



Cyber Peace
Foundation

CYBER SECURITY & CHALLENGES

WHY INDIA NEED TO CHANGE IT ACT

AUTHORED BY: Ms N. S. NAPPINAI

ADVOCATE, Supreme Court of India | ADVISOR, Cyber Peace Foundation

February 5, 2017

www.cyberpeace.org

Table of Contents

Topic	Page No.
BACKGROUND	2
- The Rationale Behind the Initiative	3
- The Entities & Persons Behind The Initiative	4
1. Cyber Security & The Law	6
2. Cybercrimes – The India Story So Far	7
a. Cybercrimes	8
b. Cybercrime Statistics	9
i. Reporting of Cyber Crimes and Arrests	9
ii. Case pendency and closure rate	10
iii. Case status in Courts;	
iv. The 2016 Norton Cyber Security Insights Report	11
v. Statistics for motives for Cyber Crimes in India	12
c. Regulatory Mechanisms	
d. Legislations / Policies	13
i. Proposed Amendments to the Information Technology Act, 2000	15

A. Amendments to IT Act	16
1. S.65 IT Act	16
- Recommendation.	17
2. S.66 IT Act	17
- Recommendation.	18
3. S.66 r/w S.43(i) IT Act	18
- Recommendation.	19
4. S.66 C IT Act	19
- Recommendations.	19
5. S.66 D IT Act	19
- Recommendations	19
6. S.66 E IT Act	20
- Recommendations	20
7. S.66 F IT Act	21
- Recommendations	21
8. S.67 IT Act	22
- Recommendations	22
9. S.69 – S.69B IT Act	23
- Recommendations	23
B. Additions to IT Act	24
1. Cyber Bullying	24
- Recommendations	25
2. Self – Harm	25
- Recommendations	25
3. Hate Speech	25

- Recommendations	26
A. Review of Procedural Laws	26
1. S.65A & S.65B of the Indian Evidence Act, 1872;	26
- Recommendations	26
2. Jurisdiction	27
- Recommendations	27
3. Other Amendments	27
a.Appointment of Special Tribunals / Appellate Authority for Cyber	27
- Recommendations	28
b. Intermediary Liability	29
- Recommendations	29
c. Policies & Government Initiatives	29
d. Judiciary and Cyber Crimes	30
e. International Perspective	30
f. International Perspective	31
g. Suggestions	31
Acknowledgement	34

BACKGROUND

The Information Technology Act, 2000 (“**IT Act**”) was enacted primarily as a facilitator for Ecommerce. Almost, as an afterthought, about ten provisions were introduced to combat cybercrimes (Chapter XI comprising Sections 65 to 78 IT Act). Offences that were already rocking the world like virus attacks and hacking were relegated to civil violations for which penalties were prescribed under S.43 of the IT Act. The civil enforcement of the provisions listed under this section also leaves a lot wanting with the Cyber Appellate Tribunal established under S.48 (1) of the IT Act, being dysfunctional since about 2011. To add to the litigants’ woes the Finance Bill of 2017 seeks to disband this separate Tribunal and to vest this authority with the Telecom Disputes Settlement and Appellate Tribunal (“**TDSAT**”). This would merely create further confusion and backlog.

Amendments to the IT Act based on the issues that arose in its implementation were taken up for consultation as early as in 2005 itself and again in 2006. However, it took the Mumbai terror attacks for an expedited knee-jerk reaction to bring in extensive amendments to the IT Act in 2008. The amendments were passed without even an attempt at a debate in December 2008. With substantial Rules remaining to be drafted, the amendments came into effect only on October 27, 2009.

The amended IT Act has already faced many challenges. S.66A was struck down by the Hon'ble Supreme Court in *Shreya Singhal v. Union of India*¹. The entire proving of electronic evidence in many a case was under severe challenge after the Supreme Court reversed its decision in *State (N. C. T. of Delhi) Vs. Navjot Sandhu*², when it decided the case of *Anvar V.*

¹ (2015) 5 SCC 1 : 2015 SCC OnLine SC 248;

² AIR 2005 SC 382; 2005 AIR SCW 4148;

*Basheer*³. The Supreme Court rightly held that special provisions such as S.65A and S.65B of the IEA would take primacy over general provisions for secondary evidence. However by not making it a prospective overruling, the Supreme Court's decision fatally affected the outcomes of earlier cases decided on the basis of *Navjot Sandhu's case*. The provision i.e., S.65B IEA in itself requires urgent review⁴.

The Rationale Behind the Initiative

Any attempt at repairing a defective piece, results in either temporary relief at best. Most importantly, the band - aid remedy started to unravel in no time. One instance is of S.66 under the 2000 Act was deleted. It was however included in S.43 and the violations under S.43, when committed with dishonest or fraudulent intent was made a criminal offence under the new S.66 IT Act. The complications that the piecemeal modifications have brought forth is felt most in the enforcement of the provisions.

Further, separate heads of offences like hacking, data theft, virus attacks, denial of service attacks and more have been clubbed together into one provision. With this, an offender is not even aware that he is committing an offence. The victim is confused about the rights and remedies available to them. The police and prosecution are more confused and hence resort to invoking the entire S.43 r/w S.66 IT Act instead of the sub-provision applicable. Such blanket prosecutions weaken the evidence collection and proving thereof.

Even these blanket provisions suffer from serious inconsistencies and anomalies. These further weaken prosecutions. Abuse of existing provisions, as was done with S.66A have further resulted in the very provisions being struck down. Other provisions, which have already been

³ 2014 (10) SCC 473;

⁴ Refer to Chapter 5 of the book Technology Laws Decoded by Ms. N. S. Nappinai for the etymology and a detailed analysis of S.65B of the Indian Evidence Act, 1872 and also the need for amending the same.

subjected to rampant misuse such as S.66F IT Act and which otherwise are very important to safeguard interests of Indian citizens and residents require to be reviewed and revised to ensure effective enforcement and to prevent abuse.

Laws pertaining to “cyber” are not limited only to the IT Act. Several provisions were incorporated in the Indian Penal Code, 1860 (“**IPC**”) and in the Indian Evidence Act, 1872 (“**IEA**”). Provisions intended to facilitate electronic commerce and transactions such as S.65A and S.65B IEA have become impediments in enforcements – be they civil or Criminal. There are substantial inconsistencies between similar provisions in such general laws and similar provisions under the IT Act. In particular, provisions pertaining to jurisdiction have to be reviewed across general and special laws and harmonized to ensure that the very inconsistencies between the two do not hamper effective enforcement.

The Entities & Persons Behind The Initiative

Centre for Economic Policy Research (“**CEPR**”) and Cyber Peace Foundation (“**CPF**”), spearheaded this initiative to review the existing Indian Legal Framework to ensure that India has effective legal enforcement mechanisms to combat the emerging cyber threats. **Ms. N. S. Nappinai** has authored a seminal book titled “**Technology Laws Decoded**”, which sets out the interplay between multiple laws for the cyber domain in detail. The book also analyses in depth, both the civil and criminal provisions and also internal and international enforcement. One aspect of the book, that stands out is her practitioner’s perspective on the need to review various aspects of cyber laws that require to be reviewed and recast. Ms. Nappinai also dons the role of Advisor to CPF.

CEPR, CPF together with Ms. N. S. Nappinai, have therefore conceptualized the need for this White Paper highlighting the urgency for an expedited review of the Information Technology Act, 2000, as amended

in 2008. The same will form the basis for the formulation of proposed amendments to the IT Act. Though the research undertaken by Ms. Nappinai goes into every aspect of cyber laws that require to be incorporated, reviewed or revised to meet the cyber security requirements of India, this White Paper authored by Ms. N. S. Nappinai sets out primarily the criminal provisions and the procedural aspects that require to be reviewed.

India is stepping out to create the next level of revolution in the digital space. It is only appropriate that it does so keeping in mind the security concerns and issues of the Nation and the People, who comprise it. CEPR, CPF and Ms. Nappinai believe that the above initiative and the outcomes therefrom will further India's goal to be a secure innovator in the field of Cyber.

WHITE PAPER ON THE NEED FOR PROPOSED AMENDMENTS TO THE IT ACT

1. Cyber Security & The Law

“There are two kinds of organizations: Those who have been hacked and those who will be.” - Kaffenberger, Lincoln (2015)⁵

The skeptical yet closer to reality quote of Kaffenberger forms the bedrock for the need for strong laws and its effective enforcement, for if vulnerabilities are inevitable, it is only the framework of the law that can protect users from rampant crimes.

Quoting from the book “Technology Laws Decoded”, *“Every computing system has its vulnerabilities and plugging the same is a continuous and evolving process. For with every closure of one loophole, the young and tech-savvy offenders find ten or probably more. The progressively decreasing demographic of cyber criminals is real cause for concern especially for a very ‘young India’. Keeping that aside, the primary concern more so in the light of the ‘Digital India’ movement ought to be for a stringent and effective ‘Cyber Security Policy.’”⁶*

It is for this reason that the criminal provisions of the IT Act have been dealt with first in this White Paper. For the security of the Nation, be it pertaining to law and order or protecting and preventing crimes, from within its territories or from outside rests on clear and precise laws being formulated and more importantly

⁵ <http://inpublicsafety.com/tag/cyberattacks/>;

⁶ Nappinai N. S. (2017), Technology Laws Decoded, published by LexisNexis.

implemented. The Government's role is that of a guardian protecting its Nation and the People comprising it would commence with the formulation and thereafter effective implementation of laws and regulations for societal good.

Absence of either simple and clear laws that would ensure due compliance by young and old in itself is against the common good. Law's role as a deterrent then becomes weak if not non-existent. The next level is of security that any State actor would require is for its laws to be duly implemented and enforced. Clarity in such laws therefore help not only to deter crime but to also help enforcement agencies such as the police and prosecutors to effectively implement the law. If these authorities themselves are unclear of what the law says, then the criminal justice system would fail us even at the first level.

The role of the judiciary is of utmost importance to ensure effective and expeditious enforcement against violations of law. There again clarity in law is most important, which is missing from the existing draft of the IT Act. The need for urgent review of the IT Act is manifest in the abysmal criminal prosecution statistics. A quick look at the statistics, which are themselves a bit outdated but that which is available online demonstrate the following.

2. Cybercrimes – The India Story So Far

Cybercrimes, as with the digital domain, have been spawning and growing exponentially. Crimes of this category are doubly dangerous, as the criminal is also more evolved. Whilst the cybercriminal has mastery over this domain, the same may not be applicable to the legal enforcement machinery. The system is already collapsing under the weight of existing prosecutions and proceedings. The double whammy of the increase of cybercrimes,

complexities in investigations and prosecutions thereof on the one hand and the need for speed given the tenuousness of electronic evidence on the other, highlights the need for urgent review of existing processes.

The speed of enforcement by law against cybercrimes is akin to the tortoise, which unfortunately is unable to keep pace with the technology here, thereby creating chaos and havoc not only in the world of the inimitable Indian but of businesses and industries. Recent trends in cybercrimes have given a clarion call to Nation-States to wake up to the reality of not just the larger issues of cyber terrorism but also cyber warfare.

The present report is restricted to cybercrime and its impact on law enforcement. The report highlights current statistics available online of pending cases falling within the domain of cyber. It highlights the urgent need for creating systemic changes to combat this real and present menace, with expedition.

a. Cybercrimes

India, as with most jurisdictions has sensibly shied away from defining cyber crimes⁷. Saudi Arabia's Anti-Cyber Crime Law⁸ is a rare instance of a statutory definition of "cybercrime", as "Any action, which involves the use of computers or computer networks, in violation of the provisions of this law".

Cybercrime today has grown and permeated fields, least expected. It is no longer the simple hacking of one system or spamming to block a competitor's mailbox. From hacking to virus attacks and denial of service attacks, the cybercriminal reaches out to bring down even

⁷ Nappinai N. S. (2017) "*Technology Laws Decoded*". Published by LexisNexis.

⁸ Royal Decree No. M/17.

Nations, their Internet, banking systems, media or even power plants⁹.

On business front, cybercrimes cause heavy and irreplaceable losses running in most instances to several crores of rupees. Individuals are affected doubly due not only to commission of crimes against them online ranging from Cyber stalking to cyber bullying and financial frauds.

The Supreme Court of India has taken *suo motu* cognizance of the menace of Rape Videos being hosted online for instance, in *Prajwala v. Union of India*¹⁰ and has recently appointed a Committee to review feasibility of rooting out this menace in a preemptive manner. Recent trends in such crimes highlights the menace of jilted paramours posting morphed pictures online (akin to a cyber acid attack) and “revenge porn” i.e., consensual acts of intimacy being uploaded online without the consent of partners. The colossal threat that child pornography poses was demonstrated with the recent arrest in India of an individual having over 20,000 images of child pornography. Innocent children fall prey due to online trolls engineering contact and then enticing children to expose themselves. Even without this, morphing seems to assuage these perverts’ requirements too. Further, instances of pictures taken on the streets being uploaded on sites dedicated to child pornography and also in general social media sites, throws serious doubts about existing enforcement mechanisms. Finally, present processes have proven to be sadly deficient in dealing with these menaces to women and children.

⁹ Estonia Attacks; Ukraine hacking attack and other such instances, enumerated in “*Technology Laws Decoded*” by Ms. N. S. Nappinai (refer supra);

¹⁰ *Suo Motu Writ Petition* (Crl). 3 of 2015;

b. Cybercrime Statistics

The details culled out from the National Crime Records Bureau for India, as of 2015¹¹, are set out hereunder.

i. Reporting of Cyber Crimes and Arrests¹²

Out of 9,622 cases of Cyber Crime reported in 2014, there were 5,752 people arrested, whereas in 2015 out of 11,592 cybercrime cases reported, 8,121 people were arrested. This translates to an increase of 20.5% cases reported and 41.2% accused being arrested.

In the beginning of 2015, there were 482 people in custody and 3695 people on bail during the investigation stage. The same number was 937 people and 5800 respectively at the end of 2015. 633 people were released or freed by police or the magistrate before trial for want of evidence or other reasons. 4928 people were charges sheeted in 2015.¹³

ii. Case pendency and closure rate¹⁴

Out of a total of 19,423 cases open for Investigation in 2015, 7,364 cases, were disposed of by Police and 11,789 cases were still pending investigation. Charge sheets were submitted only in 3206 cases (46.8%). Case pendency at end 2015 stood at 60.1%.

¹¹ Statistics set out in this report pertain to 2015, as they are the latest available online.

¹² <http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Table%2018.1.pdf>.

¹³ <http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Table%2018.5.pdf>

¹⁴ <http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Table%2018.2.pdf>

iii. Case status in Courts¹⁵

There were a total of 7,123 cases involving trial of Cyber Crimes in 2015. 640 trials of such cases were completed in 2014 resulting in 234 cases with convictions and 406 cases with acquittals/dismissals. 48 cases were either compounded or withdrawn. Conviction rate in completed trials was 36.6%. 90% cases were still pending.

In the beginning of 2015, there were 451 people in custody and 5155 people on bail during the trial stage. The same number was 1632 people and 630 respectively at the end of 2015. 10,534 people were under trial for cybercrimes in 2015.

302 people were convicted, 519 people were acquitted and 27 people were discharged by the Court. There 848 people for whom the trial was concluded in 2015. Cases were compounded against 67 people and against 10 people were withdrawn.¹⁶

iv. The 2016 Norton Cyber Security Insights Report¹⁷

Below are a few details, from the 2016 Norton Cyber Security Insights Report ("**Norton Report**"), with respect to cybercrimes in India¹⁸:

- a. 40% Indian parents allowed their children to access the internet before age 11
- b. 17% parents reported that their child was cyber bullied;

¹⁵ <http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Table%2018.3.pdf>

¹⁶ <http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Table%2018.6.pdf>

¹⁷ <http://economictimes.indiatimes.com/industry/tech/internet/2016-norton-cyber-security-insights-report-family-edition/articleshow/56731001.cms>;

¹⁸ <http://economictimes.indiatimes.com/industry/tech/internet/2016-norton-cyber-security-insights-report-family-edition/articleshow/56731001.cms>;

- c. 71% of parents had concerns that their children would download malicious programs or softwares;
- d. 69% of parents had concerns that their children disclosed too much personal and confidential information online;
- e. 65% of parents had concerns that their children would be lured by strangers online to meet them personally;

v. **Statistics for motives for Cyber Crimes in India¹⁹:**

Sr. No.	Motives	No. of Cases
1.	Personal Revenge / Settling Scores	304
2.	Emotional Motives like Anger, Revenge, etc.	223
3.	Greed / Financial Gain	3855
4.	Extortion	295
5.	Causing Disrepute	387
6.	Prank / Satisfaction of Gaining Control	214
7.	Fraud/Illegal Gain	1119
8.	Insult to Modesty of Women	606
9.	Sexual Exploitation	588
10.	Political Motives	47
11.	Inciting Hate Crimes Against Community	205
12.	Inciting Hate Crimes Against Country	12
13.	Disrupt Public Services	33
14.	Sale/ Purchase of Illegal Drugs/Items	14

¹⁹ <http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Table%2018.7.pdf>

15.	For developing own Business/Interest	170
16.	For spreading Piracy	185
17.	Serious Psychiatric Illness viz. perversion, etc.	12
18.	Steal Information for Espionage	22
19.	Motives of Blackmailing	293
20.	Others	3008

ASSOCHAM - Mahindra SSG study suggests that Cyber Crime is increasing at an alarming rate. According to the report, the number of Cyber Crimes in India may touch a humongous figure of 3,00,000 in 2015, almost double the level of last year²⁰.

The country has registered 107% of CAGR (Common Annual Growth Rate) in the number of Cyber Crimes registered in last few years.

c. Regulatory Mechanisms

Registering a complaint in a cybercrime case is in itself a nightmare and to a large extent the very impediments in this act as a deterrent to victims seeking remedies. There is much ambiguity and opacity with respect to the jurisdiction within which such a complaint needs to be registered.

Presently, for instance in Mumbai, cybercrime complaints may be filed either at the Cyber Crime Cell, Crawford Market Police Station, Mumbai or at the Cyber Crime Cell BKC Police station, Bandra East, Mumbai or even at the local jurisdictions, within which the offence

²⁰ <https://dazeinfo.com/2015/01/06/cyber-crimes-in-india-growth-2011-2015-study/>

is committed. In addition, Maharashtra has purportedly also initiated the e-FIR process. There should be rationalization across India and clarity on the available remedies and also the mode and manner of availing such remedies.

For the general litigant, such choice does not give clarity with respect to the best alternative. Further reality is that a victim is made to run from pillar to post to even get a Complaint taken on record. There is inordinate delay from the time of submission of Complaint to the registration thereof as First Information Reports (“FIR”). Such delays are sometimes fatal for effective prosecution of cybercrime cases, as electronic evidence is bound to be tampered with once notice of prosecution has already reached the perpetrator.

Absence of specialized investigation teams; provisions for search and seizure, which are followed more in their breach; lack of awareness and / or guidance at the stage of collation of evidence; want of specially trained prosecutors, who are familiar with the digital domain and its nuances and the heavy workload in courts, which delay prosecutions to such extent, as to make proving of electronic records nearly impossible, contribute to a very low conviction rate.

Litigants sometimes resort to settling cases instead of carrying prosecutions to its finality due to the delays and obstacles in cybercrime prosecutions.

In 2013, the NCRB recorded that 15.6% of cybercrime case, total such cases (681 out of 4,356 cases reported in India in 2013) were reported from Maharashtra.²¹ Further the report also discloses that 20.3% of the 2,098 persons arrested in cases relating to offences

²¹ <http://ncrb.nic.in/StatPublications/CII/CII2013/Chapters/18-Cyber%20Crimes.pdf>;

under the Information Technology Act, 2000 were from Maharashtra (i.e., a total of approximately 26 persons).

In 2013, Maharashtra also recorded the second highest number of Cybercrime cases relating to forgery (about 215 cases).

The NCRB has reported that as of 2014, in Maharashtra 1,879 cybercrime cases, were reported, being the highest number of such crimes accounting for 19.5% of total cybercrimes in India in 2014.²²

The above details set out a strong case for establishment of special machinery to deal with and dispose of cybercrime cases. absence of effective enforcement is merely likely to embolden the evolved cybercriminal. These statistics do not even take into account the complexities that extraterritorial enforcement poses.

d. Legislations / Policies

i. Proposed Amendments to the Information Technology Act, 2000²³

The Information Technology Act, 2000 was passed as a special legislation to deal with the intricacies that the digital domain raises in law. It is however by no means the only legislation applicable to the cyber domain. Pursuant to the said enactment, amendments were brought forth in general laws including the IPC and the Indian Evidence Act. Presently several general and special enactments include provisions impacting the digital domain and would therefore fall within the broader category of cyber laws. Criminal or penal

²² <http://ncrb.nic.in/StatPublications/CII/CII2014/chapters/Chapter%2018.pdf>;

²³ The amendments proposed are in furtherance of and in addition to or modification of the amendments carried out in 2008.

provisions under each such legislation would also be amenable to prosecution as cyber crimes²⁴.

The difficulty in enforcement arises in part due to this scattering of provisions across multiple legislations. Effective enforcement requires the system from police to courts to be aware of the interplay between the IT Act and other general and special legislations to give due effect to enforcing the same.

Some of the Criminal provisions requiring a review are set out hereunder:

A. / Amendments to IT Act

Chapter XI sets out the Criminal provisions in the IT Act. The modifications suggested to the same are, as under:

1. S.65 IT Act:

The heading to S.65 mentions the provision to be for punishing “tampering with Source documents” but the provision in full applies squarely to theft of source code. S.43(j) was introduced through the 2008 amendments to the IT Act to penalize stealing, concealing, destroying, altering source codes or causing the same to be done with intent to cause damage. This is also made an offence through reading S.66 with S.43, when such act is committed with dishonest and fraudulent intent.

There is a clear overlap between the two provisions. This overlap and also the fact that a provision has to be read backwards to even figure out that it is a criminal offence in certain

²⁴ Refer Chapter 2 “*Technology & Crimes*” in the book “*Technology Laws Decoded*” by Ms. N. S. Nappinai, Advocate. Published by LexisNexis.

circumstances are patent impediments in effective enforcement. Possibly S.43(j) IT Act was introduced with intent to either delete S.65 (as was done with the old S.66) or it was meant to add to the provisions therein.

Either way it is pertinent to review both provisions and to harmonize the same.

Recommendation:

S.65 IT Act and S.43(j) IT Act to be reviewed and harmonized. Both provisions may also be combined into one provision i.e., under S.65 and the other deleted.

2. S.66 IT Act:

S.66 IT Act makes any offence set out under S.43 IT Act, when committed with dishonest and fraudulent intent to be punishable. S.43 however sets out as many as NINE sub-sections. Each of these being a separate offence in themselves like hacking, virus attacks, denial of service attacks and data theft, it is imperative that these be set out separately under specific heads. Further law's role, as a deterrent disappears with such ambiguity and opacity in the law.

It is important that a reasonable person knows what actions are offences and what he therefore should not commit. The Supreme Court elucidated on this in *Kartar Singh v. State of Punjab*²⁵. This will also help police to enforce each head of offence separately and to collect the evidence required to sustain a prosecution under each head.

²⁵ (1994) 3 SCC 569 ; refer also *Shreya Singhal v. UOI*. The importance of such clarity is set out in more detail in the Chapter "Technology & Crimes" (supra);

Similarly, judiciary will also be better equipped to deal with such cases in a more focused manner. The detailed analyses warranting the above change is more fully set out in the author's book²⁶.

Recommendation:

1. To set out separate heads of offences under S.66 for each of the offences forming part of S.43 of the IT Act;
2. To review the errors and omissions in S.43(i) r/w S. 66 IT Act to ensure that it is not misused;
3. To review the inconsistency in S.43(j) and S.65, as set out above;

3. S.66 r/w S.43(i) IT Act:

In addition to the generality of the above, S.43(i) IT Act may be reviewed and either deleted or modified. The same makes destruction, deletion or alternation of information residing in a computer resource **or** diminishing its value **or** utility **or** affecting it injuriously a civil and criminal penalty.

In *Shreya Singhal v. UOI*²⁷, the Supreme Court held the addition of *mens rea* to help sustain the constitutionality of S.66 IT Act. The Hon'ble Court however does not go into the error specific to S.43(i) IT Act. The absence of *Actus Reus* and the implications thereof along with case studies are more fully set out in the book "Technology Laws Decoded" by N. S. Nappinai²⁸ and the same

²⁶ Supra;

²⁷ Supra;

²⁸ Pl refer Pg.115-140; Chapter 2 of the said book for pointers;

may be read as part hereof to support the need for either amending the above provision to read “and” wherever the word “or” is highlighted above.

Recommendation:

Amendment of S.43(i) IT Act, as above.

4. S.66 C IT Act:

This provision to combat identity theft is precise except for the absence of precision in the definition of the parameters such as biometrics which warrant initiation of prosecution. Specific instances or addition of illustrations would help invoking this provision including for cases of phishing.

Recommendation:

- a. Clarity in the parameters of “identity” that are protected under the provision;
- b. Addition of illustrations;

5. S.66 D IT Act:

This provision is on par with the IPC provision for cheating by personation but applies to the online domain. The same may be harmonized. Whilst this addition is most relevant especially in cases of phishing and banking frauds, addition of illustrations will give pointers to victims of the remedies available under law.

Recommendation:

- a. Addition of illustrations;

- b. Harmonizing with IPC;

6. S.66 E IT Act:

S.66E, even in its limited application to publishing or transmission of images or videos of private parts of individuals without their consent, has been put to much misuse in the short period of its existence. However, for the sake of upholding privacy, the constitutional mandate of which has now been definitively affirmed by the Hon'ble Supreme Court in *Justice Puttaswamy v. Union of India*²⁹, and despite the possibility of its abuse, it may be imperative to review the provision to include protection of privacy of persons and not just of their private parts.

The analysis, as in the above instances, is done in detail in the book of the author, as set out above. The same may be referred for further details and analysis.

This provision is also squarely applicable for offences of “Revenge Porn” and the heinous offences of rape and gang rape videos being uploaded online. In such cases, a more stringent punishment than what is presently prescribed would be warranted. The same would then act as a deterrent and also help combat the above types of crimes against especially women and children.

Recommendation:

- a. To review and amend to include a larger protective measure of privacy of individuals.

²⁹ Available at:

http://supremecourtindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf;

- b. To have two levels of punishments – a simple and lesser punishment for violation of general privacy and a more stringent punishment of higher sentence for serious offences such as “Revenge Porn”;
- c. To make such higher levels of offences to be non – bailable offences;
- d. To review and strengthen restrictions on compounding of serious offences under this provision;
- e. To impose specific timelines for initiation of prosecution and for completion of trials;

7. S.66 F IT Act:

S.66F dealing with cyber terrorism, was single-handedly the reason for the expedited passing of the IT Act. This was included after the Mumbai attacks in 2008.

Whilst S.66F (A) is suitably signposted to ensure that it is not abused, the same is not the case with S.66F(B) IT Act. The same therefore requires urgent review and amendments. This provision is already being put to much abuse. The same would merely increase and the intent and purpose of the legislation will otherwise be lost.

A more detailed discussion and analysis of this provision and what ails it, is set out in the book Technology Laws Decoded by N. S. Nappinai.

Recommendation:

- a. S.66F(B) IT Act to be reviewed and deleted;
- b. Suitable amendments to S.66F(A) be introduced without the same becoming a blanket provision for abuse;

8. S.67 IT Act:

S.67 IT Act is similar to S.292 IPC. Yet the same have not been harmonized and the IT Act provision is “*not tempered with the exceptions set out in S.292*”³⁰ which protect free speech and expression. Recently, S.67 IT Act has also been put to much abuse after the strike down of S.66A. It is being used to initiate prosecutions for so called “cyber defamation”. To curtail the same exceptions may be specifically set out and also illustrations.

This provision may also be called into effect for combating revenge porn cases. For this, it is imperative that higher punishment is prescribed as a separate head under this provision for such cases which fall short of “sexually explicit acts”, which would otherwise fall under S.67A IT Act;

Recommendation:

- a. Exceptions, as in S.292 IPC may be specifically set out in S.67;
- b. Illustrations be added to bring clarity to the actual applicability of the provision;
- c. Higher punishment for cases such as revenge porn to be prescribed;
- d. Consequently, revenge porn cases to be non – bailable offences;

³⁰ Nappinai N. S (2017) in Technology Laws Decoded (Supra);

9. S.69 – S.69B IT Act:

S.69, S.69A and S.69B deal with decryption, monitoring and blocking of content online. Rules have been framed under these provisions to provide checks and balances. However, many of these are circular and mostly the same Government entities are in charge of ordering the above actions, which are otherwise infringement of civil rights³¹.

It is therefore imperative that these provisions be reviewed, as well as the rules framed thereunder to ensure due protection of free speech and expression.

It is also noted that India tops the list of nations where the maximum instances of Internet blockages have been ordered. This is being done in most instances, by resorting to S.144 Cr. P. C instead of the more stringent provisions set out above under the IT Act. There should be explicit provisions for review of such orders also by the Competent Authorities to ensure that a faster and alternative remedy is available to victims. This will also help deter such rampant misuse of Cr. P.C provisions.

Recommendation:

- a. S.69, 69A and 69B and Rules framed thereunder to be reviewed and recast;

³¹ Refer pages 248-252 of Technology Laws Decoded by N. S. Nappinai (Supra);

- b. More stringent provisions to be included for implementation to stop / deter circumvention of checks and balances;
- c. Monitoring committees to either be absolutely independent entities or to have independent members with suitable powers for calling for meetings; reviewing orders for monitoring or blocking of web content and for reversing the same or implementing the orders of the committee;

B. Additions to IT Act

The following may be required to be added in the IT Act, more so in the light of the strike down of S.66A:

1. Cyber Bullying

S.66A IT Act was primarily called to use to combat cyber bullying of various forms. Its rampant abuse resulted in its strike down by the Supreme Court in *Shreya Singhal v. UOI*³². It is important for India to evaluate the need for a specific and precise provision (unlike the open-ended one in the struck down S.66A) to combat cyber bullying.

The instances of extreme verbal violence and “trolling” have now even resulted in personal harm to individuals. In some instances it has also resulted in loss of life. Admittedly such instances of bullying or trolling definitely take its toll on the mental health of victims. Hence the need for this urgent addition.

³² Supra;

Recommendations:

- a. Addition of a provision to combat Cyber bullying;
- b. The provision to be precise and not open-ended;
- c. Addition of illustrations to ensure correct application;

2. Self – Harm

The blue whale incidents highlighted the need for specific provisions to combat instances of self-harm or instigation thereof. IPC offences can be invoked in such cases including of aiding and abetting commission of offences. Yet, to ensure that there is deterrence of such actions, it is important to ensure that there are specific and special provisions for the same.

Recommendations:

- a. The formulation of the above i.e., specific provisions to combat offences of instigation of self – harm may be evaluated and included in the IT Act;

3. Hate Speech

There is already a proposal for including a specific provision for combating hate speech through addition of a new S.66A in the IT Act. It may be imperative to keep in mind the need to protect free speech and expression, while formulating such provisions.

Recommendation:

- a. To carefully evaluate any such proposed inclusions to ensure protection of free speech and expression online;
- b. Nothing done ought to impinge on free speech including possible misuse of such provisions;

A. Review of Procedural Laws**1. S.65A & S.65B of the Indian Evidence Act, 1872**

S.65B and the requirement of a certificate under S.65B(4) of the IEA were heavily drawn from UK laws. The UK law itself underwent changes before the above provisions were introduced. Yet the above provisions were introduced into Indian laws.

The complicated and convoluted requirements under S.65B have and will continue to cause grave harm in enforcing against cybercrimes. It is therefore most urgent that this provision be reviewed, as also the other amendments that were brought into the IEA.

Recommendations:

- a. S.65B to be amended to make the procedures simple and transparent for proving secondary forms of electronic records;
- b. Other amendments of Indian Evidence Act, 1872 to be reviewed to ensure harmonization and effective implementation³³.

³³ Refer Chapter 5 of Technology Laws Decoded by N. S. Nappinai (supra) for a more detailed discussion on the amendments required;

2. Jurisdiction

S.75 of the IT Act provides extra territorial jurisdiction for enforcement of the provisions of the Act. This section however and the provisions under IPC and Cr. P. C have not been harmonized. With prosecutions being initiated under multiple legislations, it is important for harmony between all of these enactments.

Recommendation:

- a. To review provisions for applicability of Criminal jurisdiction under general laws (IPC and Cr.P.C) and the IT Act and to harmonize all three³⁴;
- b. To formulate Cyber Policies for ease of enforcement across borders, as most cybercrimes are multi-jurisdictional³⁵;

3. Other Amendments:

a. Appointment of Special Tribunals / Appellate Authority for Cyber:

The discussion above only sets out the recommendations for the Criminal justice system. Civil remedies also require much harmonization and amendments. For instance, the post of Adjudicating officer was created under S.46 of the IT Act.

Whilst this was to be a separate Tribunal, the same was never constituted and this authority now stands vested with the

³⁴ Refer to Chapter 5 (Supra) for detailed discussions;

³⁵ Refer to Chapter 7 of the book Technology Laws Decoded by N. S. Nappinai (Supra) for a detailed discussion on the need for effective international enforcement mechanisms;

Secretary, Ministry of IT. Judicial functions have therefore been vested with the executive. Apart from this overlap itself causing problems, there are innumerable legal and logistical problems that affect victims of cyber violations under S.43 IT Act.

It is important to provide a quick and inexpensive remedy to victims. Cases of phishing for instance have mostly been dealt with by this authority. However, the same should not be merely an authority which otherwise provides very extensive functions. This will merely result in inordinate delay in handling of such cases.

Vesting the authority with the Cyber Appellate Tribunal with TDSAT is also counterintuitive and counterproductive. Non-appointment of this authority since 2011 has itself caused huge backlogs. To now combine the same with a completely unrelated Tribunal, which may not be equipped to deal with the same is self-defeating.

Recommendation

- a. A separate Tribunal to handle civil remedies under the IT Act to be constituted;
- b. Cyber Appellate Tribunal to be reinstated and the Chairperson to be appointed, as per the provisions of the IT Act;
- c. Awareness of victim rights to be created extensively to ensure clarity and to provide effective remedies;

b. Intermediary Liability:

IT Act 2000 provided very limited protection for intermediaries. Pursuant to cases such as *Avinash Bajaj Vs. State of Delhi*³⁶, S.79 IT Act was revised. Intermediary Rules have also been formulated setting out the preventive and protective measures to be adopted. Of this Rule 3(4) was read down in the case of *Shreya Singhal*³⁷.

The amended S.79 IT Act still gives much leeway for interpretation and may therefore be counterproductive both from the perspective of the intermediaries as well as victims. It is therefore time for this provision as well as the Intermediary rules to be reviewed to ensure that there is absolute clarity on (a) the rights and protections accruing to intermediaries; (b) their duties and (c) the penalties for violation.

Recommendation:

- a. To review and revise / amend S.79 to ensure balancing of rights and duties of Intermediaries qua victims and Indian law enforcement agencies and Courts;

e. Policies & Government Initiatives

In addition to the legislations, after rampant zero day attacks³⁸, the Indian Government also formulated the **National Cyber**

³⁶ Criminal Prosecution initiated in the Delhi MMS circulation case, which was decided in *Aneeta Hada Vs. Godfather Travels & Tours Pvt., Ltd.*, (2012) 5 SCC, 661; Also see *Sharat Babu Digumarti Vs. State, Govt. of NCT of Delhi*, 2015 SCC OnLine Del 11591;

³⁷ *Supra*;

³⁸ Unprecedented and unexpected attacks, which took place across the world.

Security Policy, 2013³⁹. For the first time “cyber security” became a catch word and critical infrastructure were identified, as national vulnerabilities requiring special attention.

The Government has also given impetus to other initiatives including the proposal for setting up the Cyber Crime Prevention Against Women And Children (“CCPWC”). These are primarily Central Government initiatives with the first being a general initiative, which also touches upon protection of women and children from online crimes. The timelines for implementation of both of these schemes are still open-ended, with IC4 in fact still remaining to be approved.

f. Judiciary and Cyber Crimes

It was earlier suggested in or about 2004 that Special Courts should be assigned to deal with cybercrimes. However, the idea was mooted, as at that time the Government felt that, at that time, the number of cases did not warrant the additional expenditure.

Today, enforcement agencies⁴⁰ and Courts, have realized the importance and need for special courts to deal with cybercrime cases.⁴¹ In the light of present statistics with respect to increasing cybercrime cases, the time is now ripe for appointment of Special Courts, to deal specifically with cybercrime cases. In fact a separate machinery of special prosecutors and Courts and also specially trained police may be the need of the hour to combat the rising menace of cybercrimes.

³⁹ Available at: <http://meity.gov.in/content/national-cyber-security-policy-2013-1>;

⁴⁰ <http://www.dnaindia.com/mumbai/report-two-special-courts-for-cyber-crimes-mumbai-police-writes-to-home-department-2168670>;

⁴¹ <http://timesofindia.indiatimes.com/city/ahmedabad/Special-courts-needed-for-cases-of-cyber-crime/articleshow/54400724.cms>;

g. International Perspective

In Singapore, in or about September 2016, a Special Court was set up in Kuala Lumpur court complex in Jalan Duta to handle the increasing number of cybercrime cases⁴².

The Special Court was set up, equipped with proper facilities as well as with highly trained Judges and Prosecutors to deal with cybercrime cases.

h. Suggestions

India is ill-equipped to deal with emerging threats and attacks on the cyber domain and secondly that India continues its policy of reactive responses rather than proactive measures to meet the cyber security challenges. The various issues and concerns highlighted above mandate the urgent need for a quick rethink by India and to put in place effective enforcement alternatives⁴³. The pointers set out above of the various provisions requiring review and amendments in the IT Act and the suggestions set out hereunder are merely preliminary inputs, which require to be further elaborated upon. These suggestions would indeed alleviate the problems faced by many a victim of cybercrimes. With the menace of cyber terrorism and cyber warfare looming, India has to take the first step to combat effectively cybercrimes in its jurisdiction to even consider the process of dealing with larger offences against the Nation.

The suggestions in brief are:

⁴² <http://www.thestar.com.my/news/nation/2016/09/01/first-cyber-court-in-jalan-duta-activated/#rM38kVozm7W0aYMU.99>;

⁴³ Absence of effective enforcement, is referred to, as “Broken Windows in Cyberspace”, in Chapter 7 of her book “*Technology Laws Decoded*” written by Ms. N. S. Nappinai, Advocate. Published by LexisNexis (2017).

- Review and Formulation of a more robust Cyber Security Policy for India;
- Review and amendment of the Information Technology Act, 2000 (as amended);
- Assignment of Special Courts to deal with cybercrimes;
- Offences against women and children to be given special and urgent status for expeditious disposal⁴⁴.
- Assignment of Special Prosecutors for such Special Courts for Cybercrime, who are duly trained;
- Cyber and cyber law training of police personnel across India to ensure effective enforcement against cybercrime;
- Specially trained task forces to be deputed for collating evidence in cybercrime cases;
- Special prosecutors to be assigned for accompanying police to crime sites to oversee such collation of evidence;
- Chain of custody of evidence to be ensured;
- Cyber forensic labs / capacity to be increased to remove backlog and fixed timelines to be given to such labs for submission of reports;
- Clarity in filing, acknowledgment and registration of cybercrime cases to be ensured;
- Details for the initiatives, laws, regulations and remedies available to the victims and public to be made available online in a National Website;
- Filing of cybercrime cases and its suitable allocation and progress to be facilitated online with transparency about the filing, status and developments therein;
- Case laws from all Courts including lower courts, which would not be precedents but which would guide other

⁴⁴ A recent case in Pune demonstrated that a case of cyber stalking could be investigated and disposed off in 48 hours;

victims to be clearly set out online in the National Portal / Website;

- Timelines to be fixed for receipt to disposal of cybercrime investigations;
- Reasons to be recorded by police for non-registration of complaints;
- Power of supervision under S.154(3) Cr.P.C. to be exercised proactively in cybercrime cases;
- All courts across the State to give priority to cybercrime cases in jurisdictions without specially designated Courts;

In conclusion, it is only fitting to reproduce Justice Krishna Iyer's quote that "An '*ephemeral*' measure to meet a perennial menace is neither a logical step nor national fulfilment." (Nappinai. N. S. (2017))^{45 46}. Hence merely having vague or ambiguous provisions to combat a growing menace is neither sufficient nor justifies the role of Government and its commitments to its populace. Any measure to combat the serious and growing menace of cybercrime would therefore have to be concrete and effective. Else applying band - aids to a wound, as and when it comes to the fore, is neither going to heal the wound nor prevent them from reappearing or increasing in intensity.

⁴⁵ Justice V. R. Krishna Iyer, In Re The Special Courts Bill v. Unknown, AIR 1979 SC 478 : (1979) 1 SCC 380 : (1979) 2 SCR 476.

⁴⁶ Chapter 2, Page 289, "Technology Laws Decoded", by N. S. Nappinai. Published by LexisNexis (2017);

Acknowledgement

The Author Ms. N. S. Nappinai is an Advocate practicing in the Supreme Court of India and the Bombay High Court and the author of the book “Technology Laws Decoded. She has relied on her practical experience and expertise in the field of cyber laws in the preparation of this above White Paper.

Cyber Peace Foundation and Centre for Economic Policy Research have ably assisted and contributed to the above through their vast experience in conducting and facilitating many national consultations, conferences and meetings to reconcile workable action points towards developing progressive policies and frameworks. This paper follows many leads from such proceedings.

The Author thanks the entire team of Cyber Peace Foundation, which she is also a part of, as its Advisor, through whose efforts, the need of an immediate intervention in this domain was felt. She also acknowledges the able contribution of her team of Advocate Ms. Noelle Ann Park, Advocate Mr. Akhil Mahesh and Mr. Rohmin Aref, Advocate, at the Law Firm Nappinai & Co., Advocates, situated at Delhi, Mumbai & Chennai. She also places on record her appreciation for the Cyber Peace Foundation’s team of Ms. Titiksha Seth, Ms. Sahana Chaudhri, Ms. Janice Verghese, Ms. Sukhmani Kaur, Mr. Raj Pagariya and Mr. Abhay Singh Sengar from University of Petroleum and Energy Studies, Dehradun for contributing towards the materialization of this paper.

Acknowledgements

1. Shri Shwait Malik, MP, Rajya Sabha
2. Dr. Ashwani Mahajan, National Co-Convener, Swadeshi Jagran Manch
3. Dr. Subhash Sharma, Director, CEPR
4. Shri Devansh Sinha, Convenor for Cyber Security, CEPR
5. Shri Vineet Kumar, President, Cyber Peace Foundation
5. Shri NC Bipindra, Convenor, Forum for Integrated National Security
6. Shri Rakshit Tondon, Cyber security professional & advisor
7. Shri Dinesh Bareja, Infosec Practitioner, consultant & advisor
8. Shri Anil Sharma, Director, UCO Bank
9. Shri Rajiv Nayan, IDSA
10. Shri Santosh Khadsare, Information Security and Cyber Forensics Professional
11. Shri Kislay Chaudhuri
12. Shri Shri Uttam Kumar Sinha, IDSA
13. Shri Navdeep Singh Brar, IPS
14. Shri Pavan Duggal, Advocate, Supreme Court of India



"IN PURSUIT OF CYBER PEACE"

Secretariat : B-55, Birsa Munda Rajpath Harmu Housing Colony,
Ranchi Jharkhand Pin - 834002 India Ph.: +91.651.645 8865

Delhi : K-51 (First Floor) Green park Main, New Delhi - 110016



INDIA : +91 82350 58865



USA : +1 71624 11555



UK : +44 20 32870765

email: secretariat@cyberpeace.net

www.cyberpeace.org



/cyberpeacefoundation



/cyberpeacengo



/cyberpeacefoundation