data to a single app "creates a single point of failure, from a hacking standpoint," he said.

For years, "the government of India has been collecting and linking data sets together without creating silos between them," Mr. Pahwa said, which has paved the way for forms of fraud that exploit a victim's personal information to gain confidence.