INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on Internet

## CONSUMER DATA BREACH

In 2020, coronavirus upended daily lives worldwide, with the government taking tough decisions to stop the spread of the virus. Work from home became the new normal, and the world witnessed a rapid online shift. With this shift, one would surely agree that the pandemic amplified the criticality of security. Organizations had to take care of menaces like data breaches and data leaks to safeguard their users and brand value.

The majority of massive data breaches in 2020-21 witnessed the vulnerability of user's Personally Identifiable Information (PII), Sensitive Personal Information (SPI) and other sensitive and personal data. PII data refers to any data used to identify a specific individual, such as phone numbers, email address, social security number like Aadhar card number. SPI data refers to any information that could harm an individual if it is made public, like bank card details or biometric data. The threat vectors put this user data on the dark web for their personal gain. The dark web is a part of the Internet that is not visible or indexed by search engines like google and is mostly used by such threat vectors.

## OTHER STORIES INSIDE THIS ISSUE:

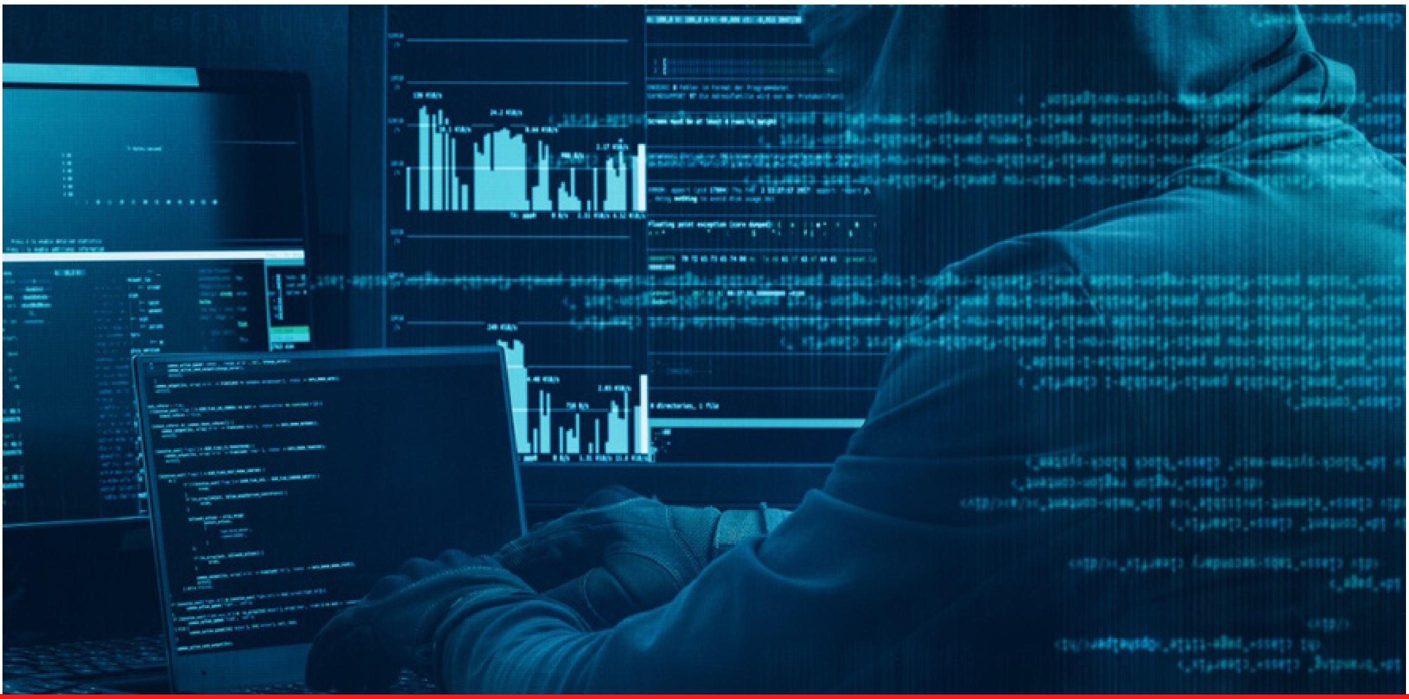
MobiKwik is a digital payment platform that faced a significant data leak recently. The 8.2 Terabytes of leaked customer data includes phone numbers, bank details, email addresses, card details and KYC details of 9.9 crore users. Hackers built a dark web search-engine portal where people could check if their personal information were on the hacked database.

Upstox, a leading brokerage firm in India, incurred a data breach involving 25 lakh customer's data stolen and made available for sale on the dark web. The stolen data includes names, email addresses, date of birth, bank and KYC details of users.

Domino's Pizza, a popular food chain, went through a significant cyber-attack, resulting in over 18 crore user records on dark web forums and marketplaces. The leaked data includes the customer's name, phone numbers, email IDs, addresses, and payment details.

Juspay, a popular payment gateway, encountered a cyberattack recently, resulting in Juspay losing hold of its thirty-five million users masked card records, 100 million users metadata information, and fingerprints belonging to its clients, including popular service providers were leaked in this data breach.

A hacker leaked approximately 20 million user records of  BigBasket, an Indian online grocery delivery service containing detailed personal information (which includes email ids, mobile numbers, date of birth and home addresses) and hashed passwords on a popular hacking forum. The said database (15 GB file in SQL format) has been posted for free and is available for anyone to download.



# STAYING SAFE ON THE INTERNET

Remember these tips to have a secure browsing experience and make your information invulnerable to threats:

- The website https://haveibeenpwned.com/ takes up an email address or a phone number as input from the user and checks whether their data has been compromised or not. If the website shows that your data is pawned, consider updating your passwords with stronger ones.
- Enable two-factor authentication or multi-factor authentication.
- Avoid short URLs or other dubious-looking email and links.
- Being proactive on the Internet and avoiding scams like lottery or other tempting scams is another trait of good cyber hygiene.
- Setting up alerts for purchases and login of your account.
- Lastly, it comes down to trust in this digital era. A quick check-up on the website or the app before using their services and giving your personal details, checking if the permissions it is asking is required, and not impulsively providing sensitive information can help you to become a safe user of the Internet.

# DON'T FORGET YOUR DIGITAL FOOTPRINT

Imagine walking on a beach, and with each step, you leave your footprint on the sand. The footprints indicate your origin and give an idea of where you are heading. Similarly, while browsing something on the Internet, downloading something, watching a video on YouTube, or shopping on Amazon, you leave digital traces behind. Digital Footprint means the traceable online activities one leaves behind while using the Internet.

A digital footprint can reveal much information about you. We often don't think of our online activities and how much data different platforms collect. For example, photos we upload may have location data. You can turn off the geotagging feature to stop adding location data to your photos. Malicious actors often correlate such data and find sensitive information about their target.

You can enter your full name on different search engines and review the results and images section to check if any unintentional data is available. Check your privacy settings on social media platforms and use good VPNs and ad-blocker extensions.

# SECURING CONSUMER INTERNET OF THINGS (IoT)

Internet of Things (IoT) is one of the emerging technologies that refers to a system of interrelated and inter-connected systems to connect and exchange data with other devices and systems over the Internet. In a study by GSMA (Global System for Mobile Communications Association), it is estimated that there will be 13.3 Billion IoT devices by 2025.

Government of India (GoI) is taking measures to enable a well-connected ecosystem in India through its policies to provide an impetus for IoT growth.

The Telecom Engineering Centre (TEC), a body under the Department of Telecommunications (DoT) and Ministry of Communications and Information Technology, Government of India, released draft guidelines for Securing Consumer Internet of Things (IoT).

## TEC releases draft guidelines for Securing Conusmer IoT

IoT guidelines will affect the consumer (retail, healthcare, and services) and industrial sectors, such as transportation, water, oil and gas, agriculture, and manufacturing. Security is a critical aspect to keep in mind as these IoT devices become a part of our daily lives.

The draft guidelines/code of practice for securing consumer Internet of Things (IoT) will affect IoT device manufacturers, IoT Service provider's/system integrators, IoT mobile application developers, component providers and consumers. The code of practice applies to all consumer IoT products connected to the Internet or the home network and associated services.

## The guidelines cover key issues on securing IoT, such as:

- Develop a secure way to store sensitive security parameters. These parameters should not be hard-coded or obfuscated as these methods can be broken by threat actors.
- Ensure the devices are easy to install and make it easy for the consumer to delete personal data if needed.
- Manufacturers and developer should try to minimize the attack surface.
- To keep the software updated till the end of the product's life cycle.
- The communication channel should be encrypted.
- All IoT devices should have unique default passwords and not universal default passwords such as 'admin' or 'password'. These kinds of default passwords are expected to be changed by the end-user. If the consumer doesn't change the password, it gives the attackers an easy way to hack into these systems.
- IoT manufacturers, system integrators and service providers should have a vulnerability disclosure policy for security researchers to report vulnerabilities and bugs and develop a mechanism for these vulnerabilities to be addressed promptly.

Source: https://www.tec.gov.in/pdf/Circular/Code%20of%20Practice_Consumer%20IoT_28.12.2020.pdf

# INDIA'S MOVE TOWARDS INTERNET REGULATION

## Intermediary Guidelines and Digital Media Ethics Code, 2021

The Digital India program has now become a development that is engaging Indians with the force of innovation. The digital revolution empowered numerous online media stages to extend their impressions in India.

Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, on February 25, 2021. Intermediaries are entities that store or transmit data on behalf of other persons like internet or telecom service providers, online marketplaces, and social media platforms.

As per the Indian Information Technology Act (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, MeitY will be responsible as a nodal agency to ensure compliance of Intermediary guidelines and Press Information Bureau for a publisher of news and current affairs content or a publisher of online curated content. The guidelines define the following activities to be carried out by the intermediaries:

### SOCIAL MEDIA

- Identify the 'first originator' of content that authorities consider anti-national.
- Appoint grievance officer to resolve complaints in 15 days.
- File monthly compliance reports on complaints received and action taken.

### DIGITAL NEWS

- Follow Press Council of India, Cable TV Networks (Regulation) Act norms.
- Self-regulatory bodies to oversee adherence to Code of Ethics.
- I&B Ministry to form a panel to oversight mechanism.

### OTT PLATFORMS

- Self-classify content into five age-based categories: U (universal), U/A 7+ (years), U/A 13+, U/A 16+, and A.
- Parental locks for any content classified as U/A 13+ or above.
- Age verification mechanism for content classified as 'A' (adult).

**A social media intermediary shall, within three months from the date of publication of these rules, observe the following additional due diligence:**

- Appoint a Chief Compliance Officer responsible for ensuring compliance with the Act and rules made thereunder.
- Appoint a nodal contact for 24x7 coordination with law enforcement agencies and officers to ensure compliance with their orders.
- Appoint a Resident Grievance Officer.
- Every six months, publish periodic compliance reports mentioning the details of complaints received and action taken thereon.

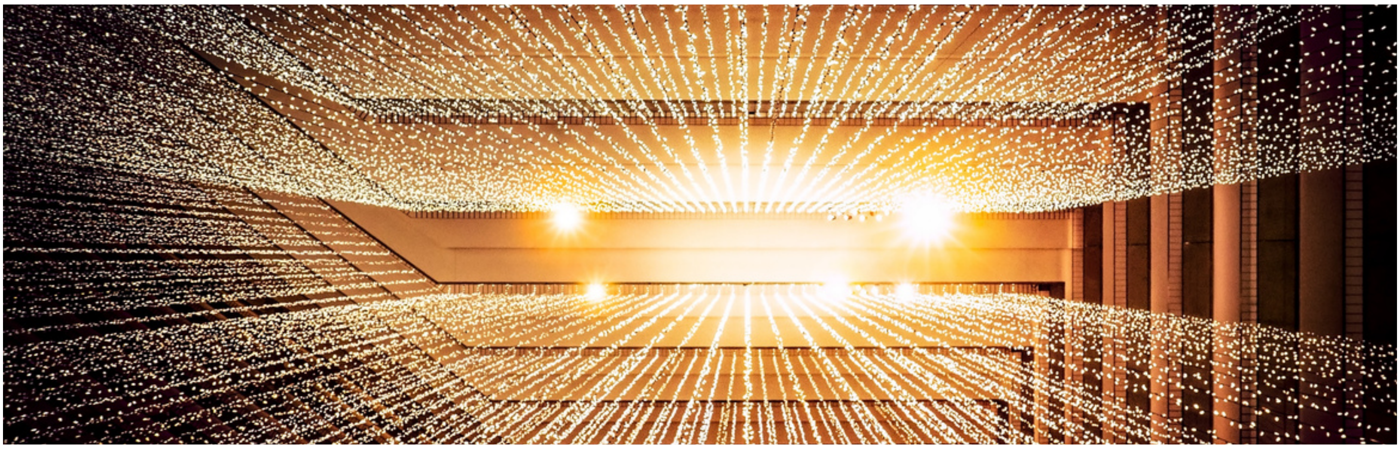
Intermediaries need to inform its users at least once every year, that in case of non-compliance with rules and regulations, it has the right to terminate the access or usage rights of the users.

Intermediaries shall inform their users of its rules and regulations at least once a year.

The intermediaries shall retain user information for 180 days after the cancellation of their registration.

Intermediaries shall take all reasonable measures to remove access to any content that is not suitable for the platform within 24 hours from the receipt of the complaint.

Source:https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf



# INDIA'S CYBER SECURITY STRATEGY

A national cybersecurity strategy (NCSS) is a collection of measures to enhance the protection and resilience of critical national infrastructure and services. A high-level approach to cybersecurity identifies a set of national goals and targets that must be met within a specific timeframe.

The Office of National Cyber Security Coordinator at the National Security Council Secretariat is responsible for preparing India's Cyber Security Strategy. Lt. Gen. (Dr) Rajesh Pant, appointed as Special Secretary to Government of India in 2019, spearheaded the initiative to prepare India's Cyber Security Strategy.

Data Sovereignty - A government has the first right to its citizen's data. The Government of India reserves the right to access locally stored data to protect national interests. The Personal Data Protection Bill, 2019 under Clause 35 exempts the government from seeking citizens' consent to access their data for national security purposes. This further mandates that in foreign attacks and surveillance on India's Cyberspace, digital companies will have to abide by Indian laws and assist the Indian Government's Defence policy.

Cyber Deterrence - Cybersecurity risks pose substantial threats to national security, public safety, and the economy. The deterrence mechanism will define how India will respond to cyber threats from malicious state actors and hacktivists.

Data Localisation - India adopted localisation norms for specific sectors deemed vital to the country's GDP, such as banking and financial services, which require the storage and processing of user data in data centres/servers located within the national borders.

Online safety of citizens - With India's rapid digitalisation government understands that exposure to online harms is increasing manifold for the vulnerable population. As a result, the Ministry of Home Affairs (MHA) Cyber and Information Security (C&IS) is allocated to safeguard citizen in cyberspace. Cyber skill development in India - The government of India recognises that Cyber Skill development is a crucial area of focus. The Cyber Security Strategy 2021 would highlight programs for cybersecurity skill development for important sectors for securing Indian information and communication technology infrastructure.

Securing Emerging Technologies - Emerging technologies like the Internet of Things (IoT) is aggravating the security threat for both consumers and businesses. Other emerging technologies like Artificial Intelligence, Machine Learning, and Robotics can introduce risks and vulnerabilities to India's cyberspace. The Cyber Security Strategy would propose Security by Design principles, Self-Assessment, 3rd Party Audits to secure countries' critical infrastructure.

# PRESS FREEDOM OR SCOURGE OF FAKE NEWS?

Freedom of speech and expression is a complex right as it may be subject to reasonable restrictions. It is not absolute and carries with it special duties and responsibilities. Media, mainly electronic, has become like an unruly horse that needs to be tamed as social media reach is much wider than traditional media. There've also been communal violence incidents in the country where social media was misused.

Fake news poses a severe threat to the freedom of media and national integrity. During the lockdown, there has been a marked increase in the circulation of fake news pushed through print, electronic, and social media such as Twitter, Facebook and WhatsApp. To counter such spread of fake news, a Fact Check Unit is formed in the Press Information Bureau (PIB) that started taking immediate cognizance of fake news, resulting in some platforms retracting these fake news items and placing facts before viewers and readers.

To combat the scourge of fake news and disinformation, promoting strong norms on professional journalism, supporting investigative journalism, reducing financial incentives for fake news, and improving digital literacy among the general public is necessary. Taken together, these steps would further quality discourse and weaken the environment that has propelled disinformation around the globe.

**Government responsibilities:** One of the most important things governments worldwide can do is encourage independent, professional journalism. The general public needs reporters who help them make sense of complicated developments and deal with the ever-changing nature of social, economic, and political events.

**News industry actions:** The news industry should continue to focus on high-quality journalism that builds trust and attracts greater audiences.

**Technology company responsibilities:** Technology firms should invest in technology to find fake news and identify it for users through algorithms and crowdsourcing. There are innovations in fake news and hoax detection applicable to media platforms. For example, fake news detection can be automated, and social media companies should invest in their ability to do so.

**Educational institutions:** Funding efforts to enhance news literacy should be a high priority for governments. This is especially the case with people who are going online for the first time.

**How can the public protect itself?**
Individuals can protect themselves from false news and disinformation by following a diversity of people and perspectives. Relying upon a small number of like-minded news sources limits the range of material available to people and increases the odds of falling victim to hoaxes or false rumours.

# INDIA-UK TRADE DEAL

The current trade between the UK and India is currently around £23 billion per year, creating over half a million jobs. The Prime Minister met with Indian business leaders from Infosys and HCL to discuss the rising importance of the UK-India economic partnership.

Indian Prime Minister Narendra Modi and UK Prime Minister Johnson held a virtual meeting for trade. They announced 1 billion pounds of private-sector investment. Both the nation leaders committed to seeking a free trade deal and creating over 6,500 jobs in vital and growing sectors such as health and technology in Britain. This includes agreeing on an Enhanced Trade Partnership. The collaboration will open new doors for British companies exporting to India and Indian companies investing in the UK.

- £200 million of these deals will support low carbon growth.
- £240 million investment by the Serum Institute of India in the UK into their vaccine business and a new sales office will create many jobs.
- British businesses have also secured new export deals with India worth more than £446 million. This includes CMR Surgical exporting its next-generation Versius surgical robotic system, which helps surgeons perform minimal access surgery being rolled out to hospitals in India.
- This export deal is worth GBP 200 million and will result in the creation of 100 new jobs in the UK.

# DRDO'S NEW COVID DRUG : A MIRACLE MEDICINE?

2-DG stands for 2-deoxy-D glucose, which is effectively modified glucose. This is the sort of glucose that has been used in anti-cancer and anti-viral treatments thus far. It should only be used as an extra treatment in moderate to severe COVID patients, according to the Defence Research and Development Organisation (DRDO). It should not be used in mild COVID patients.

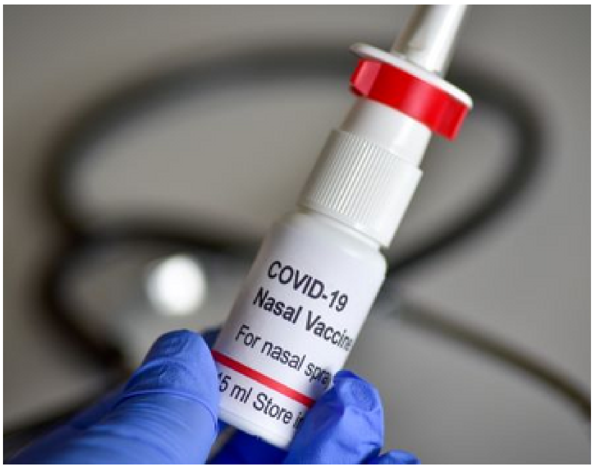
This medication was created in partnership with Dr Reddy's Laboratories (DRL) in Hyderabad by the Institute of Nuclear Medicine and Allied Sciences (INMAS), a lab of the Defence Research and Development Organisation (DRDO).

The medicine comes in a powder form in a sachet and must be taken twice a day for at least a week by dissolving it in water.

# NASAL VACCINATION

The Covid-19 pandemic has disrupted how the world used to work. The disproportional impact of the pandemic has affected many sectors and industries. In 2021, many vaccines were approved, and nations began their rollout. Currently, seven different vaccines have been rolled out.

These traditional vaccines are administered using injections. Now the recent development of nasal vaccines can be a game-changer. Nasal vaccines, unlike conventional vaccines, can be self-administered with nasal spray, with no need for syringes or needles.



## Nasal vaccination: A game changer?

The vaccines can be rolled out once approved. Bharat Biotech International Limited had sent a proposal to the Drugs Controller General of India (DCGI) for the Phase 1 trials of the nasal vaccines. The firm received approval for Phase 1 trials and conducted Phase 2 clinical trials of the intranasal vaccine.

Nasal vaccines are easier to administer. The vaccines can be rolled out once approved. Bharat Biotech International Limited had sent a proposal to the Drugs Controller General of India (DCGI) for the Phase 1 trials of the nasal vaccines. The firm received approval for Phase 1 trials and conducted Phase 2 clinical trials of the intranasal vaccine. Nasal vaccines, as compared to traditional vaccines, provide a low-cost implementation. Since the vaccines can be self-administered, a lot can be saved as nasal vaccines would not need syringes and other medical equipment to store and handle these vaccines.

Experts suggest that the effectiveness of nasal vaccines will be more than traditional or injected vaccines as they can be easily absorbed by blood vessels.

INDIA FUTURE
FOUNDATION

**India Future Foundation**

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com