INTERNET & DIGITAL POLICY TRENDS IN INDIA - September 2020

MediaNama is the premier source of information & analysis on Digital Policy in India. We focus on key issues like privacy, data governance, fake news, misinformation, cybersecurity, cyber diplomacy, digital payments policy, Net Neutrality, intermediary liability, website blocking, internet shutdowns, data localisation, e-commerce policy, IoT, content regulation and censorship, among others.

Our mission is to help build a digital ecosystem which is open, fair, competitive and global.

On MediaNama.com, our reportage attracts a readership of policy professionals, government officials, Members of Parliament, startup founders and business leaders, as well as investors with an eye on policy developments shaping the future of the Internet in India.

MediaNama’s events enable meaningful conversations for a high quality and curated audience to discuss opportunities, challenges and issues that they care about, in a manner that helps in building capacity. The fact that they are among peers with similar depth of understanding, and come at the same issues from a different point of view, ensures that our audience keeps coming back for more.

Nikhil Pahwa | Founder & Editor | nikhil@medianama.com
Harneet Singh | Business Head | harneet@medianama.com

www.medianama.com | twitter.com/medianama (@medianama)
youtube.com/user/medianama | facebook.com/MediaNama
linkedin.com/company/medianama
1. **Growing Internet market:** because India has a hyper-competitive telecom market.
   a. **Second largest number of Internet users in the world:** India has over 500 Mn Internet users, over 683.77 Mn broadband Internet connections, of which Reliance Jio has 393.72 Mn. It is among the largest markets for Facebook, YouTube, WhatsApp, etc. Most connections are prepaid.
   b. **Cheapest Internet access in the world:** Average cost of data is ~ $0.11 (Rs 8.4)/GB data.
   c. **High data consumption:** Average Wireless Data Usage per wireless data subscriber per month is 10.4 GB. Many monthly plans offer 1GB per day.

2. **Digital is strategic and geopolitical:** Digital policy (including data protection, IPR, connectivity projects, competition regulation, technology choices, and platform creation and deployment) is seen as being integral to India's strategic interests. This is defining India's participation in global agreements, especially those related to cross border data flows, payments and e-commerce regulation.

3. **Data as a national resource:** Policies tend to treat data as a national/community resource, and less from the perspective of privacy as a fundamental, individual right. ‘Data is the new oil’ is a refrain heard often in India, and it is being seen as critical for India to become an Artificial Intelligence superpower. The leaked draft e-commerce policy called data “a national resource” that e-commerce entities use to build their data, and is as important as “intellectual capital (intellectual property) or industrial capital (funds)”.

4. **Asserting sovereignty over data:**
   a. **Localise data and resist cross border data flows:** India is looking to localise/restrict ‘critical personal data’ to the physical boundaries of India, and limit overseas processing of ‘sensitive personal data’ of data generated. Registration of Cloud Service Providers with the DoT has been recommended by TRAI. When Chinese apps were banned, the fact that they were sending data outside India was highlighted.

   Financial data is already localised, and this might eventually extend to health, education, and non-personal data. India refused to sign the Data Free Flow with Trust (DFFT) at the G20 summit in Japan. The draft e-commerce policy also looks to localise data

   b. **Control over data, and access:** The Personal Data Protection Bill 2019 enables India to acquire non-personal data (aggregate or anonymised) for the “delivery of services or formulation of evidence-based policies”, from private entities. The Non Personal Data Committee recommendations suggest that decisions regarding transfer of NPD to companies or the government should be determined by a regulatory authority. This is nationalisation of privately owned intellectual property. NPD could be related to health, shopping preferences, or road traffic data. The draft e-commerce policy wants “to enable the government to have speedy access to data flowing on e-Commerce platforms that operate in the country”

5. **Government as a platform:**
   a. **Increase Access:** TRAI has recommended enabling public WiFi hotspots, delicensing 5.725 - 5.825 GHz spectrum band for outdoor usage by wireless
ISPs, and setting up of Public Data Offices. It supported Reliance Jio’s free “trial” of 6 months. It has recommended opening up WiFi on domestic flights.

b. **Digitise everything**: Citizen interfaces with the government are being digitised, including delivery of subsidy schemes and the national Census. Education, health, payments, RFID in cars, National Land Bank, smart meters, tax payments, vehicle registration, land records and even Right to Information requests are digital. There’s an app for most services, and the Umang app which aggregates many of them. The NODE system is looking to replicate the approach taken for Aadhar and IndiaStack: Create a digital infrastructure, with services, APIs and applications, with a governance structure, and a community.

c. **Centralisation using digitisation**: Aadhaar is centralisation of identification. In addition, there’s “One Nation One Ration Card”, National Common Mobility Card.

d. **Large databases of citizens’ data**: India is countering data collection by global corporations by creating its own citizen databases. Consent is often forced: denial of government services is used to force data sharing. Databases will include Aadhaar, the National Register of Citizens, the National Health Information Network, Automatic Facial Recognition System Database, Sarathi database, Vahan database, the public credit registry.

   The National Social Registry will use Aadhaar to integrate religion, caste, income, property, education, marital status, employment, disability and family-tree data of every citizen, data updated in real-time.

e. **Enable access to data**: The Digital Empowerment and Protection Architecture (DEPA) framework seeks to break data silos and enable user control over data, and allow users to share data with third parties via a consent manager. This will work with account aggregators, which allow users to maintain their data and financial accounts. This is meant to assist in developing insurance and lending ecosystems. The government has proposed a lending system called Kashi (Cash over Internet). KYC Setu enables digital KYC sharing.

f. **Embrace (some) new technologies**: India has approved a drone policy, but banned cryptocurrencies. Several departments are trying to claim leadership over the AI roadmap. AI Stack.

g. **Sandboxing**: Regulators are encouraging the usage of technology sandboxes. IRDA already has insurance-tech products in a sandbox. The National Digital Health Roadmap proposes sandboxes

h. **Monetise data in 'national interest'**: Government databases enable the conversion of personal information into public assets. As per the 2018-19 Economic Survey: “Consistent with the notion of data as a public good, there is no reason to preclude commercial use of this data for profit.” The Ministry for Road Transport & Highways made ~$8.8 million (Rs 65 crore) by selling citizen data to 142 firms. A previous draft e-commerce policy also indicated an intent to enable sharing of non-personal data with Indian startups, for a fee.

6. **Fear of ‘Digital Colonisation’**:

   a. **Push back against global corps**: India is wary of large corporations if they aren’t of Indian origin: this is most evident in conversations around e-commerce, social media and competition. The draft e-commerce policy recommends competition regulation. The report of the Competition law review committee suggests that data should be considered for assessing market power. Draft consumer protection norms mandate country of origin disclosures for
products. There is explicit support for Indian startups in e-commerce policy, Non Personal Data report. The government also has the Startup India programme, and the Atma-nirbharta app challenge. From a political perspective, co-ordinated FIR's have been filed against twitter for sedition, with the police across the country by the BJP’s Vinit Goenka and a group of people coordinating with him.

b. **Domestic companies are pushing for protectionist measures:** ShareChat against Chinese firm TikTok; Paytm against Google Pay and WhatsApp payments; local traders lobbies against Amazon and (Walmart owned) Flipkart.

7. **Online versus offline:** Traditional publishers have pushed for regulation of digital media. Gig workers - drivers, food delivery personnel - have protested against centralisation by platforms. Restaurants pushed back against Zomato Gold. Chemists are protesting e-pharmacies, and the Delhi Chemists Association asked for Aarogya Setu Mitr to be delinked from Aarogya Setu.

8. **Cyber security is National Security:** This includes not just protecting critical digital assets and prevention of data being shared overseas, but also interception of all communications, traceability of social media users, content regulation, regulation of health and financial transaction data etc.
   a. **Exemptions for government access to data:** The Personal Data Protection Bill, 2019 enables wide and unrestricted government access to data, with no proportionality and necessity related restrictions.
   b. **Linking databases together:** NATGRID (National Intelligence Grid), which intends to link multiple public and private databases together, is expected to be launched soon. In the first phase, 21 databases, including mobile, Banking, Airlines, SEBI (stock market) and Railways will be linked. In Phase 2, over 900 public and private databases will be linked.

   Database access will be available to various investigating agencies, including the Intelligence Bureau, Enforcement Directorate, R&AW, CBI, DRI, FIU, CBDT, CBEC, DGCEI and Narcotics Control Bureau (NCB).
   c. **Biometrics in use:** The DNA Technology Regulation Bill seeks the usage of DNA profiles for crime detection and prevention. The National Crime Records Bureau believes that its Automated Facial Recognition System “will not violate privacy”. Vadodara Police piloted a project with Clearview AI. CCTVs are being set up across cities, with no law in place. Police are using drones to track and record videos of protestors at public protests.
   d. **Demand for traceability of messages:** India wants traceability of originators of all communication, including encrypted, to address fake news and terrorist activity. The IT Minister has pushed for traceability despite end-to-end encryption. A crucial case on traceability is being heard in the Supreme Court of India, and Intermediary Liability rules may be modified. A Parliamentary committee has recommended, for protection of children online, that law enforcement agencies be permitted to break end-to-end encryption to trace abusers.

9. **Increased regulation of online speech and Internet access:**
   a. **Weaken safe harbour:** Changes to Intermediary Liability Rules might seek to enforce automated content takedown mechanisms by messaging services and social media platforms. Music labels are also pushing for increasing liability of ISPs and other intermediaries to address piracy.
b. **Regulation of Social Media:** The Personal Data Protection Bill creates a definition of social media intermediaries, which may lead to them being regulated separately from other intermediaries. There is a demand to regulate Facebook, following suspicions of bias within Facebook’s India team. On multiple occasions, Whatsapp group admins have been told they’ll be liable for group content.

c. **Linking social media to IDs:** While the Supreme Court and Madras High Court have rejected the idea of linking the national ID Aadhaar to social media accounts, a petition being discussed in the Supreme Court, with a demand for linking social media accounts to government IDs.

d. **Internet shutdowns:** India has the highest Internet shutdowns in the world: 134 in 2018; 109 in 2019. The Internet was shut down for 133 days in Kashmir in 2016, and 100 days in Darjeeling in 2017. In Kashmir, the Internet was shut down from August 4, 2019 to January 15, 2020.

e. **Firewalling Internet access:** While ISPs in India, without much transparency, regularly block access to different websites, a formal firewall was first instituted on January 15, 2020, wherein only a list of 329 government approved websites was accessible in Kashmir, following a Supreme Court order which stated that certain websites must remain accessible, even during an Internet Shutdown.

f. **Crackdown on VPNs:** ISPs in Kashmir, in January 2020, sought written undertakings from users saying they will not access VPN applications. Army personnel began checking phones for VPN apps.

g. **Increase in blocking activity under Section 69:** Chinese apps were banned under Section 69, but even during the COVID19 lockdown, the blocking activity increased significantly.

h. **Increased tracking of social media activity:** Information & Broadcasting Ministry wants to set up a social media hub to monitor social media activity. BECIL has put out a tender for Social Media Communications Hub eight times, latest for fact checking. The HRD ministry, in 2019, sent a letter to colleges asking for connecting all the students’ Twitter/Facebook/Instagram accounts to their own.

i. **Regulation of Online News media and aggregators:** RPP bill and restriction of FDI in Digital Media

j. **Content regulation of VoD platforms:** The government wants to certify online content on VoD platforms, following complaints and cases related to shows with controversial (but not illegal) content. The IAMAI (industry body) has created a third version of its content regulation code. Netflix has delayed a show on Indian “Bad Boy Billionaires”, following lawsuits.

k. **Protecting children online:** Local police, in the past, had placed bans on games like PUBG. PUBG is now banned. Download of TikTok was also banned briefly, for protecting children, and TikTok has now been banned. The definition of child pornography has been expanded by amending the POCSO Act. A Parliamentary committee has recommended, allowing law enforcement to break end-to-end encryption, and intermediaries be responsible for proactively identifying and removing Child Sexual Abuse Imagery (CSAM); ISPs be made liable for CSAM, and ensure that parents have family-friendly filters. India leads in generation of child sexual abuse material. In the Personal Data Protection Bill, 2019, the age of consent is 18.
10. Regulatory process trends:

a. **Segmented, verticalised regulation of platforms**: Separate frameworks are being created/considered for different technology platforms, including content, social media platforms, online pharmacy aggregators, payment gateways, e-commerce platforms, etc., even though the IT Act doesn’t segment intermediaries, nor distinguish between active and passive intermediaries.

b. **Jurisdiction challenges**: There have been instances of jurisdictional over-reach: the Commerce Ministry released a draft e-commerce policy which included provisions related to privacy, which is an IT Ministry remit. There’s lack of clarity about jurisdiction of online streaming services, between MEITY and I&B. The TRAI has made recommendations on Privacy.

c. **Increased regulation**: Since 2018, there has been a dramatic increase in regulatory activity. Un-regulated or even lightly-regulated sectors, companies and activities, whether cryptocurrency trading, online streaming of video and music, online news publications and blogs, ecommerce platforms, mobile wallets, VoIP calling and messaging, social media and even online pharmacies have seen much greater regulatory interest and scrutiny over the last year. There seems to be a belief that nothing should be allowed to operate without targeted regulation.

d. **Judiciary being asked to take on a policy-making role**: In the absence of government policies on several domains, numerous Public Interest Litigations have been filed, related to online content regulation, regulation of social media, and traceability of online content creators, seeking to instigate the regulatory process through judicial direction or intervention.

e. **Process as an inconvenience**: There is a lack of transparency in the policymaking process: the Indian government hasn’t made comments submitted to public consultations on the Personal Data Protection Bill 2018 and the Draft E-commerce Policy public. The Reserve Bank of India did no consultations before imposing data localisation and banning cryptocurrencies. Submissions for India’s National Cybersecurity policy are not public. The Right To Information Act has been diluted. Other discussions, including that of non-personal data, are without public consultation processes.

Subscribe to MediaNama: [Newsletter](#) / [Twitter](#) / [YouTube](#) / [LinkedIn](#) / [Telegram](#)