Proposed
Digital India Act, 2023

Digital India Dialogues
09.03.2023
Bengaluru, Karnataka
Background (1/2)

India’s Digital revolution and Global advancements have made our current regulatory landscape old and dated...

1. IT Act 2000 is 22 years old and was created in the early days of internet.

2. Provisioned for nascent IT ecosystem in 2000 pre-Digital India in the absence of modern internet-based service such as e-Commerce, social media platforms

3. Limited mandate- legal recognition of electronic records, transactions and electronic signatures over the electronic medium

4. Internet, Devices and Information Technology have empowered citizens. However, these have also created challenges in the form of user harm; ambiguity in user rights; security; women & child safety; organised information wars, radicalisation and circulation of hate speech; misinformation and fake news; unfair trade practices, etc.

Annexure I- Limitation of IT Act
Background (2/2)

Current Regulatory Landscape

- Intermediary Guidelines and Digital Media Ethics Code
- Reasonable Security Practices and SPDI Rules
- Use of Electronic Records and Digital Signatures
- Certifying Authorities Rules
- Information Technology Act
- Procedures and Safeguards for Blocking Rules
- Indian Computer Emergency Response Team (CERT)
- Cyber Appellate Tribunal
Digital India Act (2023)

1. Digital India Goals 2026

2. Need for Global Standard Cyber Laws

3. Goals and Proposed Structure of DIA

4. Way Forward
Hon’ble Prime Minister’s Vision for Digital India

1. $1 trillion digital economy by 2025-26: Atmanirbhar Bharat

2. Global innovation and entrepreneurship system

3. India to be Shaping the Future of Technologies

4. India to be a Significant Trusted Player in the Global Value Chains for Digital Products, Devices, Platforms and Solutions.
1. Digital India Goals 2026

2. Need for Global Standard Cyber Laws

3. Goals and Proposed Structure of DIA

4. Way Forward
Global Standard Cyber Laws
to act as a catalyst and enabler for
$1 trillion digital economy
Objectives of Global Standard Cyber Laws

1. Ensure Indian Internet is **Open, Safe & Trusted and Accountable**

2. Accelerate the growth of **innovation and technology ecosystem**

3. Manage the **complexities of internet and rapid expansion of the types of intermediaries**

4. Create a framework for **accelerating digitalization of Government** and to strengthen democracy and governance (G2C)

5. **Protect citizens’ rights**

6. **Address emerging technologies and risks**

7. **Being Future-proof and Future-ready**
Framework of Global Standard Cyber Laws

- Digital India Act
- Digital Personal Data Protection Act
- DIA Rules
- IPC Amendments for Cyber Crimes
- National Data Governance Policy
## Internet in 2000 vs Internet today

### Internet in 2000
- **5.5 million** Indians on Internet
- One type of intermediary
- Space for good – allowing citizens to interact
- **Traditional forms of User Harms:** Cybercrime, Cyber-security, Hacking
- **Source of Information and News**

### Internet Today
- **850 million** Indians on Internet - world’s largest digitally connected democracy
- Multiple types of intermediaries - eCommerce, digital media, social media, AI, OTT, gaming etc.
- Space for **criminalities and illegalities**
- **New Complex forms of User Harms:** Catfishing, Doxxing, Cyber stalking, Cyber trolling, Gaslighting, Phishing, etc.
- Proliferation of **Hate Speech, Disinformation and Fake news**

**Present Challenges in the Cyberspace - Beyond the scope of IT Act**
- Traditional forms of User Harms:
- New Complex forms of User Harms:
Digital India Act (2023)

1. Digital India Goals 2026
2. Need for Global Standard Cyber Laws
3. Goals and Proposed Structure of DIA
4. Way Forward
**Goals of DIA**

- The new law should **evolve** through rules that can be updated, and address the **tenets of Digital India**
  - Open Internet
  - Online Safety and Trust
  - Accountability and Quality of Service
  - Adjudicatory mechanism
  - New Technologies

- Urgent need for a specialized and dedicated **adjudicatory mechanism** for online civil and criminal offences. The adjudicatory mechanism should
  - be easily accessible
  - deliver timely remedies to citizens
  - resolve cyber disputes
  - develop a unified cyber jurisprudence
  - enforce the rule of law online
The new Digital law should be **evolvable and consistent** with changing market trends, **disruption in technologies**, development in **international jurisprudence** and global standards for qualitative service/products delivery framework.

In order to rapidly create, modify, and enforce regulations, it will adopt ‘**principles & rule-based approach**’ to regulation which provides a legislative framework under governing principles and effective measures for securing compliance with the ever evolving rule of law.
Digital India Act – Index

1. Preamble
2. Principles
3. Digital Government
4. Open Internet
5. Online Safety and Trust including User Harm
6. Intermediaries
7. Accountability
8. Regulatory Framework
9. Emerging Technologies, Risks and Guard Rails
10. Miscellaneous
Key Components of DIA
Open Internet

(1/2)

• An Open Internet should have
  (a) Choice;
  (b) Competition;
  (c) Online diversity
  (d) Fair market access, and
  (e) Ease of Doing Business and Ease of Compliance for Startups

• **Fair trade practices**, prevention of concentration of market power and gatekeeping, distortions through regulation of dominant Ad-tech platforms, App stores etc., promoting start-up India via **non-discriminatory** access to digital services and **interoperable platforms**.

• **Safeguard innovation** to enable emerging technologies like AI/ML, Web 3.0, Autonomous systems/ Robotics, IoT/ Distributed Ledger/ Blockchain, Quantum Computing, Virtual Reality/ Augmented Reality, Real-time language translators, Natural-language processing, etc.

• **Promotion of Digital Governance** ease access to government & other public utility services, **delivery of public services through online and mobile platforms** in a simple, accessible, interoperable and citizen friendly manner.

• May need to update provisions in the **Competition Act, 2002**
Open Internet (2/2)

Big Tech is often gaming the System

**The New York Times**

*U.S. Accuses Google of Abusing Monopoly in Ad Technology*

The Justice Department’s antitrust lawsuit, which a group of states joined, was the fifth by U.S. officials against the company since 2020.

**Bloomberg**

*Google Found to Unfairly Block Rival Payments on India Store*

- The antitrust watchdog says practices are discriminatory
- Google is grappling with a backlash at home and abroad

**Financial Times**

*Big Tech attacks tough EU measures aimed at tackling its market power*

Apple and Google criticise newly unveiled Digital Markets Act that will force a radical overhaul of their global operations

**INET**

*Big Tech: Not Only Market But Also Knowledge and Information Gatekeepers*
Online Safety and Trust (1/5)

- Adjudicating User Harm against revenge porn, cyber-flashing, dark web, women and children, defamation, cyber-bullying, doxing, salami slicing, etc.

- Age-gating by regulating addictive tech and protect minors’ data, safety and privacy of children on social media platforms, gaming and betting apps; Mandatory ‘do not track’ requirement to avoid children as data subjects for ad targeting, etc.

- Digital user rights including Right to be forgotten, Right to secured electronic means, Right to redressal, Right to digital inheritance, Right against discrimination, Rights against automated decision making, etc.

- Discretionary moderation of fake news by social media platforms should be critically examined and regulated under the Constitutional rights of freedom of speech & expression.
• **Definition and Regulation of hi-risk AI systems** through legal, institutional quality testing framework to examine regulatory models, algorithmic accountability, zero-day threat & vulnerability assessment, examine AI based ad-targeting, content moderation etc.

• **Privacy invasive devices** such as *spy camera glasses, wearable tech* should be mandated under stringent regulation before market entry with strict **KYC requirements** for retail sales with appropriate criminal law sanctions.

• **Secure Cyberspace** by empowering agencies like CERT-In for cyber resilience; strengthening the penalty framework for non-compliance, advisories on the information & data security practices, etc.

• **Content Monetisation Rules** for platform-generated and user-generated content
Online Safety and Trust (3/5)

User harm, taking various forms - Particularly unique to the internet

**CNN News**
January 2023

*Seattle public schools sue social media companies for allegedly harming students’ mental health*

**The Wall Street Journal**
February 2023

*Lawmakers Renew Push to Shield Children From Harmful Online Content*

**HT Tech**
February 2023

*Gaslighting, love bombing and narcissism: why is Microsoft Bing chatbot so unhinged?*

There’s a race to transform search. And Microsoft just scored a home goal with its new Bing search chatbot, Sydney, which has been terrifying early adopters with death threats.

**Reuters**
February 2023

*As U.S. Supreme Court weighs YouTube's algorithms, 'litigation minefield' looms*

**Washington Post**
February 2023

*AI porn is easy to make now. For women, that’s a nightmare.*

Easy access to AI imaging gives abusers new tools to target women. AI-generated tools are becoming commonplace and so too are “DeepFakes” which can easily generate realistic-looking content. Photorealistic DeepFakes add another layer of harm to women online.

**The Financial Times**
January 2023

*Sunak faces potential rebellion over online harms bill*

Tory backbenchers want tougher sanctions on tech bosses who fail to protect children from harmful content.
Online Safety and Trust (4/5)

Weaponisation of disinformation in the name of Free Speech

**The New York Times**

*Combating Disinformation Wanes at Social Media Giants*

As the companies have shed jobs recently, many teams assigned to combat false and misleading information have taken a hit.

**The New York Times**

*How Social Media Amplifies Misinformation More Than Information*

A new analysis found that algorithms and some features of social media sites help false posts go viral.

**The Seattle Times**

*The week in fake news: Misleading viral tales that fail their fact checks*

**The Wall Street Journal**

*EU Warns Twitter Over Incomplete Content-Moderation Report*

The report is a dress rehearsal for the EU’s new social-media law

**The Washington Post**

*January 2023*

*Is ChatGPT an Eloquent Robot or a Misinformation Machine?*

**The Guardian**

*February 2023*

*Revealed: the hacking and disinformation team meddling in elections*

**The Washington Post**

*January 2023*

*Weaponisation of disinformation in name of free speech by Twitter comes to grinding halt: Chandrasekhar*

**The Print**

*3 December, 2022 10:01 pm IST*

*Twitter hate speech up in large foreign markets after Musk takeover*
Online Safety and Trust (5/5)

Intermediaries have started acting upon harmful content, but that’s not enough!

**Youtube:** 58.2 lakh Channels, 56 lakh videos (30% of which are from India) Removed

- **Top 3 reasons for channel suspension:** Spam, misleading; Nudity or sexual and Child Safety
- **Top 3 reasons for video removal:** Child Safety, Violent content, nudity or sexual

*July to Sept 2022

**Meta:** 327 crore content acted upon

- **Acted upon content:** 322 crore on Facebook and 52 crore on Instagram
- **Top 3 reasons for acting:** Spam, Fake accounts and Adult Nudity & Sexual Activity

*Oct to Dec 2022

**Whatsapp:** 97.2 lakh Indian accounts banned

- Accounts are banned when abuse is detected either on the basis of user complain, or through Whatsapp’s own tools and resources

*Oct to Dec 2022
Accountable Internet (1/2)

- **Adjudicatory and Appellate Mechanisms** for accountable and responsive digital operators; **updated intermediary framework**; Obligations on significant digital operators through classification/ mandates; **Algorithmic transparency** and **periodic risk assessments** by digital entities.

- **Accountability** for upholding **Constitutional rights** of the citizens, esp. Article 14, 19 & 21; **Ethical use of AI based tools** to protect rights or choices of users; **Provision of deterrent**, effective, proportionate and dissuasive penalties, etc.

- **Whole-of-Government Response** for a unified, coordinated, efficient and responsive governance architecture including an effective appropriate government structure, a **dedicated inquiry agency** and a **specialised Dispute resolution/ adjudication framework**.

- **Disclosure Norms** for data collected by Data Intermediaries, collecting data above a certain threshold.

- **Standards for ownership** of anonymized personal data collected by Data Intermediaries
### Need for Responsible and Ethical Use of Online Technologies

- **The Forbes**
  - Deepfakes - The Danger Of Artificial Intelligence That We Will Learn To Manage Better
  - *Sep 8, 2022*
  - ...more widespread abuse is expected with more widespread availability.

- **FTC Press Release**
  - FTC Report Warns About Using Artificial Intelligence to Combat Online Problems
  - Agency Concerned with AI harms such as inaccuracy, bias, discrimination, and commercial surveillance creep.

- **The Washington Post**
  - March 2023
  - ‘Noah’ and ‘Daren’ report good news about Venezuela. They’re deepfakes.
  - The avatars are the latest tool in Venezuela’s disinformation campaign, experts say

- **The New York Times**
  - Supreme Court Seems Wary of Limiting Protections for Social Media Platforms
  - The case, concerning a law that gives websites immunity for suits based on their users’ posts, has the potential to alter the very structure of the internet.

- **The New York Times**
  - Alarmed by A.I. Chatbots, Universities Start Revamping How They Teach
  - With the rise of the popular new chatbot ChatGPT, colleges are restructuring some courses and taking preventive measures.

- **World Economic Forum**
  - Is blockchain really secure? Here are four pressing cyber threats you must consider
  - Feb 21, 2023
Intermediaries

Different types of intermediaries

- eCommerce
- Digital Media
- Search Engines
- Gaming
- AI
- Over-the-top (OTT) Platforms
- TSPs
- Ad-Tech
- SSMIs, etc

Need for separate rules for each class of intermediaries

Should there be “Safe Harbour” at all for intermediaries?
Digital India Act (2023)

1. Digital India Goals 2026
2. Need for Global Standard Cyber Laws
3. Goals and Proposed Structure of DIA
4. Way Forward
Way Forward

Core Team in MEITY: [MOS, Addl Secy, GC Cyberlaw, ASG, Outside Legal Expert, Outside Industry Expert]

1. Comparative Study of all relevant Global laws pertaining to the internet and technology in other countries

2. Draft Bill

3. Consultations with experts, general public, industry, media, academia, student community, internet governance forums and consumer forums

4. Draft Cabinet Note and Policy

5. Digital India Act (DIA)
THANK YOU
Annexure I- Limitations of IT Act 2000

The current IT Act has following limitations, among others:

i. Lack of comprehensive provisions on user rights, trust & safety;

ii. Limited recognition of harms and new forms of cybercrimes, without any institutional mechanism for awareness creation;

iii. Lack of distinct regulatory approaches for harmful and illegal content;

iv. Absence of adequate regulations to address the regulatory requirements of emerging technology, assessments of high risk automated-decision making systems modern, digital businesses including monopolies and duopolies;

v. Lack of adequate principles for data / privacy protection;

vi. Lack of a converged, coordinated & harmonized institutional regulatory body; a dedicated & efficacious investigatory/ enforceability and a swift adjudicatory mechanism;

vii. Lack of coordinated cyber security incident response mechanism