All Things Internet

In this article, we will discuss all the major issues pertaining to the misuse, regulation and censorship of internet and social media platforms.

IF, someday after the doomsday, the history of modern human is written, the dawn of internet is definitely going to be the marker for the start of a new phase, with data stored in chips serving as archaeological evidences of the life that existed. No matter, how big a transformation internet has proved to be and how much benefit people are reaping out of it, there is no denying in the fact that issues associated with it have been a nightmare for the regulating authorities all over the world.

As the lines between public and private are getting blurred, the questions of identity, individuality and privacy are out in the public sphere for debate. In this section, we will be discussing some of the major issues concerning the internet, social media and its regulation which have been come into light in recent days.

1. Net Neutrality

Net neutrality is the principle that individuals should be free to access all content and applications equally, regardless of the source, without Internet Service Providers (ISP) discriminating against specific online services or websites. The user is free to access any web location at the same paid-for speed without any discrimination by the ISP.

Arguments in favour of Net Neutrality

- Net Neutrality democratizes the internet space as the telecom provider cannot charge differently for different websites and allows everyone on the internet to participate in it.
- It does not let Telecom providers or ISPs to act as “gatekeepers” and control, filter or block data according to their will without the court order.
- This provides a level playing field to all the big and small companies in IT sector and does not let a handful of companies control the internet.
- Ensuring that all people and websites have equal access to each other, regardless of their ability to pay, fosters the principle of freedom of speech.

Arguments against Net Neutrality

- Facebook and many companies have argues against Net Neutrality. Facebook has launched a campaign by the name of “Free Basics”. The arguments put forward were:
- Net Neutrality will stifle innovation on the internet as it won’t be possible to explore consumer choices and create content accordingly
- ISPs will not be able to make investment in Broadband services.
- It will make kill competition as every data packet will be treated the same and content providers will not get a chance to advance their data at a better rate by paying the telecom providers.

Net Neutrality in India

- The Department of Telecommunications accepted the TRAI (Telecom Authority of India) recommendations in favour of Net Neutrality which Bars Telcos from discriminatory treatment on the Web, based on content, sender, receiver, protocols or equipment
- Penalizes for violation of license rules on net neutrality
- Includes exceptions for critical services such as remote healthcare diagnostics, self-driving cars, some financial services etc.
- Exempts content delivery networks, which do not use public Internet from open web rules.

Net Neutrality in other countries

- **US:** The old law passed by Barack Obama government has been repealed and internet providers can now slow down or prioritise certain types of content over others.
- **Europe:** Internet providers can't block or slow down traffic but can manage traffic to comply with legal order, to ensure network integrity, security or manage congestion
- **Brazil:** Net neutrality exists, fast lane for some emergency services or blocking of spmas is allowed.
- **Australia:** Internet providers offer zero-rated content but cannot throttle or block competitors' content.

Thus, the principle of Net Neutrality acts as the custodian of democratic functioning of internet. It is important that it is upheld by the collective effort of the government and companies of IT sector.

2. Data Protection and Privacy

Internet (internet companies, online government databases etc.) has staggering amounts of information available about almost everyone of us. Every website we visit, search engines we use, and even products we buy, profiles us, or some part of us to say the least. With this, the concerns of our private information being shared by third parties, without our knowledge or consent and its use for commercial purposes have been raised again and again Most of the countries are trying to come up with legislation governing the extent to which the private data can be collected and used.

Issues with Data Protection:

Data Protection and Privacy: Data protection deals with data protection is about securing data against unauthorized access. Data privacy is about authorized access — who has it and who uses it. Data protection is essentially a technical issue, whereas data privacy is a legal one.

Fairness: It is important that the information is collected in a lawful and transparent manner. It needs to be ensured that the data is obtained with the consent of the user.

Repurposing: If the data obtained for one purpose is analyzed for some other purpose, which the user was not made aware of, then this is known as repurposing. Recently, Facebook was accused of selling data to a third party, Cambridge Analytica which repurposed Facebook user's data.

Unfair advantage in elections: The private data of citizens may be manipulated by political parties to gain unfair advantage in elections. The Democratic Party in the USA has been accused of using such means in the US presidential elections.

Cyber crimes: Data leaks may propagate cyber crimes, hacking, and leak of financial information like bank account details etc.

Surveillance capitalism: This term is used in reference to the monetization of personal data by the big companies for profit-making.Collecting and processing data in the context of capitalism's core profit-making motive might present an inherent danger.

Other issues which are associated with data privacy include selective profiling of individuals and witch-hunting, violation of consumer rights etc.

Data Protection Law in India

There is no specific data protection law in India. However, certain legislations can be used against breach of privacy like

- **The (Indian) Information Technology Act, 2000** deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in cases of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.
- **Section 43A of IT Act 2000** holds heads of the organizations handling personal data accountable for its unlawful disclosure.
- The Government has notified the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**. These Rules only deals with protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to passwords, financial information, physical, physiological and mental health conditions, sexual orientation, biometric information.
- **A.P. Shah Committee report:** This report recommended an overarching law to protect privacy and personal data in the private and public spheres.
- **Justice Srikrishna panel** is working on drafting a data-protection law for India.
- In the recent case of Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors., the constitution bench of the Hon'ble Supreme Court has held **Right to Privacy as a fundamental right,** subject to certain reasonable restrictions.
- **TRAI Recommendations**
    - Recently, TRAI announced that companies collecting user data have no primary rights over such data and emphasised that **consumers' consent should be made mandatory**. TRAI said it would like to see consumers being given the "Right to be Forgotten".
    - TRAI has also recommended regulation of all platforms that deal with consumer data — meaning devices, operating systems, browsers and apps — by including them in licence conditions that apply to telecom service providers until the time a general data protection law is in place.

Data Protection Laws around the world

- **European Union: General Data Protection Regulation (GDPR)** is a regulation on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It upgrades the erstwhile data protection law with stricter provisions regarding privacy of individuals, consent, and the “right to be forgotten”.
- **USA:** The US has sector specific data protection laws and regulations that work together with state-level legislation to safeguard American citizens’ data such as Federal Information Security Management Act (FISMA), NIST 800-171 etc.
- **Australia:** The Privacy Act 1988 (Privacy Act) is an Australian law which regulates the handling of personal information about individuals.

Big Data

Definition: Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. Big data is also defined as “high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making”

But it’s not the amount of data that’s important. It’s what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves. However, we still do not have tools to handle such a vast amount of data, notwithstanding the fact that many big organizations are betting to gain access to as much data as they can.

Why to use big data? The reasons why every company is inclined towards adopting big data?

1. **Timely —** Gain instant insights from diverse data sources
2. **Better analytics —** Improvement of business performance through real-time analytics

3. **Insights —** Can provide better insights into consumer choice and behaviour
4. **Decision-making —** Helps mitigate risk and make smart decision by proper risk analysis

Applications

- **Healthcare:** Big data is used extensively to store patients health history. This data can be used to analyse the patient's health condition and to prevent health failures in future.
- **Fraud detection:** Credit card companies face a lot of frauds and big data technologies are used to detect and prevent them.
- **Weather forecast:** Large amount of data on the climate is feeded to supercomputer based modelling software and results are taken to predict the weather. This can be useful to predict natural calamities such as floods, cyclones, etc.
- **Public sector:** Big Data is used in a lot of government as well as public sectors. Big data provides a lot of facilities such as power investigation, economic promotion, etc.
- Big Data is used in many other cases such as Education sector, Insurance services, Transportation, Security Intelligence, etc.
- Big data has become an important part for business analysis and is needed in order to understand the growth of businesses and to build strategies that help it grow.

3. Mob Lynchings and Fake News

In the recent times, India is facing yet another menace of internet, particularly social media, that is, fake news followed by mob lynchings. The number of cases involving mob lynchings as a result of rumours spread through whatsapp forwards is increasing day-by-day. While some feel that the social media platforms should be held accountable for not regulating the content circulated on them, some other are of the opinion that it is more of a law-and-order situation which needs to be curbed by the government.

Factors Responsible for Spread of Rumours and Lynchings

- **The class and community of victims**
  - Experts point out that victims are usually "soft targets"who are outsiders or come from the marginalized section.
- **The background of perpetrators**
  - Most of the perpetrators of these kinds of violence are jobless or daily-wagers, ill-educated youth.
  - Unemployment serves as a factor that lead to criminal bent of mind.
  - Also, these youth are not educated enough to differentiate between fake and real news and are thus more prone to be carried away by hate-mongering news.
- **Lack of active interference by the state**
  - The political leaders have not been openly and quickly condemning such instances sets out a signal to the administration and people at large that such acts are "acceptable".
- **Change in the structure of the society**
  - Sociologists and mental health experts point out that there has been a change in the societal set-up, from a traditional and inclusive one to that smitten by fear and hate.
- **Lack of media literacy**
  - Media literacy encompasses the practices that allow people to access, critically evaluate, and create media. This also includes the ability of people to form opinion on the basis of certain news.
  - Presently, lack of media literacy is one of the important reasons which lead people into believing fake news and rumours.
- **No-anti lynching law**
  - At present, India does not have a law that criminalizes mob-lynchings.
  - Section 223 (a) of the Criminal Procedure Code (CrPC) can be used to prosecute together two or more people accused of the same offence committed in the course of the "same transaction", but the extent of its applicability is limited.
- **Difficulty in tracing instant messages**

    - For messaging services other than Whatsapp, the information is with the parent server and police have to request the company for access to information, such as IP addresses, for investigation.
    - However, it is most difficult to trace messages on Whatsapp as everything on the platform is encrypted end-to-end at the device level — all data is stored on the device and not on servers.
    - Also, the metadata on Whatsapp is stripped (i.e.All data about other data of all personally identifiable information such as username, device info and log-in time is removed by Whatsapp).
- **Limited Legal liability of messaging platforms**
    - Experts point out that in the existing legal framework, Whatsapp is not bound to comply with government directive as:
        - It is a non-licensed app and does not operate on any telecom or internet regulatory license which can be revoked if it fails to comply with government directives.
        - It does not have servers in India and is thus not bound by Indian Laws.

In other countries:

- **Germany:** Passed anti-fake news laws
- **Malaysia:** Enacted Anti-Fake Act
- **China:** Heavily censors the internet in order to combat fake news.
- **Singapore and Philippines:** In the process of coming out with laws penalising those spreading misinformation.
- **Brazil:** Whatsapp works with news organisations to fact-check messages.
- **Mexico:** Whatsapp verifies messages during elections.

What can be done?

- **The responsibility of the law-enforcement agencies**
    - Since, mob-violence is a product of politics, mobilizations and protection by some powerful vested forces, it is the primary responsibility of the state to control such hate-mongering elements in the first place.
    - Shutting down internet or enforcing impositions on what-can-be-said will be a violation of freedom of speech. Therefore, there is a limit to which social media platforms can be controlled.
- **Accountability of Social Media**
    - **Unique ID for public Messages:** WhatsApp needs to change its platform to enable messages to be either public or private. Messages between individuals should remain private and not be those that can be forwarded. However, if a message creator wants to enable the forwarding ability of that message, the chat should be treated as public, and attributed with a unique ID linked to the original creator. This will allow WhatsApp to shut down such a messages across its network once it is reported, and identify the creator when a court-directed request is made by law enforcement agencies.
- **Apart from this, the following steps can be taken:**
    - The government needs to invest much more resources into education, of children and adults alike, especially in media literacy.
    - Campaigns and awareness programs focussed on getting people to respect other communities, not believing WhatsApp rumours and fake news, should be carried out.
    - It should be ensured that the investigative agencies and local administrations are free of political pressure while investigating such sensitive cases.
- From the increasing instances of mob-lynchings across the country, it is imperative that government takes instant steps to curb such incidences. The mob-lynching events are more of a law and order concern than technological. But above all, to change the dehumanizing mindset of mobs, it is the society as a whole who needs to educate itself and move away from the retrogressive path towards ‘barbarism’.

Other issues

4. Revenue sharing

It has been argued that search engines like Google take most of the revenue generated by the audience away from the original content created by non-Google entities such as news organisations. This may lead to revenue crunch for content creators and will act as a setback for innovation in terms of content.

5. Pornography and other unadvisable content

There has been a lack of internet censorship laws and mechanism that prevent users upto a certain age from using particular websites. Although, a certain amount of censorship is there but it is easily bypassed by the creators and users alike.

The age of internet is marred with technological as well as legal impediments that needs to be addressed by the governments of the world collectively as this issue has transgressed boundaries of nations. We need to come up with a global system of regulating content on internet so, that it can be utilized in the best interest of the public.