



WHAT INDIA'S LANDMARK COURT RULING ON PRIVACY MEANS FOR DATA PROTECTION

AUGUST 25, 2017

SUMMARY

- The Supreme Court of India unanimously ruled that privacy is a fundamental right protected by the Indian Constitution, a decision with far-reaching implications for the Indian government, society, and foreign investors.
- The ruling has immediate consequences for India's landmark digital identification program known as [Aadhaar](#), which is already facing challenges from multiple parties in court for privacy infringement.
- The verdict prioritizes the establishment of data protection regulations to specifically protect citizens' right to informational privacy, which spells uncertainty for technology companies in India.

ABOUT ASG

Albright Stonebridge Group (ASG) is the premier global strategy and commercial diplomacy firm. We help clients understand and successfully navigate the intersection of public, private, and social sectors in international markets. ASG's worldwide team has served clients in more than 110 countries.

ALBRIGHTSTONEBRIDGE.COM

PRIVACY IN AN ERA OF RAPID TECHNOLOGICAL CHANGE

On August 24, 2017, India's Supreme Court ruled unanimously that Indian citizens have a fundamental right to privacy—a decision that will have sweeping implications for India's foundational digital identity and authentication initiative known as [Aadhaar](#), the collection and storage of personal data, as well as personal and social life in India.

The case was referred to the Supreme Court earlier this year amid hearings of petitions against the constitutionality of Aadhaar. In their judgments, India's Supreme Court justices recognized the game-changing role of technology in interpreting citizens' right to privacy today, overruling past decisions denying a fundamental right to privacy in the process.

The Indian government [had argued](#) that privacy is not an intrinsic right protected by the Constitution, but has since expressed support for the Supreme Court ruling while emphasizing that privacy is "[not absolute](#)." Specifically, the government is interested in preserving the continuation of Aadhaar in its current state.

The decision adds precedent to the emerging global debate on privacy rights in the digital age. Citizens are building complex digital identities based on their online activity and transactions that present both

"TECHNOLOGICAL CHANGE HAS GIVEN RISE TO CONCERNS WHICH WERE NOT PRESENT SEVEN DECADES AGO..."

— JUDGEMENT OF JUSTICE D.Y. CHANDRACHUD

opportunities and challenges. Moreover, this phenomenon is occurring at a time when online trust is low and security threats are growing more sophisticated.

A Setback for Aadhaar?

All eyes have been on Aadhaar since its rollout in recent years. The biometric database contains detailed records on India's billion+ population and aims to streamline government services, accelerate financial inclusion, and ultimately create a digitally secure way for citizens to interact in daily civic life.

To encourage adoption, the Indian government made enrollment compulsory in exchange for certain services and processes, including filing tax returns, opening bank accounts, and receiving government subsidies. This ruling draws the mandatory aspect of Aadhaar enrollment into question, and raises additional questions about the boundaries of collecting and sharing citizens' data, including with private companies.

Aadhaar represents one of the most impressive data collection undertakings between a government and its citizens and has the potential to transform that relationship, yet privacy advocates cite high-profile data breaches as a major cause for concern. With the question over citizens' right to privacy settled, a three-judge bench is now set to rule on the constitutionality of Aadhaar in its current state.

WHAT THIS MEANS FOR BUSINESS: UPCOMING DATA PROTECTION REGULATIONS

Big data collection and sharing has introduced unprecedented levels of personalization and convenience to today's consumers. At the same time, this immense data exchange has triggered security and privacy concerns that call for new safeguards.

The Supreme Court ruling prioritizes the establishment of data protection regulations, which presents risks to technology companies that may have to spend significant resources adapting their data practices—including how they collect, share, process, store, and delete data. Spending on information technology climbed to almost \$90 billion in 2017 as firms prepare for the implementation of the European Union's General Data Protection Regulation that goes into effect in 2018.

India's Ministry of Electronics and Information Technology recently established an expert committee to study data management and put forth a draft of a comprehensive data protection law, which will build on existing sector-specific protections and the Information Technology Act of 2000. Coinciding with the Supreme Court ruling, the National Institution for Transforming India Aayog also called for a comprehensive framework to protect digital payments specifically.

The Supreme Court verdict puts further pressure on the establishment of a data protection law, making this an opportune moment to engage in the dialogue on best practices for data collection, protection, and storage and to gain insight into how policymakers in India are preparing for compliance. ASG will continue to monitor the implications of this ruling and its impact on Aadhaar and data protection laws.

ASG's [India and South Asia Practice](#) has extensive experience helping clients navigate markets across South Asia. For questions or to arrange a follow-up conversation please contact [Ashlyn Anderson](#).

