The Dialogue™

INFORM ENGAGE IDEATE

ANALYSING THE AMERICAN SAFE HARBOUR REGIME: TAKEAWAYS FOR INDIA

The Dialogue™
INFORM ENGAGE IDEATE

Analysing the American Safe Harbour Regime: Takeaways for India

December 2020

Authors: Shruti Shreya and Pranav Bhaskar Tiwari
Editor: Kazim Rizvi

The Dialogue™
INFORM ENGAGE IDEATE

Table of Contents

List of Cases

American Cases

Elrod v. Burns, 427 U.S. 347 (1976)

Cubby, Inc. v. CompuServe, Inc, [1991] 776 F. Supp. 135 (S.D.N.Y.)

Stratton Oakmont, Inc. v. Prodigy Services Co., [1995] INDEX No. 31063/94

ACLU v. Janet Reno (June 11, 1996)

Woodhull Freedom Foundation et al. v. United States, 2020 WL 398625 (D.C. Cir. Jan. 24, 2020)

Indian Cases

Brij Bhushan v. State of Delhi, 1950 AIR 129

Avinash Bajaj v. Union of India, [150 (2008) DLT 769]

Sabu Mathew George v. Union of India, [WP(C) 341/2008]

Kamlesh Vaswani v. UOI [W.P.(C) No. 177/2013]

Shreya Singhal v. Union of India, (2013) 12 SCC 73

Re: Prajwala, SMW (Crl.) No(s).3/2015

Re: v. State of Uttarakhand, WP (PIL) No. 158/2018

Ms. X. v. State and Ors., WP (Crl.) No. 1080/2020

Janani Krishnamurthy v. UOI, WP 20214/2018

Swami Ramdev and Anr. v. Facebook Inc. and Ors., C.S. (O.S.) No. 27 of 2018

List of Figures

Index of Abbreviations

ADHD	Attention Deficit Hyperactivity Disorder
CDA	Communications Decency Act
CSAM	Child Sexual Assault Material
E2EE	End-to-End Encryption
EARN IT Act	Eliminating Abusive and Rampant Neglect of Interactive Technologies Act
FOSTA	Fight Online Sex Trafficking Act
IL Guidelines	Intermediary Liability Guidelines
ISPs	Internet Service Providers
IT Act	Information Technology Act, 2000
LAED	Lawful Access to Encrypted Data Act, 2020
LEA	Law Enforcement Authorities
NCMEC	National Centre for Missing and Exploited Children
NCRB	National Crime Records Bureau
NGO	Non-Government Organisation
OTT	Over-the-top Platforms
PDP Bill	Personal Data Protection Bill, 2019
POCSO	Protection of Children from Sexual Offences Act, 2012
PTSD	Post-traumatic Stress Disorder
SESTA	Stop Enabling Sex Traffickers Act
TRAI	Telecom Regulatory Authority of India
UOI	Union of India
USA	United States of America
v.	Versus

Acknowledgement

We would like to thank Ms. Maanya Vaidyanathan, Research Fellow, AI for Peace, for her valuable inputs and support towards shaping this study. We are extremely grateful to Ms. Riana Pfefferkorn whose work at Stanford Center for Internet and Society and her inputs during our stakeholder consultation have informed this study.

Special thanks to Mr. Joan Barata, Non-Residential Research Fellow, Stanford Center for Internet and Society for his valuable insights and other key discussants of our consultation on safety issues, whose views have helped in shaping The Dialogue's research in this area. We also extend our gratitude to Mr. Abhinav Kashyap for the thematic designing of the report.

Grant for this study is supported by Facebook, India.

Executive Summary

Technology has made it easier for citizens from marginalised backgrounds to voice their concerns publicly, however some people are using these technologies to harass innocent people especially those who belong to underprivileged and marginalised communities. With the vices like Child Sexual Abuse Material (CSAM) and non-consensual adult content spewing across platforms, the proposal for technological solutions towards eradicating such content has been gaining traction. An integral part of this debate revolves around the role and liability of intermediaries including the network service providers, online marketplaces, search engines and payment sites.

However, every attempt of internet regulation must be balanced against the right to privacy and free speech, which are the key fundamental rights available to the citizens of any democratic state. This report sheds light on the US experience of Platform Regulation beginning from the evolution of the safe harbour regime to the recent legislative developments designed to curb the Online Safety challenges by limiting the ambit of safe harbour protection accorded to the internet intermediaries. This is also accompanied by an examination of the real-life implications of these developments and the takeaways for India from this experience.

The report envisages the inception and growth of the internet and its significance in facilitating right to freedom of speech and expression for people in general, and members of the marginalised communities in particular. This is followed by a discussion of the intermediary liability regime in the US beginning from the enactment of Section 230 Communications Decency Act, to the recently enacted SESTA-FOSTA legislations, and the proposed EARN IT and LAED Acts which seek to limit the ambit of safe harbour protection accorded to the intermediaries by way of creating overarching legislations. The objective of this discussion is to understand the socio-economic impact of these legislative interventions and the need for the same despite appropriate federal laws already existing to combat the challenges of online safety.

This is followed by a juxtaposition of the US intermediary liability experience upon the recent trends witnessed in the Indian safe harbour regime and by examining the key takeaways that India can have from the US experience, to build a robust intermediary liability framework that is steered

towards the objective of promoting user safety without compromising with the fundamental rights of the citizens.

The American experience explicates that compromising privacy and free speech to promote online safety does not render the desired results and in turn undermines the freedom and inclusivity on the internet. The Draft IL Guidelines, in their current form, as envisaged by the Indian Government, may cause more challenges than it seeks to resolve. It is very clear from the American intermediary liability experience that over-regulating the space is not the solution. The need of the hour is to deploy evidence-based research, on areas of policy implementation, meeting enforcement gaps, as well as acting on pending complaints, without over-regulating a space which may end-up creating new challenges that threaten both speech and privacy of the users. Online Safety and Privacy are two sides of the same coin, one cannot be ensured while compromising the other. To this end, it is crucial to ensure privacy of the users on online platforms and focus on effective investigation and timely prosecution in cyber-crime matters in order to truly realise the objective of a 'safe for all' internet ecosystem.

1. Introduction

1.1 Background

The rapid adoption of the internet and its impact on the rights of individuals and the economy lead to the creation of 'safe harbour' provisions, to protect internet intermediaries from liability against 'third party content' on their platform in the absence of 'actual knowledge'. The Indian safe harbour provisions under S. 79 of the Information Technology Act (IT Act) is modelled on S. 230 of the American Communications Decency Act (CDA).[1]

With increased accessibility of internet-based technologies, the intermediary liability regime both in the US and in India have witnessed new challenges, especially on the issue of ensuring child safety on online platforms. The two largest democracies in the world, both of which recognise the fundamental right to privacy and free speech, are facing multiple challenges and have been grappling to ensure safety of the users in general and safety of children in particular on online platforms. This paper analyses the American experience of tackling the safety challenges based on existing literature and carves out lessons and key takeaways for the regime in India.

1.2 Methodology

This report is the result of literature review based on the inputs gathered from the stakeholders during the roundtable discussions conducted by The Dialogue on user safety on the online platforms in 2020. The suggestions brought to the table by the discussants were read in light of the available literature to understand the American intermediary liability regime, and the challenges emerging in the recent years owing to the attempts to create overarching exceptions to the safe harbour provisions. Accordingly, the American experience has been juxtaposed alongside the Indian internet governance regime to draw ideas that India can utilise to build a robust intermediary liability ecosystem, that is steered towards the goal of promoting online safety without compromising with the democratic rights of privacy and free speech of the users.

[1] Ikigai Law (2019, Nov. 12) Intermediary Liability: Evolution of Safe-Harbour Law in India (Part I), *Ikigai law, retrievable from* https://www.ikigailaw.com/intermediary-liability-evolution-of-safe-harbour-law-in-india-part-i/#acceptLicense.

2. Safe Harbour and Safety Regulations in the US and India: A Robust Framework for Countering Crimes Against Children

The intention of the safe harbour provisions is to promote the development of an open internet ecosystem and encourage innovation[2], without letting go of the scope to allow reasonable checks in the interest of user safety through appropriate legislations. It is in light of this fact that governments across the world create robust regulatory mechanisms towards promoting online safety.

In order to control the proliferation of Child Sexual Abuse Material (CSAM), S. 2258A of Chapter 110 of Title 18 of the U.S. Code limits the ambit of S. 230 CDA. Legislated with the objective of protecting child rights on digital platforms, this federal law criminalises everything related to viewing, possessing, receiving and transmitting CSAM.[3] This provision read with S. 230 CDA strikes a careful balance between *'enabling the pursuit of justice'* and *'promoting free speech and innovation online'*. This is ensured by imposing a duty on the intermediaries to compulsorily report CSAM in order to continue enjoying the safe harbour immunity, however, this liability is only limited to cases when the intermediaries have an 'actual knowledge' of such content existing on their platform.

In India, Rule 11 of the recently notified Prevention of Children from Sexual Offences (POCSO) Rules, 2020 under the POCSO Act creates a similar exception to S. 79 of the IT Act in order to check the proliferation of CSAM. It directs the intermediaries to hand over all the material or information relating to CSAM it has received, including the source, to the extent possible, from which it was generated, the details of the device in which it was noticed, and suspected device

[2] Bambauer,D.E (2020, Jul. 1) How Section 230 reform endangers Internet free speech, *Tech Stream, retrievable from* https://www.brookings.edu/techstream/how-section-230-reform-endangers-internet-free-speech/.

[3] Pfefferkorn,R. (2020, Jan. 30) The EARN IT Act: How To ban End-To-End Encryption without actually banning it, *Centre for Internet and Society,* Stanford Law School *retrievable from* *http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it* .

from which it was received to the Special Juvenile Police Unit.[4] This rule should be read in light of the limited liability regime created by the *Shreya Singhal* judgment to ensure child safety without compromising with the fundamental right to privacy and free speech of the citizens.

Figure 1

ANALYSING THE CHALLENGES IN THE INDO-US INTERMEDIARY LIABILITY REGIMES

AMERICAN LAW			PROPOSED INDIAN LAW	
LEGAL PROVISION	CHALLENGE	FUNDAMENTAL RIGHTS INFRINGED	CHALLENGE	LEGAL PROVISION
S. 4 of EARN IT Act	Vaguely worded & envisages an unconstitutionally broad list of 'Best Practices' leading to a chilling effect on free speech	Fourth & Fourteenth Amendment Right to Privacy & Equality & Equal Protection of Laws Art. 21 & Art. 14	Envisages an arbitrarily broad list of 'Unlawful Materials' leading to a chilling effect on free speech	Rule 3 (2) of Draft IL Guidelines 2018
S. 6 of EARN IT Act	Compelling Intermediaries to adopt Proactive measures to check CSAM	First Amendment Right to Freedom of Speech & Expression Art.19	Mandates deployment of Automated tools for identifying, or removing or disabling access to unlawful information or content	Rule 3 (9) of Draft IL Guidelines 2018
S. 4 of EARN IT Act	Mandating intermediaries to identify originator of information by empowering them to search user accounts and that too without a warrant based on probable cause	Fourth Amendment Right to Privacy & Personal Liberty Art. 21	Mandates Traceability requirement to identify originator of information	Rule 3 (5) of Draft IL Guidelines 2018
S. 202 of LAED Act	Mandates every communication service with more than 1 million active users in U.S. to provide access to encrypted data to LEAs - Yardstick of 1 million remains unexplained.	Fourteenth Amendment Right to Equality & Equal Protection of laws Art. 14	Absence of 'reasonable classification' of Intermediaries	Rule 3 of Draft IL Guidelines 2018
S. 301 of LAED Act	Overarching powers to Attorney General undermining the Right to Equality & Privacy of the citizens	Fourth & Fourteenth Amendment Right to Privacy & Equal Protection of Laws Art. 21 & Art. 14	Excessive powers to the Union Government violating the citizen's Fundamental Rights to Equality & Privacy.	Rule 3 (2) and (7) of Draft IL Guidelines 2018

[4] Rule 11, Protection of Children from Sexual Offences Rules, 2020.

3. Diluting Safe Harbour to Achieve Safety: A Counterproductive Approach

We are witnessing a growing appetite within the regimes in both the US and India to impose stricter regulations on intermediaries, to cater the challenges of CSAM, despite the existence of adequate regulatory mechanisms as evidenced from S. 2258 A of the Federal Law in the US and Clause 11 of the POCSO Rules in India.

It is indeed crucial to keep checks on the intermediaries and ensure that they are taking adequate steps and uniform measures to check the proliferation of CSAM on their platforms. At the same time, it is essential to steer away from over-regulation that might harm the spirit of the 'safe harbour regime' which is necessary for ensuring an open and free internet.

The American regime has legislated the Fight Online Sex Trafficking Act (FOSTA), The Stop Enabling Sex Traffickers Act (SESTA), Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) despite existing Federal laws to cater to the challenges pertaining to Child Safety. The FOSTA-SESTA is broadly worded and instead of protecting the victims of sex trafficking, ends up prosecuting websites that help them connect with their family.[5] Similarly, the EARN IT or the Lawful Access to Encrypted Data Act (LAED Act) entail unreasonable restrictions on right to free speech and privacy in the endeavour to ensure child safety.

While it is important to note that the Government wants to do more to protect children and minors, it is also important to ensure that the efforts are not misguided. These efforts need to be focused, via evidence-based research, on areas of policy implementation, meeting enforcement gaps, as well as acting on pending complaints, without over-regulating a space which may end-up creating new challenges that threaten both speech and privacy of the users.

[5] Blunt and Wolf (2020, Apr. 27) *Erased: The impact of FOSTA-SESTA and the removal of Backpage,* Hacking Hustling.org *retrievable from* https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/ .

3.1 FOSTA-SESTA

FOSTA-SESTA limits the protection accorded by S. 230 CDA, leading to a disproportionate impact on online free speech. The Acts birthed in the backdrop of a lawsuit filed against a 'classified' website *Backpage.com* on charges of facilitating illegal sex work.[6] Initially, the Court dismissed the matter, citing S. 230 CDA. In response, the US Congress passed the FOSTA-SESTA Acts, however as scholars explicate, *"in passing these bills, the lawmakers failed to separate their good intentions from a bad law"*.[7]

Later Backpage and its creators were found guilty of editing and helping in creation of the illegal advertisements and the victim's lawsuit was allowed to proceed on the ground that she had discharged her initial burden of proof to show that Backpage was not merely acting as a conduit for the advertisements but was actively involved in their creation.[8] Hence, the website could not claim the defence of S. 230 CDA and was liable for prosecution under the federal law. This was possible under the already existing regulatory mechanism and FOSTA-SESTA was not required to ensure this.

In fact, these Acts upend the balance between online safety and privacy enabled ecosystems created by S. 230 CDA read with S. 2258A of the US Code. The legislation expands the ambit of existing federal criminal and civil laws to target online platforms where sex trafficking content appears and makes them liable for their user's sex trafficking activities.[9] The platform liability created by the amended S. 230 has been applied retrospectively, violating the constitutional

[6] Chamberlain, L. (2019) FOSTA: A Hostile Law with a Human Cost, 87 Fordham L. Rev. 2171 retrievable from https://ir.lawnet.fordham.edu/flr/vol87/iss5/13.

[7] Stewart, E. (2018, Apr. 23) The next big battle over internet freedom is here, *Vox.com retrievable from https://www.vox.com/policy-and-politics/2018/4/23/17237640/fosta-sesta-section-230-internet-freedom See also: https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet.*

[8] Jackman T. (2018) Top Officials at Backpage indicted after classifieds site taken offline, retrievable form https://www.washingtonpost.com/local/public-safety/top-officials-at-backpagecom-indicted-after-classifieds-site-taken-offline/2018/04/09/0b646f36-39db-11e8-9c0a-85d477d9a226_story.html.

[9] Mackey, A. (2017, Sept. 7) Stop SESTA: Congress Doesn't Understand How Section 230 Works, *Electronic Frontier Foundation, retrievable from https://www.eff.org/deeplinks/2017/09/stop-sesta-congress-doesnt-understand-how-section-230-works.*

protection against ex-post facto clause, especially in respect of criminal provisions.[10] The Act is worded so broadly that it can even be used against platform owners who have no *'actual knowledge'* about their platform being used for trafficking activities.[11] The proponents of FOSTA-SESTA provided little to no evidence whether increased platform liability will help to restrict trafficking, during the debate over the Bill in the Senate. However, the opponents of the Act have presented a plethora of evidence to show that shutting down platforms that advertise sexual services in fact exposes victims of trafficking to greater danger.[12] In fact, two years since its enactment numerous reports have surfaced proving that instead of protecting sex workers, the legislation has endangered their lives.[13]

Facing the risk of ruinous prosecution, FOSTA-SESTA leaves little choice before the intermediaries in becoming more restrictive about the type of discussions and the kind of users they allow on their platforms. While for some platforms it will mean more stringent terms of service, for the others it will mean over-reliance on automated filters. Both these mechanisms will lead to unreasonable restriction on free speech, violation of right to privacy and stifling of innovation. Irrespective of the means adopted by the platforms to mitigate risk, intermediaries erring on the side of censorship is certain to disproportionately restrict marginalised voices[14] and make the internet a less inclusive space.

---

[10]Boyd, S.E. (2018, Feb. 27) *Letter to the Committee on the Judiciary on H.R. 1865,* Office of the Assistant Attorney General *retrievble from https://assets.documentcloud.org/documents/4390361/Views-Ltr-Re-H-R-1865-Allow-States-and-Victims.pdf.*

[11] Mackey and Cope (2017, Sept. 8) Stop SESTA: Amendments to Federal Criminal Sex Trafficking Law Sweep Too Broadly, *Electronic Frontier Foundation, retrievable from https://www.eff.org/deeplinks/2017/09/stop-sesta-amendments-federal-criminal-sex-trafficking-law-sweep-too-broadly.*

[12] Romano, A. (2018, Jul. 2) A new law intended to curb sex trafficking threatens the future of the internet as we know it, *Vox.com, retrievable from https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.*

[13] Llansó, E. (2017, Aug. 1) SESTA Would Undermine Free Speech Online, *Centre for Democracy and Technology, retrievable from https://cdt.org/insights/sesta-would-undermine-free-speech-online/.*

[14] Blunt and Wolf, *Supra Note* 5 See also: https://www.eff.org/deeplinks/2017/09/stop-sesta-whose-voices-will-sesta-silence.

Figure 2

SESTA-FOSTA | Impact Assessment

- An estimated 73.5% of the sex workers in the US say that their financial situation has changed since FOSTA-SESTA.
- 72.5% of them are facing increased economic instability after FOSTA-SESTA was signed into law.
- 68.4% of them have received a mental health diagnosis (depression, anxiety, ADHD, PTSD were most common) since the passing of SESTA-FOSTA.
- 46.94% of them had no other form of income.
- 45.74% of them cannot afford to place an advertisement for their services.
- 33.8% reporting an increase of violence from clients.
- 99% of them report that this law does not make them feel safer.
- 60% had taken sessions with unsafe clients they would not have normally seen.
- Number of children trafficked has increased 32 times since 2016.

Source: The data is based on the surveys carried out by The Hacking Hustlings, Coyoteri and the Report published by Department of Health and Human Services on the condition of sex workers post SESTA-FOSTA.

3.2 The EARN IT Act

The EARN IT Act targets the safe harbour enjoyed by intermediaries by mandating that they would not automatically be exempt from liability against content related to CSAM but will have to 'earn it'. The First Draft of the Bill was met with severe criticism for its arbitrary provisions that gave unchecked powers to the Attorney General to decide a list of 'best practices' that the intermediaries must comply with in order to enjoy the safe harbour protection.[15] Following the censure from the civil society, significant changes were made in the Bill and its amended version was introduced. However, the new version of the Bill also fails to protect the digital rights of the users. It still provides the Attorney General the power to notify a 'broad category' of best practices for unrestricted regulation of the platform's editorial activities amounting to a violation of the First Amendment.[16] In fact, the Bill's selective removal of S. 230 immunity for CSAM content

[15] Pfefferkorn, *Supra note* 3

[16] Miami Herald Pub. Co. v. Tornillo, 418 U.S. 241. See also Mackey and Crocker (2020, Mar. 31) The EARN IT Act Violates the Constitution, *Electronic Frontier Foundation, retrievable from* https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution.

creates an unconstitutional condition as explained by the US Supreme Court again amounting to a violation of the First amendment.[17] Not to anyone's surprise, the Attorney General has already made it clear that he intends to ban encryption to allow LEAs 'lawful access' to digital messages.[18] By legalising search of user accounts by LEAs and intermediaries without a warrant explaining probable cause, the bill violates the Fourth Amendment.[19]

The most galling concern pertaining to the Bill is that like FOSTA-SESTA, it would not succeed in checking proliferation of CSAM content. On the contrary, UNICEF very recently released a working paper "*Encryption, Privacy and Children's Right to Protection from Harm"* explaining why encryption is crucial to ensure child safety and re-victimisation.[20] Further, the threat to take away safe harbour immunity for failure to comply with the notified 'best practices' will only scare the good-faith providers who already assist the LEAs by providing metadata to aid in investigations. On the other hand, CSAM traders would simply shift to dark web sites or other encrypted platforms, and could potentially develop their own encrypted systems making it even more onerous for LEAs to catch them. Sites solely dedicated to CSAM already do not qualify for S. 230 immunity, so threatening to take away this protection will have no effect on them. Lastly, even the good-faith platforms will not be free from CSAM material even if they follow the 'best practices' and not provide end-to-end encryption, because the users can still encrypt their files before transmitting it over the platform's service.[21]

[17] Elrod v. Burns, 427 U.S. 347 (1976). See also: *Ibid.*

[18] Brumfield, C. (2020, Mar. 10) Is the EARN-IT Act a backdoor attempt to get encryption backdoors?, *CSO, retrievable from https://www.csoonline.com/article/3531393/is-the-earn-it-act-a-backdoor-attempt-to-get-encryption-backdoors.html.*

[19] Mackey and Crocker *Supra note* 15

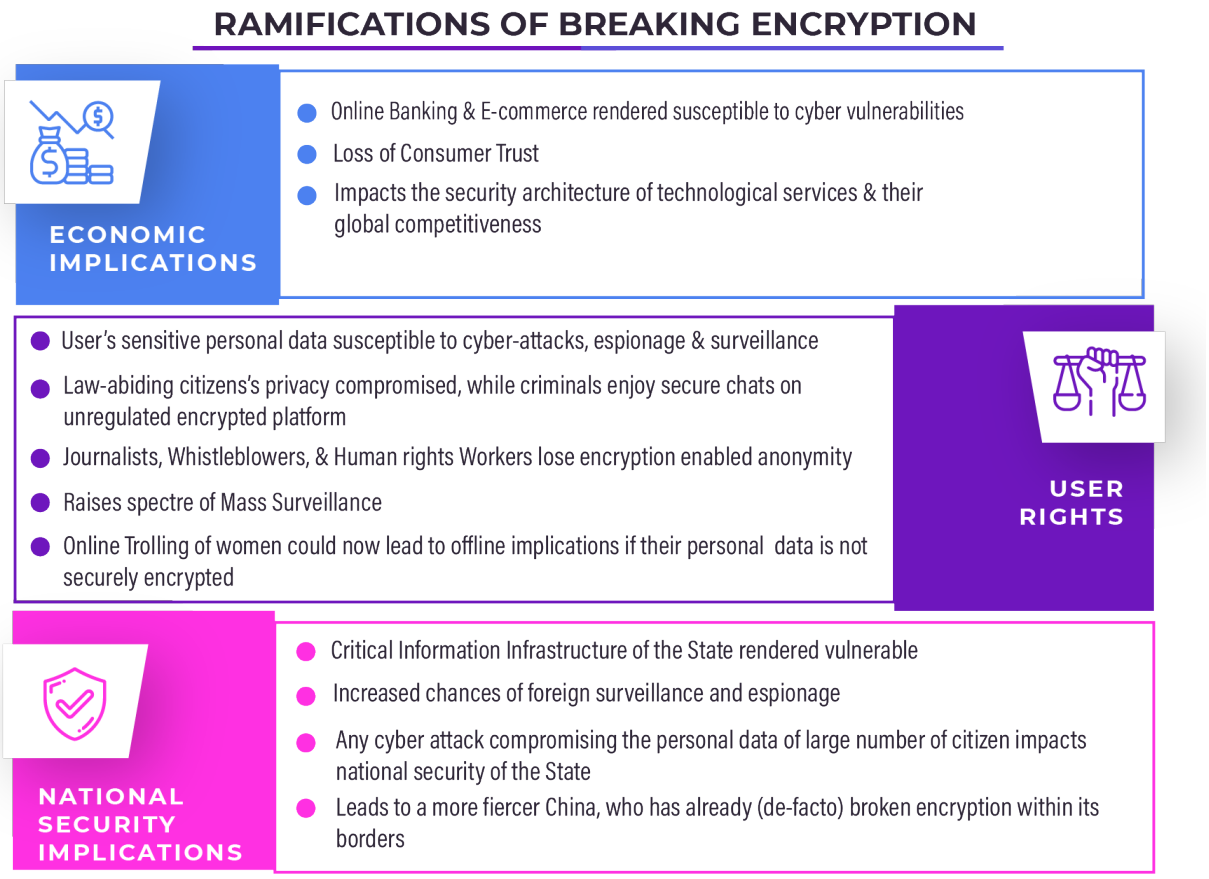
[20] Daniel Kardefelt-Winther et. al. (2020, Oct.) Encryption, Privacy and Children's Right to Protection from Harm, *UNICEF, Office of Research - Innocenti Working Paper WP-2020-14, retrievable from https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf.*

[21] Blunt and Wolf, *Supra Note* 5.

3.3 The LAED Act

Similar to the EARN IT Act, the Lawful Access to Encrypted Data Act, 2020 allows LEAs to seek access to encrypted data from the intermediaries which for all practical purposes would mean breaking encryption and amounting to a violation of the First Amendment and Fourteenth Amendment rights.[22] Similar to the challenge posed by the EARN IT Act, this legislation will restrict the good-faith providers from using encryption on their platforms while the savvy criminals will shift to other (or their own) encrypted platforms. Creation of backdoors will also render the platforms vulnerable to foreign surveillance. While it will be harder to catch savvy criminals, the law-abiding citizens will be left susceptible to cyber vulnerabilities in the digital age wherein the right to privacy has been held to be a part of right to life.

Figure 3



[22] Pfefferkorn,R. (2020, Jul. 13) The Senate's twin threats to online speech and security, *Tech Stream, retrievable from* https://www.brookings.edu/techstream/the-senates-twin-threats-to-online-speech-and-security/.

4. Is India Echoing the Shift in the American Safe Harbour Regime?

4.1 Analysing the Legislative Approach

In India, S. 79 IT Act modelled on S. 230 CDA, provides safe harbour protection to the intermediaries and builds a free speech enabling and privacy respecting digital ecosystem. This objective of the Indian State was supported by the judicial mandate in *Shreya Singhal v. Union of India* wherein the Apex Court explicitly held that

> *"Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material."*

The Indian regime seems to be echoing the shift in the intermediary liability regime in the US as evidenced from the Draft National Encryption Policy of 2015 (Draft Policy) and the Draft Intermediaries Guidelines (Amendment) Rules of 2018 (Draft Rules). The Draft Policy was revoked after receiving backlash from all quarters.[23] The Draft Rules which called on intermediaries to provide backdoor access to LEAs[24] and proactively identify and remove unlawful content from their platforms using automated tools or other appropriate mechanisms[25] have not been enforced, post two rounds of public consultations.[26] However, if implemented, they are likely to do more harm than good. As noted in the *Shreya Singhal* case, making intermediaries adjudicate upon the legitimacy of content takedown requests can be very problematic. For all practical purposes, it will mean the intermediaries acting as the arbiters of truth and morality to

[23] The Wire Staff (2015, Sept. 22) National Encryption Policy Withdrawn, *The Wire, retrievable from* https://thewire.in/tech/national-encryption-policy-withdrawn.

[24] Rule 3 (10) Draft IL Guidelines, Rules 2018.

[25] Rule 3 (9) Draft IL Guidelines, Rules 2018.

[26] Public Consultation Link MeitY: https://www.meity.gov.in/comments-invited-draft-intermediary-rules.

restrict the fundamental rights of the users, something which only the judiciary is empowered to do constitutionally.

Further, the Ad Hoc committee of the Rajya Sabha (Upper House of the Indian Parliament) endorsed the clause for backdoor access on encrypted platforms in the Draft Rules.[27] The challenge with such mandates is that the intermediaries will be compelled to indulge in proactive monitoring and develop technology to break encryption to acquire such information leading to pre-censorship, violation of privacy, and raising the spectre of mass surveillance. It is crucial to note that very recently, the TRAI recommended that the security architecture of end-to-end encrypted platforms must not be tinkered with else it will render the users susceptible to cyber vulnerabilities like hacking and espionage.[28] The recommendations are a result of five years of extensive consultations, analyses of international jurisprudence, and discussions at the International Telecommunications Union. Similarly, the report published by leading cryptographers of the world explains that backdoors and key-escrows only lead to more cyber-vulnerabilities.[29]

The lack of clarity in the IT Act regarding the differential roles and obligations of various classes of intermediaries is a major concern in the Indian intermediary liability regime. Though the government has been issuing specific guidelines for different sets of intermediaries,[30] it is crucial to have clearer delineations through appropriate statutory interventions, as already done in Draft E-commerce Policy, 2019.

---

[27] Rajya Sabha, (2020, Jan.) *Report of the Ad-hoc Committee in the Rajya Sabha to study the alarming issue of pornography on social media and its effect on children and society as a whole*, Parliament of India, *retrievable from* https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf.

[28] Telecom Regulatory Authority of India, Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services https://www.trai.gov.in/sites/default/files/Recommendation_14092020_0.pdf.

[29] Harold, A. et al. (2015, Jul.6) *Keys under doormats: mandating insecurity by requiring government access to all data and communications.* Journal of Cybersecurity 1.1 (2015): 69-79 *retrievable from http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.*

[30] For instance, order issued to ISPs operating cable landing gateway stations to adopt a filtering mechanism for child sexual abuse material (Government of India, 2017). https://www.meity.gov.in/writereaddata/files/Order%20regarding%20online%20CSAM.pdf.

4.2 Analysing the Judicial Trend

The recent judicial pronouncements reveal a retrogressive trend in India with the courts retracting from the *Shreya Singhal* mandate, by limiting the ambit of safe harbour protection accorded to the intermediaries. The decisions of the Indian Supreme Court in *In re: Prajwala*[31], *Sabu Mathew George v. Union of India*[32], the Uttarakhand High Court in *In re: v. State of Uttarakhand*[33] and the Delhi High Court in *Ms. X. v. State and Ors.*[34] are evidence of the same.

4.2.1 In re: Prajwala

In the *Prajwala* case, a committee was constituted to assist and advise the Apex Court on the feasibility of preventing sexually violent videos from appearing online. The committee held extensive deliberations and made recommendations that include blocking of search queries containing certain key words and preventing upload of sexually abusive videos at the source using hashing and other technologies. Enforcement of such technical measures involving the use of automated tools will lead to pre-censorship[35] and could have a chilling effect on free speech.

4.2.2 Sabu Mathew George v. Union of India

The Apex Court in this matter issued orders to the intermediaries to 'auto block' content pertaining to pre-natal sex determination, 'based on their own understanding'. The Apex Court in *Shreya Singhal* clearly laid down that the intermediaries do not have to make a legal determination pertaining to the nature of the content and only have to act based on 'actual knowledge'. The Court in *Sabu Mathew case* has patently overlooked the binding precedent of *Shreya Singhal and*

[31] *In re: Prajwala,* SMW (Crl.) No(s).3/2015.

[32] *Sabu Mathew George v. Union of India,* [WP(C) 341/2008].

[33] *In re: v. State of Uttarakhand,* WP (PIL) No. 158/2018.

[34] *Ms. X. v. State and Ors.,* WP (Crl.) No. 1080/2020.

[35] *Brij Bhushan v. State of Delhi,* 1950 AIR 129.

ordered the intermediary to make a legal determination. This will place the intermediaries to legally determine the rights of users, which is essentially the domain of the State.

4.2.3 In re: v. State of Uttarakhand

The Uttarakhand High Court in this matter held that the order of the Department of Telecommunication, notified on 31st July, 2015, asking Internet Service Providers (ISPs) to disable 857 websites hoarding pornographic content, be strictly complied with. The decision is challenging on two fronts. *Firstly,* the Department itself had modified its order in August 2015 and limited the applicability of the order to websites having child pornography, and the High Court completely overlooked this. *Second*, the Court insufficiently relied on Section 79(3)(b) of the IT Act. Per S. 79 (3) (b) an intermediary will be liable for third party content when despite knowing or being notified by the government, the platform is used for unlawful acts. The High Court relied on S. 79 (3) (b) but failed to clarify what this unlawful act is, which is being committed.

4.2.4 Ms. X v. State and Ors.

The Delhi High Court observed that 'it would be necessary for the intermediaries to take all effective measures that may be available with them' to combat CSAM, which imposes an obligation on intermediaries beyond what is required for them to enjoy the safe harbour protection. The essentials for enjoying this protection are in S. 79 of the IT Act and reiterated in the *Shreya Singhal* case, which provides that the platforms risk liability only when they fail to act after receiving 'actual knowledge' of unlawful content from a court/government order. CSAM is a challenge that needs to be tackled, and obligations for the same are already in place via the IT Act.

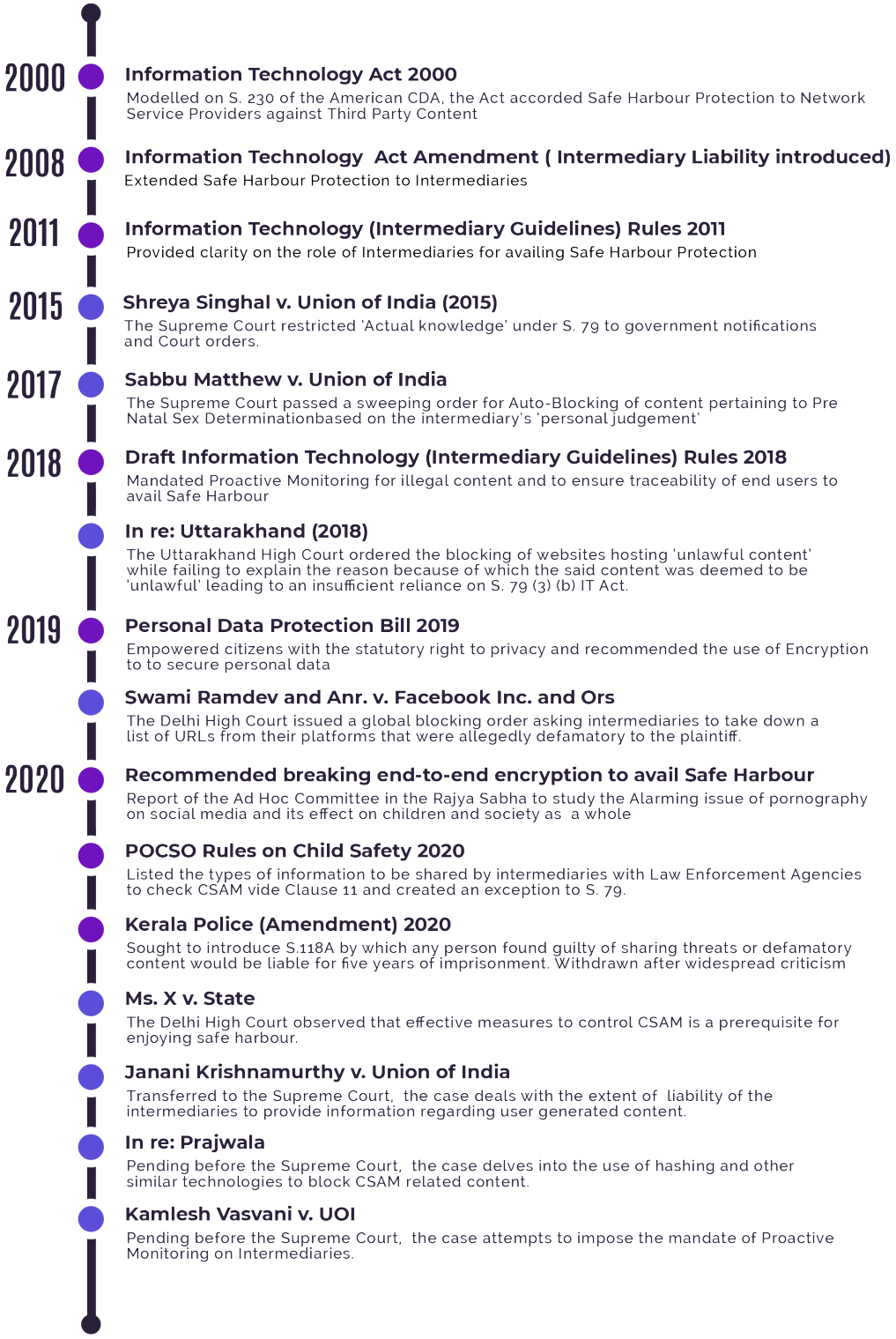
4.2.5 Swami Ramdev and Anr. v. Facebook Inc. and Ors.

An injunction order was issued by Delhi High Court directing YouTube, Facebook, and Google to globally auto-block a list of URLs that were found to be defamatory against the plaintiff. Citing the liability under the Intermediary Liability Guideline Rules, 2011, the Court held that the

intermediaries were obliged to take down and block all such illegal content and videos which had been uploaded from I.P. addresses within India, on a global basis. Further, for illegal content, which was uploaded outside the Indian territory, the Court directed geo-blocking access and disabling viewership of such content from within India.

Figure 4

TRACING THE INDIAN INTERMEDIARY LIABILITY REGIME



5. Encouraging both Safe Harbour and Safety: The Way Forward

The American experience explicates that compromising privacy and free speech to promote online safety does not render the desired results and in turn undermines the freedom and inclusivity on the internet. Accordingly, there is a need to address these challenges with a more practical approach.

Evidence based Approach: Given that the intermediaries are already bound to share crucial metadata with the LEAs under the IT Act, it is important to understand the exact challenge that the LEAs are facing. There is a need to gather in-depth research to understand and act on increasing the number of FIRs registered with the rise of CSAM reports being submitted by organisations to the NCRB.[36]

Collaborative Efforts: It is important that the tech companies, academia, industry bodies and the LEAs work together to find innovative solutions to better understand and respond to cyber-crime. Such meaningful collaborations will help increase the number of prosecutions in CSAM cases.

Building capacity of the LEAs: Rendering greater economic support to the underfunded criminal justice machineries is also crucial to ensure time bound investigation and prosecution in online child exploitation matters. The recently introduced Invest in Child Safety Act is a laudable initiative by the U.S. government in this regard. The Act creates a mandatory funding of 5 billion dollars, adds 100 new FBI agents and 65 positions at National Center for Missing and Exploited Children (NCMEC) to respond to online sex abuse. Substantial funding has also been directed under the legislation to promote community-based efforts to prevent child abuse in the digital space and a new office has been created at the White House to coordinate all these efforts aimed at combating CSAM and promoting child rights in the country. It would be appreciable for the Indian State to deliberate upon such measures and consider the feasibility of enacting similar legislations aimed at enhancing capacity of the LEAs.

[36] Sharma, J.P. (2019, Aug. 14) 31 FIRs Against Over 15,000 Complaints Filed On Govt's Website To Report Child Pornography: RTI, *Outlook India, retrievable from* *https://www.outlookindia.com/website/story/india-news-31-firs-against-over-15000-complaints-filed-on-govts-website-to-report-child-pornography-rti/336192*.

Adopting the Global Soft Law Principles for Platform Regulation: The Manilla Principles[37] and the Santa Clara Principles[38] are considered the global soft laws for the intermediary liability regime. Based on the ideals of transparency and accountability, these Principles strive for a balance between limited platform liability that is necessary to ensure online safety without compromising with the right to free speech and privacy of the users. Regimes across the globe including India and the USA must ensure the incorporation of these Principles in their internet governance regulations to build a robust, liberal and inclusive internet ecosystem.

Sensitisation: Needless to say, education, awareness and sensitisation is the key to ensure online safety in the long run. It is important that the regime acknowledges the inherent vices of the proposed solutions and picks up a practical approach by engaging with the academia, civil-society and organisations to find meaningful solutions.

[37] Manila Principles on Intermediary Liability, *retrievable from* https://www.manilaprinciples.org.

[38] Santa Clara Principles On Transparency and Accountability in Content Moderation, *retrievable from* https://www.santaclaraprinciples.org/.

APPENDIX

Table of Contents

1. Introduction to Intermediary Liability Regime in the US and India

The internet has presented unprecedented challenges and opportunities for the citizenry. It is not only an integral part of our social life, but also that of the global economy. Despite the obvious distinctions in the legal systems of the US and India, their regulatory regimes for Intermediary Liability are surprisingly similar, de-facto.

Both the USA and India are constitutional democracies embedded with the values of democracy and rule of law. Both these nations are acclaimed world over for their liberal and progressive values as evidenced from the non derogable nature of fundamental rights that these countries provide to their citizens. In pursuance of their democratic values, both the countries have secured to their citizens the right to free speech and right to privacy towards building an open and safe internet ecosystem that ensures the furtherance of these values. One of the key ingredients of an open internet ecosystem is 'safe harbour' which both these countries provide to the online intermediaries, to encourage them to provide the users a safe and free speech promoting platform without fearing prosecution in respect of third party generated content. With the growing perils of CSAM on the internet, both nations have been considering diluting the safe harbour protection of the intermediaries for ensuring child safety in the digital space. However, this measure, instead of rendering a solution, is likely to create more problems.[39] Proactive monitoring and creation of backdoors as a result of diluting safe harbour will not just invade privacy of the users and have 'chilling effect' on their free speech, but can also lead to a national security challenge.[40]

[39] Choudhary and Sugathan (2020, Jul. 1) From India to US, Forcing Proactive Policing of Online Content Is Censorship by Proxy, *The Wire, retrievable from* https://thewire.in/tech/online-content-policing-censorship.

[40] Joshi, D. (2018, Dec. 26) Accountability, Not Curbs on Free Speech, is the Answer to Harmful Content Online, *The Wire, retrievable from* https://thewire.in/law/accountability-free-speech-online-content.

2. The Regulatory Framework for Intermediary Liability Regime in the US

The American intermediary liability regime traces back its origin to the traditional defamation liability for intermediaries. The tort based common law jurisprudence of defamation has evolved over multiple judgements by various states and the Supreme Court of the United States which builds upon the First Amendment right.[41] The First Amendment also empowers the traditional privacy-based liability for intermediaries, which is a patchwork of tort law and legislative enactments.

With an absolute right to freedom of speech and a limited right to privacy, the American intermediary liability regime presents unique facets which have been localised by many countries. Section 230 of the Communications Decency Act, 1996, is the cornerstone of the intermediary liability regime in the USA and the Indian safe harbour provisions have been modelled on the same as well.

Intermediary Liability with respect to third party content is governed by two legislations in the USA- Section 230 of the Communications Decency Act, 1996 (CDA)[42] and Section 512 of the Digital Millennium Copyright Act, 1998 (DMCA).[43] The CDA grants broad immunity to any interactive computer service provider. It also calls for a 'Good Samaritan' protection where such service providers shall not be liable for taking any action to screen or block any content, they deem offensive. Such immunity extends to all claims except violation of federal criminal law and intellectual property right legislations. In 2018, a new set of legislations, i.e., the Senate bill called the Stop Enabling Sex Traffickers Act was passed (SESTA) and the House bill known as Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) was signed by President Donald

[41] Post, C.R.(1986) *The Social Foundations of Defamation Law: Reputation and the Constitution*, California Law Review, no.74 , *retrievable from* https://digitalcommons.law.yale.edu/fss_papers/217/.

[42] Section 230, Communications Decency Act, *retrievable from* http://www.columbia.edu/~mr2651/ecommerce3/2nd/statutes/CommunicationsDecencyAct.pdf.

[43] Digital Millennium Copyright Act, 1998, retrievable *from* https://www.copyright.gov/legislation/dmca.pdf.

J. Trump. FOSTA-SESTA has narrowed the scope of such immunity by adding a new exception for claims involving prostitution and sex trafficking.

2.1 Communications Decency Act, 1996

Liability for online intermediaries first emerged as a legal issue in 1991 in the case of *Cubby Inc. v. CompuServe Inc.*[44] In this case, the New York Federal Court dismissed a defamation suit against an online platform *CompuServe* on the ground that it had not edited the newsletter and no liability could arise unless it 'knew or had reasonable reason to know' about the alleged harmful content. However, four years later in *Stratton Oakmont, Inc. v. Prodigy Services Co.*[45], the New York State court refused to dismiss a defamation suit in a similar matter. The primary reason for the liability for the online service provider *Prodigy* was that it had reserved the right to edit content and filter offensive user posts. These two judgements laid down the law that intermediaries can only be held liable for third party content when they take steps to control it, such as through forum moderation or user guidelines.

These rulings caught the attention of the public as advocacy groups, and policy makers worried that such precedents would turn the internet into a 'no man's land' with highly inappropriate content that is harmful for children.[46] To cater to these concerns, the Congress could have imposed stringent regulations on the intermediaries, but realising that such measures would have received strong opposition from the internet service providers and intermediaries, the Congress decided to address online content moderation by means of enacting S. 230 CDA.[47] This is a manifestation of the Congress's twin goals to encourage voluntary moderation of user generated content by the

[44] *Cubby, Inc. v CompuServe, Inc*, [1991] 776 F. Supp. 135 (S.D.N.Y.).

[45] *Stratton Oakmont, Inc. v Prodigy Services Co*., [1995] INDEX No. 31063/94.

[46] Kosseff, J. (2017, Jun.) Twenty Years of Intermediary Liability: The US Experience, *Scripted Journal, retrievable from* https://script-ed.org/article/twenty-years-of-intermediary-immunity-the-us-experience/.

[47] Id.

intermediaries and to promote development of the internet as a platform for exercising free speech and carrying out commercial activities.[48]

The CDA is the cornerstone of the American intermediary liability regime. In its original form certain provisions of CDA were a little restrictive and impinged upon the Constitutional guarantee of free speech, but subsequently the violative sections of the CDA were held unconstitutional.[49] Section 230 of the CDA provides a safe harbour to intermediaries from liability for user generated content as long as the intermediary adheres with other provisions of the CDA. It provides that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider and that intermediaries shall not be liable on account of efforts to monitor or enforce policies against inappropriate or unlawful user-generated content. It immunizes platforms for nearly all claims except for those under federal criminal law and intellectual property law. This 1996 law, a long pillar of US Internet legal practice, was amended for the first time since its enactment in 2018.

US Government's Policy on Safe Harbour

Section 230(B)(4) of the CDA

"encourage the development of technologies that maximize user control over what information is received by individuals to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."

2.2 Digital Millennium Copyright Act, 1998

Safe Harbours for ISPs against monetary liability for copyright infringing material that is posted or sent through an intermediary's system is laid down via the Digital Millennium Copyright Act, 1998. It protects four classes of intermediaries- conduit providers such as telephone companies,

[48] "Statement of Representative Goodlatte" (1995) 141 Congressional Record, at p. H8471, *retrievable from* https://www.congress.gov/crec/1995/08/04/CREC-1995-08-04.pdf.

[49] *ACLU v. Janet Reno* (June 11, 1996) *retrievable from* https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0612decision.html.

those who store or cache content hosted by another and those who host content posted by another, and search engines. The benefit from safe harbour can only be derived if the intermediaries establish, publicise and implement both, a notice and takedown system for removing infringing content, and also a system to identify and remove repeating infringers.

2.3 Federal Law: Limiting the ambit of Safe Harbour

Though S. 230 of CDA immunises the intermediaries from prosecution in respect of third party generated content, it is important to note that the safe harbour is not a blanket immunity for the intermediaries. Legislators have created exceptions to the safe harbour rule in order to counter the proliferation of online social vices like CSAM. S. 2258 A of Chapter 110 of Title 18 of the U.S. Code makes everything relating to CSAM illegal.[50] The Department of Justice has the power to prosecute anyone who is found guilty of producing, viewing, storing or sharing CSAM content. The provision makes it mandatory for the intermediaries to report CSAM whenever they discover CSAM content on their platform or when they receive a report in this regard. Failure to comply with this liability shall result in the intermediaries losing their safe harbour protection under S. 230 CDA. Based on the test of 'actual knowledge', this law creates a reasonable balance between protecting child rights in the digital space and enabling free speech.

3. Contemporary Debate in the USA

The intermediary liability regime in the USA, though generally progressive, has been facing troubled waters currently. The Executive Order on Preventing Online Censorship[51] coupled with the legislations introduced by the administration have a dilutive impact on the safe harbour provided under Section 230 of the CDA.[52]

---

[50] 18 U.S. Code CHAPTER 110—Sexual Exploitation and Other Abuse Of Children, *retrievable from* *https://www.law.cornell.edu/uscode/text/18/part-I/chapter-110*.

[51] "Executive Order on Preventing Online Censorship", Infrastructure and Technology, White House, May 28, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/.

[52] Thomas and Grover (2020, Jun. 25) Donald Trump is attacking the social media giants. Here's what India should do differently, *Scroll.in, retrievable from* *https://scroll.in/article/965151/donald-trump-is-attacking-the-social-media-giants-heres-what-india-should-do-differently*.

3.1 FOSTA-SESTA

Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act (FOSTA-SESTA) creates an exception to Section 230, that means website publishers would be responsible if third parties are found to be posting ads for prostitution — including consensual sex work — on their platforms. The goal is supposed to be that policing online prostitution rings gets easier. What FOSTA-SESTA has actually done, however, is create confusion and immediate repercussions among a range of internet sites as they grapple with the ruling's sweeping language.[53]

The new law is the first amendment since 1996 to Section 230 of the CDA. It further goes ahead to amend existing federal criminal laws covering prostitution[54] and trafficking[55]. It exposes intermediaries to two new categories of lawsuits. One is civil claims brought by private parties under federal law, and the other is criminal claims brought by state officials. State attorneys general may now bring criminal prosecutions under state laws, if they target content that would violate FOSTA's federal prostitution and trafficking provisions.

Liability for intermediaries under this law turns in an important part on mental state or scienter. For most aspects of the law, a plaintiff or prosecutor must show "knowledge," but for some situations, liability may instead be premised on "reckless disregard." Numerous critics of the Act, including advocates for start-ups, argued that the standard was confusing, leaving intermediaries with very little certainty about their legal obligations and with great incentive to err on the side of taking down both lawful and unlawful content.[56] The well intentioned FOSTA-SESTA dilutes

[53] Woolery, L. (2018, Mar. 8) It's All Downsides: Hybrid FOSTA/SESTA Hinders Law Enforcement, Hurts Victims and Speakers, *Centre for Democracy and Technology, retrievable from https://cdt.org/insights/its-all-downsides-hybrid-fosta-sesta-hinders-law-enforcement-hurts-victims-and-speakers/.*

[54] Section 2421A, U.S. Code, [18 USC 2421A], *retrievable from* https://www.law.cornell.edu/uscode/text/18/2421A.

[55] Section 1591, U.S. Code, [18 USC 1591], *retrievable from* https://www.law.cornell.edu/uscode/text/18/1591 and Section 1595, U.S. Code, [18 USC 1595], *retrievable from* https://www.law.cornell.edu/uscode/text/18/1595.

[56] Burnitis, C. (2020) *Facing the Future with FOSTA: Examining the Allow States and Victims to Fight Online Sex Trafficking Act of 2017*, 10 U. Miami Race and Soc. Just. L. Rev. 139, *retrievable from https://race-and-social-justice-review.law.miami.edu/wp-content/uploads/2020/08/Facing-the-Future-with-FOSTA_-Examining-the-Allow-States-and-Vict.pdf.*

the protection envisaged under Section 230 CDA which is the foundation for exercising free speech on the internet.[57] Some of the major challenges posed by these two legislations include:

- **Creating Overarching Exceptions to Safe Harbour:** Section 230 is the backbone of modern internet. It creates a careful balance for when the intermediaries can be held liable for user generated content and when they cannot. The FOSTA- SESTA legislations upend that balance by opening platforms to greater civil and criminal liability.[58] The mandate in the bill to make the platforms liable in respect of sex trafficking content regarding which they had no 'actual knowledge' would frustrate the entire object of safe harbour.[59] More disturbingly, the criminal liability of the platforms would be applied retrospectively, meaning that a platform can be prosecuted for failing to comply with these legislations even before they were passed.
- **Imposing Excessive liabilities undermines Innovation and Fair Competition:** These measures will also severely impact innovation and fair competition. While big technology companies have the funds and resources to survive the demands of these legislations and face the resultant increase in prosecutions, small companies and startups don't. In fact, with the increased risk of litigation it would be difficult for new startups to ever get the funding they need to compete with big technology companies.[60]
- **These Acts have a Chilling Effect on Online Free Speech:** Needless to say, the most glaring impact of these legislations is on online free speech. Facing the danger of extreme criminal and civil liability, the intermediaries will have little option but to comply with the legal requirements, which could lead to proactive monitoring, resulting in silencing of

[57] The Copia Institute, *Open Letter to the Sponsors of SESTA, retrievable from https://230matters.com/letter.html.*

[58] Harmon, E. (2018, Mar. 21) How Congress Censored the Internet, Electronic Frontier Foundation, retrievable from https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet.

[59] Bill No. OLL20597 *to improve the ability of law enforcement agencies to access encrypted data, and for other purposes, retrievable from https://epic.org/crypto/OLL20597.pdf.*

[60] Harmon, E. (2017, Sept. 22) Google Will Survive SESTA. Your Startup Might Not, Electronic Frontier Foundation, *retrievable from https://www.eff.org/deeplinks/2017/09/google-will-survive-sesta-your-startup-might-not.*

legitimate voices.[61] It's difficult for humans to distinguish between a harmful and a legitimate post, and a computer can certainly not do it with anything close to 100% accuracy. Thus, reliance on automated filters would do nothing more than silencing marginalised voices.[62]

3.2 EARN IT Act

Although the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) does not use the word "encryption" in its text, it gives government officials, like the Attorney General, the power to compel online service providers to break encryption, or be exposed to potentially crushing legal liability.[63]

The Act strips Section 230 protections away from any website that does not follow a list of 'best practices,' meaning those sites can be sued into bankruptcy.[64]

As noted earlier, the S. 2258 A of the Federal CSAM law already creates reasonable exceptions to S. 230 CDA and if it is felt that the law is not doing enough, then the most reasonable mechanism would be to amend the provision rather than introducing an altogether new legislation. Most importantly, like SESTA-FOSTA trying to combat sex trafficking has actually ended up endangering sex traffickers more, the same is feared with EARN-IT Act. The most likely effect of this Act will be that it will become even more difficult to detect CSAM traders, as for one they

[61] Untangling SESTA – FOSTA: How the Internet's Knowledge Threatens Anti-Sex Trafficking Laws, *retrievable from* https://btlj.org/data/articles2019/34_4/11_McKnelly_WEB.pdf.

[62] Freedom Network USA, *Public statement of caution in Reforming CDA, retrievable from https://www.eff.org/files/2017/09/18/sestahearing-freedomnetwork.pdf*.

[63] Mackey and Crocker (2020, Mar. 31) The EARN IT Act Violates the Constitution, *Electronic Frontier Foundation, retrievable from https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution*.

[64] Mullin, J. (2020, Mar. 12) The EARN IT Bill Is the Government's Plan to Scan Every Message Online, *Electronic Frontier Foundation, retrievable from* https://www.eff.org/deeplinks/2020/03/earn-it-bill-governments-not-so-secret-plan-scan-every-message-online

can still encrypt their files before transmitting it, and secondly it will incentivise them to move off the good-faith platforms to dark web sites.[65]

Experts and activists argue that the EARN-IT Act is a veneered attempt to hand over the control of online privacy to federal law enforcement agencies under the garb of crimes against children. The creation of backdoors will put the citizens at a more vulnerable spot. Their personal data will now be susceptible to surveillance owing to the backdoor access while the savvy criminals would conveniently use superior encryption on a different open-source platform.

Such an Act is bound to impact the security architecture of an end-to-end encrypted platform and render its users vulnerable to espionage, surveillance and cyber-attacks by foreign states and non-state actors.[66] Afterall, it is the collective security of all citizens which is the cornerstone of national security.

3.3 LAED Act

Recently, the Lawful Access to Encrypted Data Act, 2020 (LAED)[67] provided law enforcement agencies the tools required to protect the public from crime and manage the threats to national security. The Act requires service providers and device manufacturers to assist law enforcement in accessing encrypted data. It also lays down the prerequisite to such assistance to be a court issued warrant, based on probable cause that a crime has occurred. However, what is challenging here is that the legislation sets an extremely low bar for breaking encryption. All that the LEAs have to do is to prove that there is reasonable ground to believe that decrypting a device will help them garner some useful information that will be beneficial in their investigation, and it will become mandatory for the Court to issue the warrant. It also allows the Attorney General to issue

[65] Azarmi and Quay-de la Vallee (2020, Aug. 25) The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions, *Centre for Democracy and Technology, retrievable from* https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions/.

[66] Eoyang and Garcia (2020, Sept. 9) Weakened Encryption: The Threat to America's National Security, *Third Way, retrievable from* https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security.

[67] Lawful Access to Encrypted Data Act, *retrievable from* https://www.docdroid.net/IHiIrMA/oll20597-pdf.

directives to service providers and device manufactures to report on their ability to comply with court orders.

The Act amounts to an explicit attack on encryption contrary to the advice of cyber security researchers.[68] The primary challenge posed by this legislation is again the fact that any encrypted platform with a backdoor is fundamentally insecure. If there is a vulnerability on a platform then eventually someone will find it out and exploit it. In case a service does not have a known decryption method, the Act enables LEAs to issue a directive ordering the said company to develop a 'way around encryption'. The bill has even created a prize competition to incentivise researchers to find new ways of breaking cryptography.

4. The Recent Judicial Trend in India

4.1 Sabu Mathew George v. Union of India

Facts: In 2008, Sabu Mathew George, a gender activist and doctor, filed a writ petition in the Supreme Court of India to ban advertisements related to pre-natal sex determination from search engines like Google, Bing and Yahoo for violation of Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994.[69]

Decision: The court issued interim orders directed Google, Microsoft and Yahoo to 'auto-block' pre-natal sex determination ads from appearing in search results 'based on their own judgement'. The Supreme Court also directed the Central Government to constitute a nodal agency for receiving complaints from anyone who came across anything that has the nature of an advertisement or has any impact in identifying a boy or a girl in any method, manner or mode by any search engine. The nodal agency was then required to convey actionable complaints to the concerned intermediaries, who were obliged to delete the content in question within 36 hours and intimate the nodal agency.

[68] Harold A. et al. *Supra note 28.*

[69] *Sabu Mathew George v. Union of India,* [WP(C) 341/2008].

Impact: In this matter, the Apex Court held that intermediaries are obliged to keep unlawful content from appearing on their networks. Even after the ruling of the Supreme Court in *Shreya Singhal,* wherein the court made it clear that intermediaries must not be asked to exercise their personal judgment in determining the legality of content for takedown purposes, the court continues to ask intermediaries to proactively filter their platforms for illegal content.

4.2 In re: Prajwala

Facts: The Founder of Hyderabad based NGO Prajwala wrote a letter to the Supreme Court highlighting the circulation of pornographic videos on social media platforms. The Supreme Court's social justice bench took *suo moto* cognizance of the letter and ordered a Central Bureau of Investigation (CBI) inquiry into the videos. A committee was constituted under the Chairmanship of Dr. Ajay Kumar, the then Additional Secretary of the Ministry of Electronics and IT, to assist and advice the court on the feasibility of preventing sexual abuse/ violence videos from appearing online. The committee held extensive deliberations and made recommendations towards preventing the upload and circulation of sexually violent videos online.[70]

Decision: The matter is still pending before the Apex Court for final disposal. However, all parties including Google, Facebook, Microsoft, WhatsApp and the Government have been directed by the Court to implement all recommendations of the committee with consensus at the earliest.

Impact: Many of the accepted recommendations of the Ajay Kumar Committee involved blocking of search queries containing certain key words and preventing upload of sexually abusive/violent videos at the source using hashing and other technologies.

4.3 In Re: v. State of Uttarakhand

Facts: The Uttarakhand High Court took *suo moto* cognizance of three newspaper articles that revealed the rape of a minor student by her four classmates. The news items revealed that the

[70] *In re: Prajwala,* SMW (Crl.) No(s).3/2015.

boys were inspired by the porn movies to commit this crime. The court also noted that the Department of Telecommunications had already ordered the blocking of all websites containing obscene content in August 2015.[71]

Decision: Despite the Department of Telecommunications modifying its order to block 857 websites hoarding pornographic content, the Uttarakhand High Court directed the implementation of the order in its original form. The High Court failed to appreciate S. 79 (3) (b) of the IT Act as it did not explain the 'unlawful act' committed by these intermediaries for which their websites were banned.

Impact: Insufficient reliance on a provision of law by the Hon'ble High Court is noteworthy. The Court ordered blocking of the websites under S. 79 (3) (b) without an explanation about what was the unlawful act committed by them, which amounts to unreasonable restriction on the rights of both the users and the intermediaries, as enshrined under Article 19 of the Constitution.

4.4. Kamlesh Vaswani v. Union of India

Facts: A PIL was filed by an Indore based lawyer challenging the constitutional validity of Sections 72,75, 79 and 80 of the IT Act. It was argued that these provisions are inefficient in tackling the proliferation of CSAM content on the internet.[72]

Decision: The matter is pending before the Supreme Court.

Impact: This case once again intends to impose the mandate of proactive monitoring on the intermediaries, which is antithetical to free speech and privacy and stands in clear violation of the *Shreya Singhal* judgement.

[71] *In re: v. State of Uttarakhand,* WP (PIL) No. 158/2018.

[72] *Kamlesh Vaswani v. UOI [W.P.(C) No. 177/2013].*

4.5 Janani Krishnamurthy v. Union of India and Others

Facts: Two writ petitions were filed by animal rights activists who were facing cyberbullying and were unable to track the perpetrators. They demanded the court to direct social networking services to link user accounts with their Aadhaar cards in order for law enforcement agencies to track and indict cyber offenders. The Madras High Court eventually decided against linking Aadhaar with social media accounts on the basis of the 2018 Supreme Court decision that Aadhaar can only be linked with social welfare schemes of the government.

However, the Madras High Court enlarged the scope of writ petition to resolve whether enabling traceability within applications such as WhatsApp is possible, given the E2EE feature enabled by default within the application. The Apex court noted that the main issue arising in the petitions was how and in what manner the intermediaries should provide information, including the names of the originators of any message/ content/ information shared on the platforms run by the intermediaries.[73]

Decision: By order dated 24.10.2019, the Supreme Court has directed these matters to be transferred to the Supreme Court.

Impact: This case intends to introduce traceability on online platforms for the purpose of curbing online challenges. Though well intentioned, such actions will be antithetical to right to privacy of the users and will end up creating newer challenges rather than resolving the existing ones.

[73] *Janani Krishnamurthy v. UOI, WP 20214/2018.*

About the authors

Shruti Shreya is the Policy Research Assistant at The Dialogue.

Pranav Bhaskar Tiwari manages the programme on Intermediary Liability & Encryption at The Dialogue.

Imprint

Recommended citation: Shruti, S., Pranav, BT., (December 2020). Analysing the American Safe Harbour Regime: Takeaways for India. New Delhi. The Dialogue.

The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

This publication is part of The Dialogue's larger initiative to drive informed discussion on intermediary liability and online safety in India through a series of consultations and research.

www.thedialogue.co