

IKIGAI LAW

Crimes in Social Media: Law, Regulation and Policy

Aman Taneja, Principal Associate

Background

- Online platforms have a global presence as the internet is not bound by the traditional understanding of jurisdiction.
- This is why attempts to regulate online platforms in one country have a tangible impact on how other countries approach their regulation.
- Governments across the world are trying to determine the role that online platforms can and/or should play to protect users' free speech and remove unlawful content.
- They have enacted or are in the process of enacting revamped laws to suit the changing landscape of the internet.
- In this session we will cover:
 - Evolution of laws around social media in India and the motivation behind these interventions
 - Some laws applicable to some specific online crimes and practical challenges faced by platforms and law enforcement

IT Act, 2000

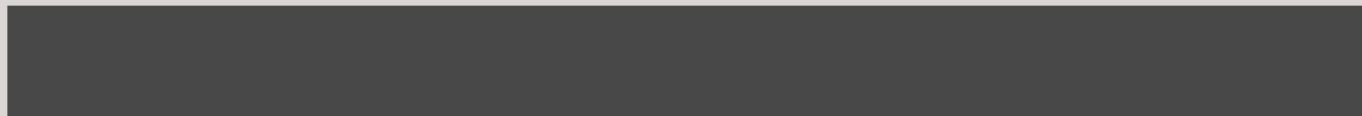
- The Information Technology Act, 2000 (IT Act) was enacted to recognise electronic data transactions including electronic communication, electronic commerce etc.
- Has extraterritorial application
- Defined terms such as computer network, digital signature, private key, public key, a breach of confidentiality and privacy
- A number of offenses – tampering with computer documents; loss or damage to computer resources; publishing of obscene materials in electronic method; failure of companies to assist in decrypting the information intercepted by the government; unauthorized access to computer system, and breach of confidentiality

Amendments to the IT Act, 2000

- IT Act was amended significantly in 2008. The amended act introduced more criminal offenses and amended the safe harbor protection
- The 2000 IT Act had only 10 chapters with limited coverage of cybercrimes: Criticisms were also raised about the lack of attention to cybercrimes against women and children.
- Newer forms of cybercrimes – identity theft, cheating by impersonation, cyberterrorism, publishing or transmitting obscene materials, publishing or transmitting sexually explicit materials, or depicting children in sexually explicit acts – were included in the 2008 ITAA
- Failure to maintain “reasonable security practice and measures” body corporates could receive not only civil penalties but criminal sanctions as well

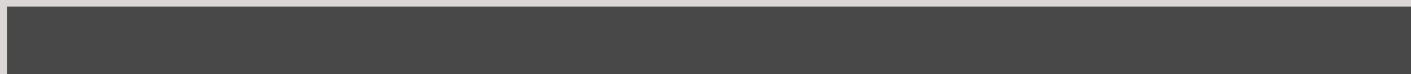
Amendments to the IT Act, 2000 (Cont)

- Safe harbour provisions were amended in 2008, following the Bazeem.com case in 2005,
 - Avnish Bajaj, the CEO of Bazeem.com (an online auction website modelled on eBay.com) , was arrested after an obscene video clip was listed for sale on the website.
 - Bazeem.com did not create the video clip, nor did it publish the listing. It was posted by a user.
 - Industry called for inclusion of safe-harbour protections in the IT Act following this case.
- The Information Technology (Amendment) Act, 2008 defined “intermediary” at Section 2(w) – , with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;



Safe-harbour protection for intermediaries

- Section 79 amended to grant safe harbour protection to intermediaries, if they –
- Only provide access to a communication system
- Do not
 - initiate the transmission,
 - select the receiver of the transmission, and
 - select or modify the information contained in the transmission.
- Observe due diligence while discharging their duties, including compliance with any other government issued guidelines
- Do not conspire, abet, aid or induce the commission of an unlawful act
- Expeditiously remove/disable access to any content hosted on the platform if,
 - They receive actual knowledge of such content.
 - Are notified by the appropriate Government or its agency



2011 intermediary guidelines

- The Information Technology (Intermediaries guidelines) Rules, 2011 (2011 Rules) specify the due diligence requirements that intermediaries must follow to qualify for safe-harbour protection provided in Sec. 79 of the IT Act
- Intermediaries are required to –
 - Take down unlawful content within 36 hours of receiving written notice regarding such content.
 - Extend support to law enforcement agencies, report cyber incidents to the appropriate authority and take reasonable measures to secure their platform.
 - Publish rules, privacy policies, terms of use and contact details of a grievance officer on the platform. Rule 3(2) specifies certain types of content that should not be published by the user on the platform.
 - Inform users that non-compliance with platform rules will result in termination of their accounts.
- Rule 3(2) identifies a specific list of content that users cannot post. This includes stolen content, sexually explicit, illegal, deceptive and false content, threatens the unity, integrity, defence, security and sovereignty of the nation among others.

Intermediary liability clarified

- In 2015, the Supreme Court in *Shreya Singhal v. Union of India* clarified key aspects of how Section 79 and the 2011 Guidelines should be interpreted.
- Rule 3(4) which states that - "the intermediary (...) upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature (...) shall act within thirty six hours (...) to disable such information that is in contravention (...)" were challenged.
- Petitioners argued that Rule 3(4) requires intermediaries to exercise their own judgment in determining if content is unlawful, and they would cease to be neutral platforms.
- The Supreme Court held that "actual knowledge" is only obtained when an intermediary receives a court order/official notification from the government.
- The court order/government notification should satisfy the exceptions to the fundamental right to free speech and expression in Article 19(2) of the Constitution of India.

2018 draft intermediary guidelines

- In 2018, then IT Minister R.S. Prasad spoke about the need for careful regulation of social media platforms in the aftermath of –
 - Violent mob lynchings and communally-charged attacks, triggered by fake news on social media like WhatsApp.
 - The Facebook - Cambridge Analytica data mining scandal raised concerns over social media platforms influencing election outcomes in India.
- The IT Ministry proposed amendments to the 2011 Rules, the 2018 draft rules required intermediaries to –
 - Bar users from posting content that threatens public health and safety, such as e-cigarettes, cigarettes and tobacco products.
 - Inform users at least once a month that failure to comply with the platform's rules and policies will result in their account being terminated.
 - Assist law enforcement agencies with any lawful order for information within 72 hours.
 - Be incorporated in India and appoint a local nodal contact person and alternate senior functionary to liaise with the government if they have > 50 lakh registered Indian users.
 - Take down content within 24 hours of a lawful order/government notification and retain records for a period of 180 days.
 - Deploy tools to proactively identify and remove unlawful content.
- Civil society organisations, companies and free speech advocates criticised the 2018 draft rules for being overbroad and that it recommends a one-size-fits-all solution to a complex problem.

2021 intermediary guidelines

- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (2021 Rules) came into force in May, 2021.
- They replace the 2011 Rules and govern internet intermediaries through the IT Ministry and OTT platforms and digital news publishers through the Ministry of Information and Broadcasting.
- Key changes include –
- Definition for “social media intermediary” as an intermediary which primarily or solely enables interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services
- Enhanced obligations on a special category of intermediaries with > 50 lakh users called significant social media intermediaries (SSMIs). These include –
 - Quick removal of “revenge porn” type content
 - Appointment of a separate chief compliance officer, who will be personally liable for non-compliance and a nodal contact officer to liaise with law enforcement agencies.
 - Tracing the first originator of a message for the purposes of ‘prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State’ etc.
- All intermediaries must comply with certain due diligence obligations such as
 - Publishing rules, privacy policies, terms of use etc.,
 - Taking down content within 36 hours of receiving actual knowledge from a judicial/government authority and taking down content which is in the nature of ‘non-consensual transmission’ of sexually explicit content, including morphed images, within 24 hours of the receipt of a complaint from the affected person.
 - Assisting law enforcement with requests for information within 72 hours.
 - Reporting cybersecurity incidents to the Indian Computer Emergency Response Team or CERT-IN.
 - Appointing a grievance redressal officer who must acknowledge complaints within 3 days and resolve them within 30 days.
 - Maintaining logs for 180 days.
- Part III of the rules sets out a code of ethics for OTT platforms and other entities. It also prescribes a three-tiered grievance redressal system comprising of self-regulation at the lower levels and oversight by the Ministry of Information and Broadcasting.

FAQs on Part II of the 2021 Rules

- FAQs on Part II of the 2021 Rules were released by the IT Ministry to clarify definitions, processes for compliance and specify the government's intent behind them.
- B2B entities are exempt from the definition of social media intermediary as SMLs must –
 - Enable online interaction as a core purpose.
 - Facilitate socialization with features like 'follow', 'subscribe' and allow interaction with unknown users.
 - Allow for 'virality' of content by allowing rapid sharing of content on their platforms.
- The 2021 Rules were drafted in response to
 - Key Supreme Court decisions such as In Re: Prajwala (on sexually explicit videos online) and the right to privacy case, among others.
 - The growth and influence of online platforms
 - International developments on the regulation of online platforms.

Amendment to the IT Rules 2021

- Earlier this year in June the MeitY released amendments to the IT Rules 2021 and sought comments to fill the gaps identified in the Rules. The amended rules came into force in October, 2022.
- The due diligence obligation under Rule 3(1)(b) has been changed down. Earlier, the clause required intermediaries to cause users to not publish certain categories of objectionable content and now the obligation is to make “reasonable efforts” towards this duty
- Intermediaries are to take all reasonable measures to ensure accessibility of its terms of services
- The amendment introduces the Grievance Appellate Committee (GAC). A user aggrieved by an order made by the Grievance Officer can appeal to the GAC within 30 days. The GAC has to dispose of the appeal within 30 days.
- The GAC shall consist of Union Government appointed public officials for adjudication of any appeals against the decision of social media platforms to remove or not remove content. However, any further details on their appointment process, qualifications and the quorum of the committee is absent.

Current status of the law

- Nearly 17 challenges to the Rules before various High Courts were transferred to the Supreme Court.
- Key issues in the challenges are –
 - Breaking of encryption to trace the originator of messages
 - Chilling effects on free speech
 - The manner in which rules introduced
 - The treatment of digital publishers among several others.
- Interim stay on Part III of the 2021 Rules granted by the Bombay High Court, Madras High Court and Kerala High Court will continue until further notice.
- SMIs are complying with other provisions such as publishing monthly reports.



Social Media Harms that need to be regulated

- Variety of harms for users on social media that need to be addressed and should be criminalised.
 - Hateful and Xenophobic Content
 - Content promoting violence or incitement to violence
 - Incitement to committing criminal offenses
 - Suicide and self-injury
 - Child sexual exploitation, abuse and nudity
 - Adult sexual exploitation
 - Cyber enabled Violence against Women and Girls
 - Bullying and harassment
 - Privacy violations
 - Fraud and deception
 - Respecting intellectual property

Crimes linked to Social Media in India

- **Obscenity, Child Pornography and Sexually Explicit Materials**
- **IT Act**
- Section 66A - Punishment for sending offensive messages through communication service, etc - Declared unconstitutional by the SC in *Shreya Singhal v. Union of India*
- Section 66E - Punishment for violation of privacy
- Section 67 - Publishing or transmitting obscene material in electronic form
 - Standard for determining obscenity has been criticised for being paternalistic and vague which allows judges to adjudicate based on their personal dispositions and value sets
- Section 67 A - Publishing or transmitting of material containing sexually explicit act, etc.,
- Section 67 B - Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

Crimes linked to Social Media in India

- Offences against the confidentiality, integrity and availability of computer data and systems
- IT Act
- Section 72 - Penalty for breach of confidentiality and privacy
- Section 72A - Offence of disclosure of information in breach of contract
- Both of these sections focus on only the disclosure of information and not any other possible data protection harm. No data protection law that would ensure would capture a range of violations of data protection best practices

Crimes linked to Social Media in India

- **Computer-related offences with the intention to defraud or deceive**
- **IT Act**
- Section 66 - Computer related offences.
- Section 66C - Punishment for identity theft
- Section 66D - Punishment for cheating by impersonation by using computer resources
- **IPC**
- Section 420 - Cheating
- Section 463 - Forgery
- Section 468 Forgery for the purpose of cheating
- Section 469- Forgery for purpose of harming reputation
- Section 471 - Using as genuine a forged document or electronic record
- Section 500 - Defamation

Crimes linked to Social Media in India

- Law concerning hateful and xenophobic content and content promoting violence or incitement to violence
- IPC
- Section 153 - Wantonly giving provocation with intent to cause a riot
- Section 153A - Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc.
- Section 295A Deliberate and malicious acts intended to outrage religious feelings of any class, by insulting its religion or religious beliefs
- Section 505 - Statements conducing to public mischief
- **Hate Speech is not criminalised itself rather it is pigeonholed into other provisions of the IPC including Section 295A and 153A. These sections and the interpretation given to these sections have been criticised for being stifling free speech and being overbroad.**

Crimes linked to Social Media in India

- **Blackmail, Harassment, and Sexual exploitation**
- **IPC**
- Section - 354A Sexual harassment and punishment for sexual harassment
- Section 354C Voyeurism
- Sec.354D - Cyber Stalking Women
- Section 503 - Criminal Intimidation
- **The absence of specific legislation regulating new harms such as cyberbullying and trolling**

Crimes linked to Social Media in India

- **Blackmail, Harassment, and Sexual exploitation**
- *State of West Bengal v. Animesh Boxi*, GR No. 1587 of 2017
- The accused, and victim were in a relationship and during the relationship, Boxi demanded intimate photos from the victim and allegedly “hacked into her phone “to get his hands on them. He then blackmailed the victim. Later the videos were uploaded on porn websites.
- Judgement: Concerning the charges of sexual harassment, voyeurism, stalking and criminal intimidation under sections 354 and 509 of the IPC, the Court said that Boxi had demanded sexual favours from the victim, captured images of her in circumstances where she would not have expected to have been observed and stalked her thoroughly online.
- The Court held that for sexual harassment, voyeurism, and stalking injury to the victim’s reputation was sufficient’
- The Court also found Boxi guilty of transmitting private images online contrary to Section 66E, Section 67 and 67A of the IT Act as well as identity theft under Section 66C as he had hacked into the victim’s phone and taken the pictures secretly.

Power of law enforcement agencies to conduct an investigation and to prevent the commission of offences under IT Act

Power of law enforcement to collect evidence and investigate

Section 78 - Power to investigate offences

Section 69 - Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

This section is supplemented by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 that provide for safeguards

The 2009 rule provides for a review committee but the efficacy and institutional capacity of the committee is suspect as the review committee that meets once over two months has the "unrealistic task" of in-depth reviewing more than over 18000 orders (BN Srikrishna Data Protection Committee Report)

Section 69 has been challenged in the Supreme Court by multiple petitions which were filed in 2019.

Section 80 - Power of police officer and other officers to enter, search, etc

Section 80(3) - IT Rules is lex specialis to the CrPC

Section 91 CrPC often used as a tool to ask for content takedowns

Power of law enforcement agencies to conduct an investigation and to prevent the commission of offences under IT Act

Power of law enforcement to restrict content and block public access to computer resources

IT Act - Section 69A

The provision is supplemented by the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules, 2009.

Despite the Rules there are multiple instances of abuse of this provision and the intermediaries arbitrarily blocking public access to computer resources.

The Section and the accompanying rules are constitutional (Shreya Singhal v Union of India)

Before an order is passed for restriction of content under the section if the "person" i.e., the originator is identified he must be given hearing and relevant material to prepare (Shreya Singhal v Union of India and Tanul Thakur v. Union of India).

Questions?