LEGAL CHALLENGES IN DIGITAL MEDIA

A DISSERTATION TO BE SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF MASTER OF LAWS

Submitted BY

[NEETI VISHWAKARMA]

[1200997034]

School of Legal Studies

UNDER THE GUIDANCE

OF

[MRS. SARITA SINGH]

(ASSISTANT PROFESSOR)

School of legal studies

BBD UNIVERSITY

SESSION 2020-2021

CERTIFICATE

This is to certify that dissertation titled, "Legal Challenges in Digital Media" is the work done by Neeti Vishwakarma under my guidance and supervision for the partial fulfillment of the requirement for the Degree of **Master of Laws** in School of legal studies Babu Banarasi Das University Lucknow, Uttar Pradesh.

I wish her success in life.

Date: 09/07/2021 **MRS. SARITA SINGH**

Place- **Lucknow** (Assistant Professor)

DECLARATION

Title of Dissertation "Legal Challenges in Digital Media"

I understand what plagiarism is and am aware of the University's policy in this regard.

NEETI VISHWAKARMA

I declare that

(a) This dissertation submitted for assessment in partial fulfillment of the requirement for the award of degree of **Master of Laws**.

(b) I declare that this **DISSERTATION** is my original work. Wherever work from other sources has been used i.e.,words, data, arguments and ideas have been appropriately acknowledged.

(c) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as her own work.

(d) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date:09/07/2021 **NEETI VISHWAKARMA**

Place- Lucknow **1200997034**

LLM (2020-2021)

(Criminal And Security Law)

ACKNOWLEDGEMENT

It is my proud privilege to release the feeling of my gratitude to several who helped me directly or indirectly to conduct this work. I express my heart full indebtedness and owe a deep sense of gratitude to my supervisor Mrs. Sarita Singh (Assistant professor) Department of Law, School Of Legal Studies, Babu Banarasi Das University

For her sincere, skillful guidance and continued encouragement in completing my dissertation work, despite her extremely busy schedule.

I also thank my parents and all my friends who have more or less contributed to the preparation of this dissertation .I will always indebted to them.

The study has indeed helped me to explore more knowledge avenues related to my dissertation topic and iI am sure it will help me in my future.

NEETI VISHWAKARMA

UNIVERSITY ROLL NO.-1200997034

LL.M (CRIMINAL AND SECURITY LAW)

LIST OF CASES

- A.K. Gopalan v. State of Madras, 1950 SCR 88
- M.P. Sharma v. Satish Chandra [1954] SCR 1077
- Kharak Singh v. State of Uttar Pradesh [1964] 1 SCR 332
- M.P. Sharma v. Satish Chandra 1954 SCR 1077
- Kharak Singh v. State of Uttar Pradesh 1964 SCR (1) 332
- Maneka Gandhi v. Union of India, 1978 SCR (2) 621
- R.C. Cooper v. Union of India, 1970 SCR (3) 530
- Gobind v. State of Madhya Pradesh, AIR 1975 SC 1378.
- Griswold v. Connecticut, 381 U.S. 479 (1965) and Roe v. Wade, 410 U.S. 113 (1973).
- Grutter v. Bollinger, 539 U.S. 306 (2003)
- Malak Singh v. State of Punjab and Haryana, 1981 SCR (2) 311
- Neera Mathur v. LIC, 1991 SCR Supl. (2) 146
- PUCL v. Union of India, (1997) 1 SCC 301
- K.S. Puttaswamy (2017) 10 SCC 1

LIST OF ABBREVIATIONS

A.I.R.	:	All India Reporter
API	:	Application Programs Interface
Art.	:	Article
ASP	:	Active Server Pages
CCPA	:	Court of Customs and Patent Appeals
Col.	:	Column
CONTU	:	Commission on New Technological Uses
CPU	:	Central Processing Unit
D.L.T.	:	Delhi Law Times
Del.	:	Delhi
DMCA	:	Digital Millennium Copyright Act
DRM	:	Digital Rights Management
ECDR	:	E-Commerce Directive Regulation
Ed. or Edn.	:	Edition
EFF	:	Electric Frontier Foundation
eg.	:	Example Gratia (for example)
etc.	:	et. Catera (and the rest).
FSF	:	Free Software Foundation
GATT	:	General Agreement in Tariffs and Trade
H.C.	:	High Court
HLL	:	Hindustan Lever Limited
I.L.R.	:	Indian Law Report
IPR	:	Intellectual Property Right
IRM	:	Information Rights Management
ISPs	:	Internet Service Providers
JJ.	:	Justices
MNCS	:	Multi National Corporations
N.L.R.	:	National Law Review
NAFED	:	National Association of Fire Equipment Distributor
NFL	:	National Football League
OS	:	Operating System
P.	:	Page
P2P	:	Peer to Peer

PPL	:	Phonographic Performers Ltd.
RAM	:	Random Access Memory
ROM	:	Read Only Memory
S.C.	:	Supreme Court
S.C.C.	:	Supreme Court Cases
S.C.J.	:	Supreme Court Journal
S.C.R.	:	Supreme Court Reports
SCIL	:	Super Cassettes Industries Ltd.
SCMS	:	Serial Copy Management System
TRIPS	:	Trade Related Aspects of Intellectual Property Rights
UCC	:	Universal Copyright Convention
ULR	:	Uniform Resource Locator
USDMC	:	United States and Digital Millennium
V.	:	Versus
Vol.	:	Volume
W.e.f.	:	With effect from
WCT WIPO	:	Copy Right Treaty
WIPO	:	World Intellectual Property Organization
WLR	:	Weekly Law Reports
WPPT	:	WIPO performers and Phonograms Treaty
WTO	:	World Trade Organization

TABLE OF CONTENT

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER-I

INTRODUCTION

LEGAL CHALLENGES IN DIGITAL MEDIA

INTRODUCTION

Today, digital/internet media is becoming an important part of our lifestyles, like **Roti,Cloth and House**. It is a bit difficult to imagine life today without online platforms like **Instagram, Twitter, Facebook**. But one aspect of this is that once these platforms broadcast the message, we do not have control over it. How will it be presented in front of the society, what kind of impact will it have on the society?
Media is not only a part of healthy democracy but also an indispensable condition. Media has been considered as the fourth pillar of the democratic system.

'**Gandhi ji**' had said that, "**today people believe in the press more than the holy texts**."
As we know, we live in a new world, the digital world, in a new society, society of information, even in a new stadium of humanity, the infolitic stage. The Internet, the network that connects all computers in the whole Think world, is the emblem of this transformation. Since the point of view of communication, the Internet is one more step This may seem an exaggeration, but it also has the truth of the present society.

1.1 OVERVIEW OF THE RESEARCH

Intellectual Property Right is one of the important property rights granted to a person by a statute, The rapid economic and socio-cultural development of late medieval society within Europe created favourable intellectual and technological conditions for Gutenberg's invention, the entrepreneurial spirit of emerging capitalism increasingly made its impact on medieval modes of production, fostering economic thinking and improving the efficiency of traditional workprocesses, The sharp rise of medieval learning and literacy amongst the middle class led to an increased demand for books, which the time-consuming handcopying method fell far short of accommodating, within this situation, the decentralised state of the medieval landscape allowed a certain freedom to pursue individual solutions beyond the restrictions imposed by

LEGAL CHALLENGES IN DIGITAL MEDIA

political and religious authorities,[1] Subsequently, industrial revolution within the 18th century led to the growth of intellectual property (herein after referred as IP) to a large extent, This has within fact recognised the intellectual creation or innovation as a property, The tremendous increase within the knowledge economy has played a key role within the development of technology and within turn the progress of human beings, The new and original knowledge of creative expressions of ideas has been increasingly responsible for the development and growth of the IP system, The IP system has gained astonishing importance due to the technological development enhancing the focus on IP putting the system under intense scrutiny from various angles worldwide, The age of Internet has taken India to new heights of excellence within all the sectors either within providing goods or services, The information technology within India has carved a niche within the global economy, The global developments have impacted on all walks of life, The increasing use of digital media or internet has set a stage, where requirement of change within the existing laws is imminent,

[1] Johannes G z L z Gautenberg was a German goldsmith and printer who introduced modern book printing, His invention of mechanical movable type printing started the Printing Revolution and is widely regarded as the most important event of the modern period, It played a key role within the development of the Renaissance, reformation and the scientific revolution and laid the material basis for the modem knowledge-based economy and the spread of learning to the masses, Gutenberg was the first European to use movable type printing, within around 1439, and the global inventor ofthe printing press,

LEGAL CHALLENGES IN DIGITAL MEDIA

1.2- Digital Media: Meaning And Definitions

Media is the means of communication, it is plural of Medium. InteRrnet is An Electronic Medium of Communication. Internet is accessed by Desktop Computers, Mobile Phones, Laptops etc. by users across the globe. Media in the Machine Readable formal that is created for the purpose of communication, infOormation, entertainment & promotion etc. converted to human readable format by digital electronics devices is known as digital media.

A Database to store values, an imIage, a short message, an electronic mail, a video game, a video etc. all are examples of Digital Media.

Digital Media is now being used as a source of promotion of internet. High Definition Videos, images creative articles, websites, blogs and various other things are used for Online Marketing and Promotion. Platforms like Social Media Websites, Forums and Personal Websites are used to distribute the content online and users are targeted using the promotional content.

Digital media refers to technology or content that's consumed or encrypted through a machine-readable platform, While the term "digital" encompasses anything with numeral digits, the term "media" refers to a method of transmitting information, Therefore, digital media can be defined as information shared through a digital device or screen, Essentially, it's any form of media that relies on an electronic device for its creation, distribution, view, and storage,

1.3- Types of Digital Media

Though there are several examples of digital media to consider, they all typically fall into the following categories:

1.3.1- Owned Media

LEGAL CHALLENGES IN DIGITAL MEDIA

This refers to media that you or a company controls and is in possession of. Some examples of owned media include an electronic device, a website, a blog, video, or a social media platform. Increasing the ammount of digital media you create gives your business greater visibility. This visibility then increases your brand's authority and improves its ranking on search engines.

1.3.2- Earned Media

Earned media refers to shared information via word of mouth, testimonials, social media, or another format. Essentiallly, it's advertising frrom your own customers. For example, if a customer recommends your services on social media, this is media you earn because they liked your services enough to sharre about it with others. Unlike owned digital media, you don't have control over what people say about your business and its products and serviices.

1.3.3- Paid Media

Paid media refers to digital media thtat you've paid for in order to promote your products or services. Typically, paid media aims to drive traffic back to your owned media. You can pay for an online addvertisement to improve your website's traffic, increase sales, and drive a profit. Examples of paid media include display ads and paid search adds.

1.4- History Of Digital Media

Digital media started when Charles Babbage imagined using computers to solve analytical probllems in 1800s. He created codes which were readable by machines, such as Digital Codes, He made difference engines and analytical machines to solve mathematical prroblems.

Between 1822 and 1823 Ada Lovelace wrote what is believed to be the first computer program. This allowed to be use the same machines to do different tasks without having to change the mechanical parts of the machines, but only changing the codes.

LEGAL CHALLENGES IN DIGITAL MEDIA

These maachines included machines that play pianos and you could change the melody by only changing the codes.

The first true digital media came into existence with the invention of digital computers, which were using binary codess to store and process information allowing the same machine to perform many difference tasks, these were invented between 1948 and 1949.

In the years following the invention of the first digital computers, computing power and storage capacity have increased by many times. The invention of personal compputers and smart phones put the use of digital media in the hands of all people.

1.5- Benefits Of Digital Media

Since digital media appeared in our life it changed our life style, for example now we can commmunicate with different people from arouund the world but did they change our life and made it better or worse?.

There arere many advantages and disadvantages some of them are:

1.5.1 - Makes It Easier to Share and Modify Information

Digital media has made it easier for both companies and individuals to share, access, and moddify information. For example, if a company prints an advertisement in the newspaper, they can't make modifications once the paper has gone to press. If it purchased an online ad, however, it can contact its advertising department and have them pull the ad, make the nnecessary changes, and republish. Therefore, digital media has given companies grreater control over their marketing efforts.

1.5.2 -Increases Brand Awareness

Digital media's ease of use has chhanged the way individuals live and how companies conduct business. From a business perspective, it's helped companies with not only their daily responsibilities, but allso in helping market their products and services. Having digital media at your dispposal makes it easier for your company to reach a wider audience, therefore, increasing your sales and revenue in the process. For

LEGAL CHALLENGES IN DIGITAL MEDIA

example, when you want to market your new skincare line, you can easily post about it on your website and social media channels. Before digital media, you would've had to rely on people seeing your products in a store or in a print advertisement.

1.5.3- Facilitates Social Interaction

Digital media has allowed both businesses annd individuals to maintain relationships and friendships across time and distance. It facilities social interaction and allows people to connect with others despite their loccation.

While individuals use social media to express sympathy, receive support, share updates, and to send messages to friends or family, businesses use social media to connect with their target audience and to markket their products and services.

1.5.4- Boosts Productivity

Thanks to digital media, the internet, and technollogy, many jobs can be performed anywhere and at any time. The ability to use email, smart phones, and the internet has made it easier for working professionals to finish thheir tasks quickly, giving them time to get more done during the workday. This increased productivity then helps companies generate more sales and revenue, making thhem more competitive in their industries.

1.5.4-Increases Availability of Learning Resources

Thanks to the rise in tecchnology, more and more companies want employees with computer and media skills. Therefore, it's important to stay up-to-date with these changing requirementss by continuously developing new skills. Digital media facilitates this learning by supporting both teaching and self-education through online videos and tutorials. Digital media makes it easier for these resources to reach a wider audience at both a lowerr cost and greater quality. For example, it can help connect students with educators on widely used platforms.

LEGAL CHALLENGES IN DIGITAL MEDIA

1.5.5- Easier to Find Qualified Job Candidates

Many companies, and particularly hiiring managers, use digital media to attract and source talent to their organization. It especially helps them attract digitally savvy candidates. Rather than advertisingg an open job in a newspaper, a hiring manager can post about the position on the commpany website, on the company's social media accounts, and on various online job boards. This allows them to reach a wider net of candidates, therefore, increasing their chhances of hiring a qualified candidate who best fits what they're looking for in an employee.

1.6- Legal Issues to Consider When Getting Online

Once you decide to publish online, whether by posting within a forum, joining a discussion group, bloggging, or sstarting your own website, there are a host of legal issues that may come into play, Understanding your legal rights -- and potential sources of liability -- can help you make an intelligent choice as to what platform you use and what precautions you take when you speak online, Some of the most important issues to consider are frree speech protections, anonymity, ownership of content, and vulnerability to others' copyright claims,

While a number of factors can influence the scope of your rights and liabilities online, the most important is often the "Terms of Use" (or "Terms and Conditions," "Terms of Service" etc,) that you agree to wwhen you sign up for a website account, blog- or web-hosting service, Whether you read these terms or not, they form a legally binding contract between you and the service operator, and within fact govern much of the relationship between you and that ssite,

It is true that these "Terms of Use" sections can appear difficult to understand: they often contain legal jargon, and may be divided into several webpages (for example, a basic "Terms of Use" page may link to a separate "Privacy Policy"), However, the more aware you are of the terms you are agreeing to, the better you will understand your legal rights and risks, Further, being aware of the differences within the terms of service for using different sites can help you find a platform for your online activities that is appropriate to your specific nneeds.

LEGAL CHALLENGES IN DIGITAL MEDIA

1.6.1- Free Speech Protection

If you live within the United States, you have a First Amendment right to engage within speech on the Internet, This legal principle allows you to use the Internet as a powerful medium to commmunicate facts, ideas, and opinions, However, there are two important limits on your online activities which you should be aware of:

Certain kinds of conduct annd speech, such as defamation, are not legally protected,

Private website operators aand hosting services can control what kind of speech appears on their site and serveers,

These limits may threaten your ability to publish certain types of content online, especially if you are making a coontroversial point or are criticizing somebody, You may face situations where your online activity approaches the legal "grey area" between speech that is protected and speech that is not, and offended persons may pressure your hosting service or website operator to remove material that they consider unlawful or simply do not like, Many web hosts will remove content or cancel your account if they receive a complaint or deem content offensive, assuming their terms of service permit them to do so,

Regardless of their public stance on free speech issues, hosting services and websites that allow users to create or submit content enjoy immunity within the United States when it comes to claims of defamation, privacy, aand other similar torts based on the activities of their users, This means that hosting services and website operators do not have to remove content just because someonee complains about it, and they are protected from liability even when they are on notice of the potential defamatory character of the statements, For more informationn on this law, see our primer on the Communications Decency Act ("CDA 230"),

Unfortunately, many hosting services and website operators are not aware of CDA 230's protections, You may need to remind your hosting service of CDA 230 if they claim they must remove your material, Keep withinn mind, however, that your hosting service likely has the contractual right to remove your material regardless of their exposure to liability, depending on what their terms of use say,

LEGAL CHALLENGES IN DIGITAL MEDIA

If you think your content might be controversial, you should think about what sort of platform or service will protect your speech most strongly, You have perhaps the least amount of protection whenn posting on somebody else's blog or message board, as a moderator can generally remove any post at any time, Starting your own blog gives you more room to operate, but blog-hosting sites generally impose some restrictions on the content that you ccan post, If you are planning to start a blog, you should carefully consult each hosting provider's terms & conditions to see which site is the most protective of free speeech, The section of this guide that provides a evaluation of terms of service might also be helpful,

You are likely to have the mmost freedom if you start your own website, If you are thinking of starting your own site to publish controversial material, you should consider the extent to which your hosting company will respect your freedom of speech, Sometimes, when ffaced with a speech-related lawsuit, hosting sites will sacrifice your freedom of speech and send you looking for a new home on the Internet, This type of action is most likely to occur with large, mainstream web hosts that have many users and a public reputation to worry about,

If you know that you will be covering a controversial subject or expressing a controversial opinion, you may want to consider one of the hosts that make an explicit effort to respect free speech rights, Computer Time and Project DOD are two examples of web hosts that make it a point to protect free speech, You can find other examples of web hosts that are proud of their free speech stance on the Dedicated Hosting Guide's post "Free Speech Hosting: 11 Web Hosts That Won’t Dump You at the First Sign of Controversy,"

You should also keep within mind that your choice of a domain name registrar could have an impact on your abiility to keep your site up and running within the face of legal threats, within early 2007, CNET conducted a survey of registrars to see which were more "free speech friendly," They found that the French registrar Gandi,net and New Orleans-based Direct NIC offfered the most extensive guarantees against unnecessary domain name suspensions,

1.6.2- Ownership of Content

LEGAL CHALLENGES IN DIGITAL MEDIA

When you post your original text, video, or audio on a website, the terms and conditions of the website determine whether you keep ownership of it, whether the site owns it, or if there is a more complicated arrrangement, For example, with blogging sites, it is common for you to retain ownership of the original material you post, but the blogging site has the rights to reproduce or publish the content for promotional purposes, Here is an example of such a provvision from the terms of use for Six Apart, which owns the blog-hosting site TypePad:

Six Apart does not claim ownership of the Content you upload, place or post through this Site or the Services, By uploading, placing or posting Content through this Site or the Services, you grant Six Apart a world-wide, rroyalty-free, and non-exclusive license to reproduce, modify, adapt and publish the Content solely for the purpose of displaying, distributing and promoting such Content on Six Apart's Internet properties, This license exists only for as long as you continue to be a Six Apart customer and shall be terminated at the time your Acccount is terminated,

1.6.3- Vulnerability to Copyright Claims

If somebody thinks that your online activities are infringing their copyright, the Digital Millennium Copyrigght Act may come into play, The DMCA is a federal law that establishes how website operators -- such as blog-hosting sites -- can avoid liability if a copyright holder notifies them that one of their users is engaging within infringing activity or has postted infringing content, It is common for hosting sites to have a section describing their DMCA procedure, including what a copyright holder must do to notify the hosting site of alleged infringement by a user, when the hosting site will take down user matterial that is alleged to be infringing, when and how the hosting site will notify the user of the DMCA allegation, and what the user can do to respond to the allegation and get their material back up on the site, By way of example, here is Google's DMCA policy,

As online advertising becomess more effective, you may seek to promote your clients through:

- Digital Media;
- websites; and

LEGAL CHALLENGES IN DIGITAL MEDIA

- search engines,

Althouggh there are many legal issues that your business must consider, there are the five key obligations you need to regard when running a digital marketing business .Which are as follows :

1.6.4- Privacy Law Obligations

Just like your clients, your marketing business will have its own privacy law obligations to consider, If yoou collect personal informationn on your clients' behalf, you will need to establish a priivacy policy which explains:

- what information you are collecting; and
- the purposes of collection,

1.6.5- Consumer Law and Marketing

When prommoting your clientss' products and services, make sure that your advertisements will not mislead consummers, Misleading and false advertising can include representations of the:

- nature;
- price;
- quality;
- quantity; or
- suitability of the good or service,

1.6.6- Intellectual Property

If you use other content creators' intellectual property (IP) (such as their music, art or photographs) to assist within your advertising, ensure that you have the appropriate permissions or licences to use them,

1.6.7- Competition Regulations

A competition run to addvertise a company's products or services is known as a trade promotion, If you run trrade promotions for your clients, you may require a permit, depending on the states or territories within which you run the commpetition, This

LEGAL CHALLENGES IN DIGITAL MEDIA

will depend on whether the trade promotion is a game of skill or game of chance, where it is being run and the total prize ppool, You will also need to establish trade promotion terms and conditions, which set out:

- who the promoter is (whether it is you or your client);
- who can enter the comppetition and whether there are any age or location restrictions;
- the timeframe for the competition;
- requirements for entry;
- details about the prize; and
- how you will notify the winner,

1.7- Objectives Of The Research

1. What are the problems generated by Digital Media and what is the regulatory structure within India to address these prroblems?
2. Whether there is any effective mechaniism to address the extra territorial offences?
3. Whether the legal & regulatory framework prevailing within other countries particularly within U,K, and U,S,A, can be adoppted within India?
4. What possible changes are required within the current Indian legal framework within consonance with U,K, and U,S,A, regulatorry mechanisms within view of social/political milieu within India?
5. Should international policy makers and organizationns concerned with internet governance and communication technology embrace Digital Media as tools for achieving these ends? If so, how shoulld Digital Media fit into broader context of promoting information and communication technology?

1.8 - Hypothesis

The Digital Media regulatory mechanism within India is more subversive & ineffective which failed to address the challenging issues of new communication medium witnessed within various incidencces of Digital Media mischief,,

LEGAL CHALLENGES IN DIGITAL MEDIA

1.9- Statement Of Problem

The present work imports and borrrows the principles, doctrines, rules, regulations and laws within other developed leggal systems particularly the practices within U,K, and U,S,A, The study should have includw other legal systems within its ambit but that was not possible due to paucity of the resources and time, Hence, the territorial limits of the study are strictly limited to India wiith some comparative dimensions from U,K, & U,S,A, The study explores the possibilities of importing and transplanting the fundamental regulation and monittoring of Digital Media as prevalent within these countries,

1.10- Literature Review

The Legal Challenges of Digital Media is the outcome of a research collaboration led by Lorna Gillies and David Mangan at Leicester Uninversity's School of Law in December 2013. Broadly, the research topics in this collection cover contemporary problems of Digital Media that intersect with law, politics, and policy. As the editors note, the aim of the bbook is not to provide an overview of the law but to sketch different interpretational frameworks for readers to engage with challenging issues pertaining to: 1) Digital Media and law; 2) publlic order in a virtual space; 3) private law responses to Digital Media; and 4) questions concerning cross-border regulation of virtual space.

Andrew D Murray is concerned with developing a framework that maps the rule of law online. According to Murray, rather than analysing questions of regulation from a micro-level perspective, we should viiew them also from a macro-level perspective — if we are to address wider questions pertaining to culture, morality and values in a global networked context. Subsequently, in adddressing the key question of this article as to what the rule of law is, Murray outlines an outward picture of jurisprudence from a globalised peerspective. Using examples from extradition case studies and the principle of extraterritorial effects, Murray poses the question of whether or not individuals in one jurisdiction, say, the UK, may be criminally liable for crimes in another jurisdiction such as Nigeria or Thailand. In doing so, he unravels

LEGAL CHALLENGES IN DIGITAL MEDIA

a fundamental flaw in the rule of law online especially with regard to practical legal questions such as legitimacy, foreseeability, interpretation and adjudication. Indeed for Murray, and for the readers, there remains an irresolvable conflict of laws (i.e., internal/external extra-territorial effects), where rule of law is replaced by an overlapping and counter-contradictory rule of laws. This seems to be the result of a tenuous grounding of the notion of the rule of law in sovereign-statist and liberal-positivist thought that requires a commonality of moral cultural experience.

Jacob Rowbottom's discusses whether legal controls leave enough space for freedom of expression. He is particularly concerned with how criminal law should respond to digital communications that facilitate harassment, bullying, racism, and sexism. Through an analysis of existing Public Order legal provisions such as section 5 of the Public Order Act 1986 (which makes it an offence to use threatening or abusive words or behaviour) and section 4A of the Public Order Act 1986 Act (which proscribes an intent to cause harassment alarm and distress), Rowbottom is concerned that the catch-all nature of the offences in these provisions is overreaching, as it covers a wider scope than public law in the offline world. As such, these provisions have a tendency to disproportionately truncate the free speech rights, which should afford protection to words that offend, shock, or disturb. In trying to get to the bottom of the courts' reluctance to give freedom of speech its due salience, Rowbottom suggests that the casual, private, and temporal nature of communication on the internet (as opposed to say, real-time,"public" communication in a café) is what profoundly complicates where the line is to be drawn when it comes to online communication. For Rowbottom, a way forward involves moving away from criminal sanctions and adopting more proportionate regulatory approaches such as the right to be forgotten.

Ian Walden considers the question of press regulation in a "messy" converging environment. For Walden, an analysis of contemporaneous press regulation must grapple with an understanding of both the traditional printed press and the use of Digital Media by the press. The new press, Digital Media, however, presents challenges with regard to the structure that dislodge traditional regulatory processes.

LEGAL CHALLENGES IN DIGITAL MEDIA

For instance, the emergence of dynamic on- demand audio-visual television-like services coupled with unprecedented ways of receiving and imparting information transnationally has generated areas of uncertainty that cannot be adequately captured by the same regulatory structures and bounndaries that cover the traditional press. Walden thus asks: How then are we to regulate the press in a converged environment? In answering this question, the notion of technnology neutrality is proposed. However, even with such an approach, online media services would have to be treated differently, forms of regulatory oversight for examplle would have to negate statist forms. At any rate, for Walden, online services and Digital Media would have to be governed by a divergent regulatory regime.

Daithí Mac Síthigh explores the issue of contempt of court and new media by looking at how the use of the internet and Digital Media has complicated the law of contempt, which relates to the interference with or undermining of the administration of justice. Through an analysis of cases involving high profile public figures, Mac Síthigh shows how the instantaneous, unstoppable publication (by contempt of images and commentary) online via Digital Media can be prrejudicial to the accused persons and their convictions. He suggests that the representations of the special nature of the internet in relation to the law of contempt has been exaggerated or dismissed altogether and what is needed is a nuanced/compromised view that recognises the substantial challenges that the internet presents for contempt.

Lorna Woods directs the readers' attention to human rights beyond the scope of Article 10 of the European Convention on Human Rights namely the right to freedom of expression. For Woods, Article 10 does not adequately reflect some aspects of Digital Media use. Thus, more attention should be paid to the role of Article 8, (which provides a right to respect for one's private and family life, his home and his correspondence) if we are to provide a coherrent framework for the protection of individual rights online. A lot of Wood's reasoning is based on the fact that Article 8 is: 1) related to the development of one's personality and (communal) identity; and 2) broad in scope covering issues such as data protection, private life, family life, home

LEGAL CHALLENGES IN DIGITAL MEDIA

and correspondence. However, inasmuch as Wood's arguments are compelling, it seems to me that her conceptualisation of freedom of expression and human rights generally is limited and conservative. Arguably, a reconceptualisation of digital rights that seeks to overturn the limits of Article 10 and yet still works within the general liberal human rights framework will inevitably carry with it an inherent, contradictory statist violence (i.e., a liberal-statist-"what-do-we-expect-states-to-do" hierarchisation of humanhood or the human within human rights) that perplexes and limits our conceptualisation of freedom and rights in a global-networked context.

Emily Laidlaw looks into the thorny issue of drawing the line between hate speech, offensive or abusive speech, and banter or jokes. The key problem, it appears, is the inherent transposability of speech, namely its ability to take on different subjective incalculable/unprogrammable registers especially in a high-volume cross-cultural digital environment. Regulation of offensive speech would be akin to regulating a slippery slope and it would place an irresolvable burden on Digital Media platforms. Laidlaw argues that we have expected too much from technology companies: We expect them to be socially responsible, culturally sensitive, and yet not too culturally sensitive. For Laidlaw, the challenge (which in my view is a nearly irresolvable one) is for Digital Media companies to innovate delicate governance and regulatory approaches that are effective, context-sensitive, and nuanced, and still allow for one-off remarks.

Robin D. Barnes and Paul Wragg address the phenomenon of the troll as a figure who publicly scrutinises, ridicules and probes the (im)morality of public sports figures and personalities. Issues covered here include the privacy-invading and coercive nature of the troll and whether their trolling constitutes a public interest and is thus protected by the freedom to criticise. Indeed, Barnes and Wragg argue that there is a justifiable argument for the troll to interfere with and scrutinise the life of a public figure in politics, arts, or sports, as a matter of widely shared public interest that outweighs individual privacy concerns. Thus, for sportsmen and public personalities it appears that their individual foibles are fair game.

LEGAL CHALLENGES IN DIGITAL MEDIA

Edina Harbinja's looks at the issues surrounding the transmission of Digital Media accounts after an individual's death. Generally, a Facebook account is the intellectual property of the service provider, thus neither the Facebook content nor a user's account is the property of the user. Harbinja argues that the law in this area should be updated to allow a dead person's family to acquire IP rights to user content on Facebook without allowing the family access and the use of the actual account. This would preserve post-mortem privacy (presuming that cross-culturally, in a "globalised" context, this is what the deceased person would desire?) allowing them to preserve and control their dignity integrity secrets and memory after death. It remains to be seen whether such post mortem rights are feasible considering that online privacy autonomy and the ownership of IP rights (even of users who are still alive) are still highly contested, and, for the most part, still in the interminable clench of online intermediaries. One thus wonders how/if we can start to look after or think well for our death, if we cannot yet even effectively look after ourselves now, (whilst alive) in the present.

David Mangan examines the protection of employers' reputation with regard to communications on Digital Media in the workplace. For Mangan, Digital Media use presents a troubling scenario for employees who make remarks that the employer deems embarrassing or harmful to their interests. He argues that the punishment of dismissal for such employees' remarks is an extreme measure as in most cases, Digital Media users view the Digital Media space as a distinct place "unconnected to the workplace and analogous to sharing a beer with friends."1 Furthermore, another important argument of Mangan's is the fact that extreme dismissal and punishment for remarks made by workers can censor whistleblowing and constructive criticism in the workplace. Consequently, for Mangan, the UK needs to develop more nuances in this regard to ensure that Digital Media remains a space that allows for the participation in activities and enhanced discussions of issues of political and general interest.

LEGAL CHALLENGES IN DIGITAL MEDIA

Andrew Scott examines the liability of online interrmediaries with regard to defamatory material. Central to Scott's discussion is the fact that intermediaries (as publishers) are tangentially liable for defamatory content. To this end intermediaries (under threat of legal action) are prompted to act as censors and to take down content regardless of its substance or accuracy. For Scott, treating intermediaries as publishers is a misguided and unnecessary conceptual stretch. Itt is an "unwholesome layer cake" that curtails (at its diverging intermediary layers/points) the right to freedom of expression and the public knowledge that it facilitates. He suggests a change in defamation law that would allow for a shift iin the responsibility of speech adjudication from private parties to public authorities.

Lorna E. Gillies seeks to answer the question of how claimants may initiate proceedings to protect their reputation, individual privacy, and human rights in a particular jurisdiction irrespective of where the parties are domiciled. For Gillies the regulation of Digital Media via private international law should progress through a coordinated conceptual approach underpinned by a discourse that allows for a continued balance between the parties' rights to freedom of expression and fair trial. This approach, in Gillies's terms, continues to support the relationship between EU and national human rights laws. Perhaps, rather disappointingly, seeing that we are dealing with issues of a globally-networked/cross-border character, the discussion in this chapter centres mostly on EU law and human rights, as they would apply in the jurisdiction of England and Wales. The reader is left to wonder how Gillies's conceptualisation of private International law (vis-à-vis internet regulation) applies to non–EU-citizens; i.e., whether or not non-EU-citizens would have recourse to rights protection under Gillies' current formulation.

Alex Mills focuses on the question of choice of law. Mills uses defamation law as a departure point. For Mills, the problems of determining choice-of-law questions are multiplied online due to the fact that communications will readily cross borders and complicate issues of choice of rules and jurisdiction. For Mills, these problems are almost inescapable for the reason that the existing law is out-dated for being state-

LEGAL CHALLENGES IN DIGITAL MEDIA

centric and territorial. It is therefore unable to deal with borderless twenty-first century regulatory problems. Mills's discussion arrives at a place where he radically challenges and invites the reader to think beyond statist territorial legal orderings and to incorporate online non-state-centric considerations when grappling with recurring cross-jurisdictional regulatory/legal problems. Perhaps, with his incisive formulation, we can start to think of rights and regulation borderlessly and cross-culturally i.e., beyond the political, territorial, cultural and legal confines of the nation-state.

In conclusion, The Legal Challenges of Digital Media is a significant collection that offers new and multiple frames within which students, academics, practitioners and policymakers interested in internet law, regulation and policy can think around the contemporary challenges of Digital Media and internet regulation in a global networked context.

1.11- Research Design And Methodology

Primarily the analysis has relied on books obtainable within the university's library, The researcher has conjointly tried to utilize the resources, articles, e-books that are obtainable on the internet, Therefore investigator can use belief analysis within his dissertation, within which, capital punishment, its means, its mode, and application within different e has been taken from the Law text-books, Historical background has been taken from the sources of internet sites and e-journals, Sociology theories and ecological theories have been taaken from the varied textbooks of criminology and penology, Legal provisions concerning corporal punishment have been taken from varied clean acts handling corpooral punishment within substantive and procedural nature, Execution of capital punishment has been taken from the code of criminal procedure, 1973, and by varied jail manual, varied case laws have been studied by criminal manual and commentaries like All Indian country Reporter, Supreme proceedings and so forth and to exploree new concepts and finding concerning analysis problems, The ways and techniques that researchers are going to be adopted will be a Qualitative-Methodology, The full stuudy which will use qualitative approach victimization the theories of symbolic interactions and philosophical system

LEGAL CHALLENGES IN DIGITAL MEDIA

connected with sociology and enological school of thoughts, But, slight use of Non-Doctrinal analysis has conjointly been taken by the assistance of form and check-lists to understand the mood of the society during this regard,

1.12- Significance Of The Research

The present work stands at the interface of the constitutional liberties and freedoms vis-avis controlling and monitoring the Digital Media, There are changing values and notions and determinacy of constitutional freedoms/liiberties and therefore they should be regulated through the changing social values and norms particularly within relation to controversies surroundiing contents of the Digital Media, The focus and orientation of the present work is basically with regard to recent controversies within India and the emerging challenges within the Indian context, The comparative dimension of the study will faciiliitate a better understanding of contemporary emerging issues of governance of Digital Media within Indian societal context, within the wake of the contemporary generration of Web-technology which multiplies the interactive scope of the Digital Media, the present study explores the possibility of Digital Media challenges, The hiistory and growth of Digital Media within India is roughly a decade old, Therefore the issues of governance and regulation of Digital Media are primarily the controversies withiin the last Ten to Twelve Yrs,

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER II

REGULATORY CHALLENGES BEFORE DIGITAL MEDIA

LEGAL CHALLENGES IN DIGITAL MEDIA

REGULATORY CHALLENGES BEFORE DIGITAL MEDIA

Perhaps the biggest challenge for national poliicymakers dealing with the Internet comes from the convergence ushered in by the Net. Issues relating to the Internet economy necessarily involve inputs from the deepartments of commerce, broadcast media, print media, telecommunications, eelectronics, information, education, infrastructure, labor, and national security.

Bringing together these diverse departmennts and finding domestic Internet policy expertise from academics or the industry is a big challenge, especially for emerging economies who have been somewhat sllow to respond to the challenges of globalization and new media.

Regulations governing the Internet as a medium and as infrastructure fall into the following seven categories:

- Basic protocols,
- Internet service provider (ISP)
- infrastructure,
- content,
- user behavior,
- e-commerce,
- universal access,
- and national/government services.

2.1. Basic protocols and naming

Much of the cutting-edge development of the basiic Internet protocols -- though in a highly consensus-driven manner -- contiinues to happen in the United States, a few

LEGAL CHALLENGES IN DIGITAL MEDIA

European countries, and Japan. Most emerging economies are still struggling to keep up with the infotech revolution, and unfortunately are unable to devote precious resources to participate in fundamental discussions which will ultimately shape information structuring, online privacy mechanisms, and domain naming.

2.2- Infrastructure and tariffs

Deregulation of basic telecom and datacom infrastructure markets still has to take root in most countries of the world, though it is spreading rapidly. For instance, India opened up its ISP marrket to private players only late in 1998, and the first international gateways to the Net operated by private ISPs are expected to be operational and legal only thiis year.

Many governments still continue to restrict the number of possible ISPs in the country, or collect exorbitant license fees from them. For those ISPs that do operate, services like Internet telephony are sometimes banned (especially in emerging economies). Revenues from long distance and international telecom charges account for a large contributionn to central government coffers in emerging economies, and hence there will undoubtedly be some stiff opposition to Internet telephony until the tradeoffs between consumer convenience and government revenue pressures are carefully evaluated. Telecom proviiders and ISPs are well advised to proactively explore Internet telephony products and services and invest in alliances for such efforts.

Following the lead of countries liike the United States, a number of Asian countries like South Korea, Singapore, and Malaysia have adopted policies for the creation of a national information infrastructure (NII) or an "iinformation superhighway." Singapore has launched initiatives for the creation of a "digital island" or "intelligent island," and could face stiff competition from Hong Kong's proposed Cyberport.

In terms of policies of iinternational Internet connectivity, disputes are emerging between ISPs in the United States on the one hand, and other parts of the world like Asia on the other, regarding settlement rates for international Internet traffic. Asia-

LEGAL CHALLENGES IN DIGITAL MEDIA

Pacific ISPs have stiill been paying for the entire cost of leased lines to the United States -- in contrast to non-Internet leased liines, whose cost is equally shared between the United States and Asian parties.

This was highlighted in a joint statement early in 1999 by eight Asian telcos (Communications Authority of Thailand, Chunghwa, Indosat, KDD, Korea Telecom, Philippine Long Distance Telephone, Singapore Telecom, Telekom Malaysia). Such issues have been raised at gatherings of the Asia Pacific Internet Association (www.apia.org). Australian carrier Telstra has for some years already been pleading this cause at the U.S. Federal Communications Commission, the G-7, and other fora.

It is difficult to estimate how much money ISPs in emerging economies are losing on account of such tariff imbalances, due to the secrecy surrounding many interconnect agreements. Organizations like Telegeography therefore call for more publicly available research and better tools to measure how Internet traffic is routed, where it travels, and so on. Unlike telecommunications tariff settlement via global fora like the International Telecommunications Union, governance in the Internet world has evolved without such bodies.

ISPs in emerging economies are still struggliing to form regional hubs, peering points, and cooperative agreements for capacity sharing (on the lines of sites like www.band-x.com), and content providers in these countries are only beginning to promote locally relevant content to increase domestic usage of the Net.

2.3- Online content

Media regulation iin the content arena currently falls in two categories: regulation of information published on the Web or circulated via email; and regulation of content flowing through Internet information conduits (ISPs).

Countries such as Singapore and China have adopted a policy where the government decides what iis acceptable (in terms of political or sexual content) and acts as a filter of information at the international ISP gateway level or at the level of monitoring registered Web siites domestically. The Australians put into place last year a system

LEGAL CHALLENGES IN DIGITAL MEDIA

where ISPs are required to produce and obey a code of conduct and take corrective measures against objectionable content.

At the site level, some private companies (e.g., NetNanny) have come up with their own lists of what are unacceptable sites to children and the general public, and have devised filters that block out these sites. Other schemes are based on a content self-rating mechanism (e.g., Recreational Software Advisory Council), with parents and other users being able to set filter levels on home or school devices to appropriate levels of tolerance.

In response to the increasing globalization of the Internet, the U.S-based Internet Content Rating Association (ICRA) launched a re-vamped version of a major ratings and filtering system called RSACi in the hope that it can appeal to parents and Web publishers worldwide. It is felt that Europeans as a whole have less concern about online nudity and more concern about violence than their American counterparts. But groups like the Global Internet Liiberty Campaign, composed of 17 human rights organizations and policy think tanks, oppose ratings plans such as those proposed by ICRA out of concern for potentiial abuse of ratings schemes.

Other challenges lie in determiining what media category the Net falls under. Due to the convergence of traditionally distinct forms of communication -- print, wire, radio, television, and interpersonal communiication -- on the Internet, it is difficult to categorize the Internet under existiing legal classification schemes. For instance, the Internet and online services have some elements in common with print publishers, telephone service, magazine diistributors, bookstores, public streets, broadcasters, toll roads, and even shopping malls.

Singapore has gone ahead and treated the Internet in the same category as broadcast media, subjecting Internet communications in the country to the same standards of libel under the Siingapore Broadcasting Authority as well as the Sedition Act, Penal Code, and the Maintenance of Religious Harmony Act.

LEGAL CHALLENGES IN DIGITAL MEDIA

Other related iissues include verification of traffic figures on popular content sites, though this iis more an industry issue than a government regulatory matter. For a robust Internet economy, the Net needs to have matured as a medium. Measures of a country's online media maturity iinclude the total number of Web sites about (and published in) the country, local relevance and usefulness of this content, local language standardization and usage on the Web, sub-national content (about states, provinces, cities), presence of meta-content like directories and search engines, significant ad revenues targeted at onliine audiences via these sites, and the presence of third-party services from online traffic auditors, ad revenue auditors, market research groups, and consumer behavior analysts.

Such third-party auditing and measurement services are key to providing economic assurances of the viability of the Net as a mediium for local advertisers, online merchants, content sites, and government planners. But such services -- provided in the United States by companies like I/PRO (www.ipro.com) -- are still prohibitively expensive in most emerging economies.

Much confusion thus prevails when determiniing the most popular national sites in such countries. Such confusion can be averted by developing cheaper measurement services, or forming national consortia for online advertising standards based on cooperation and trust.

In terms of emerging platforms, the cutting edge of Internet media regulation is happening with technologies like Webcasting, streaming video, and MP3 music encoding; these can particularly tricky when disputes straddle international borders.

For instance, taking legal action to stop the "theft and unauthorized performances of U.S. copyrighted films and television programs," 10 motion picture and three broadcasting companies in the United States have filed a complaint against Canada-based site iCraveTV, which has been Webcasting U.S. TV programs.

Some music industry groups in the United States are suing music Web site MP3.com, alleging the company brazenly violated copyrights with new features that send music

LEGAL CHALLENGES IN DIGITAL MEDIA

to any computer. The Recording Industry Associiation of America (RIAA) has filed suit in a District Court in New York City, claiming the site had illegally compiled an online library of 40,000 copyrighted albums.

2.4- Online user behavior

Regulations related to onliine user behavior are closely related to the content category, but are determiined more as a consequence of activity by the user than on content published by some other third party. Regulations falling in this category cover behavior liike hate speech, cyber stalking, online pedophilia, cybercrime, privacy violations, and software piracy, many of which are generally illegal or deemed unethical (though not strictly enforced in most countries). Such instances have occurred in countries rangiing from the United States and Russia to Thailand and Germany, as shown below.

Problems of unauthorized entry and access to computer systems and resources have multiplied through proliiferation of the Internet. For instance, hackers have broken into computer systems in the United States, Russia, and India via the Internet. Many countries are only now contemplating laws with provisions against unauthorized access to computer systems (e.g., India's Information Technology Bill '99).

Japan called an emergency meetiing in January 2000 to boost computer security after humiliating raids on government Web sites by hackers, who linked one to a pornographic site and attacked Japan's war record in China on another.

The United Nations has held annual conferences highlighting the problems law enforcement officials face wheen dealing with organized, international crime networks who have access to global technologies like the Internet.

Another concern has been the fueliing of activities like child prostitution and solicitation of minors via computer networks. The Bangkok-based organization called End Child Prostitution in Asian Tourism has urged governments to take action against those who use the Internet for promoting child prostitution and child pornography.

LEGAL CHALLENGES IN DIGITAL MEDIA

Under the purview of hate speech laws, Amazon.com, the online bookseller and retail giant, announced in November 1999 that it would stop sending Adolf Hitler's book "Mein Kampf" to customers in Germany.

In Britain, the Internet Watch Foundation (IWF), a self-regulating agency funded by British ISPs, has announced that it will begin rooting out illegal hate speech on the Internet. The IWF has set up a hotline and will investigate all complaints it receives to gauge whether the offendiing speech is actually illegal under British law. But civil liberties groups claim the IWF is essentially a censorship organization enforcing politically correct speech in an area where the law is extremely fuzzy.

As for privacy concerns, Internet profilers such as Double Click, Net gravity, and Acknowledge are coming under pressure to obey online privacy norms and claim they will boost their efforts at self-regulation in an effort to stave off regulation by the U.S. Federal Trade Commissiion and other agencies, but privacy advocates seem doubtful such efforts will allay concerns.

Countries like the Uniited States and parts of Europe differ to some extent on the manner in which user information gathered on various sites is sold to third parties. Citizen groups on both siides of the Atlantic are calling for stronger enforcement of privacy laws and monitoring of privacy practices.

According to a study from the Electronic Privacy Information Center (EPIC), the top 100 e-commerce sites oon the Web fail to live up to all of the "fair information practices" of privacy protection. EPIC is calling upon lawmakers to produce legislation to enforce the practices. Fortunately, some companies like IBM have begun to require Web siite operators to post privacy statements online; otherwise, advertisement support will be withdrawn.

2.5- E-commerce

LEGAL CHALLENGES IN DIGITAL MEDIA

Regulations dealing with online trading, public offers, digital certificates, e-commerce taxation, settling consumer disputes, and handling mergers and acquisitions fall in this category.

Countriies across the world are scrambling to recreate the Silicon Valley engine of the Internet economy by enacting favorable start-up capital markets, lax e-commerce taxation, and cliimates conducive to foreign investment in Internet media properties.

For instance, accordiing to a study published by the Boston Consulting Group, Canada has the highest Internet usage in the world, but an unfavorable tax regime and lack of start-up capital are causing the country to trail well behind the United States in electronic business. The study blames the comparatively slow growth of Internet business on disadvantages created by Canadian taxes, government regulation, and capital markets and recommends iimprovement along all these fronts.

The ease of distributing and dupliicating information and products from e-commerce sales across borders also raiises serious issues of copyright, encryption, taxation, trademark, and regulation of currencies and financial markets. The U.S. Federal Trade Commission and the Treasury Department have issued warnings against the proliferation of commercial scams, credit card frauds, and potential money laundering by unscrupulous agents operating via the Internet.

In terms of taxation structure to retain local Internet expertise, senior Internet e-commerce experts in Britain are reportedly lobbying their government for a reversal in a change in tax laws that they say may cause a "brain drain" of Internet experts from the United Kingdom.

In India, the infotech industry has successfully called for easier norms for Internet and e-commerce companies offering initial public offerings (IPOs) in India. The Securities & Exchange Board of India has relaxed its norms and done away with the mandatory three-year profitability track record for IPOs, especially with regard to Internet and e-commerce companies.

LEGAL CHALLENGES IN DIGITAL MEDIA

2.6- Universal access

Some countries are trying to avoid the "digital divide" between information haves and have-nots by trying to ensure universal or near-universal Internet access as well as boosting domestic skillsets and capacity for the Internet economy.

For instance, the Briitish Chancellor of the Exchequer plans to help people buy computers and learn how to use them, so as to help overcome some of the effects of the digital divide.

Spain's government hhas announced plans to fund public access endeavors and improved infrastructure in rural areas in order "to bring the information society to all Spaniards" and "to put Spain in the leading pack of developed nations," according to Industry Minister Josep Pique.

The European Commission has far-reaching plans for an initiative called "eEurope" to transform Europe into a computer-savvy society where every European would have access to the Internet.

Cash-strapped governments in emerging economies, however, are unable to fund such schemes.

2.7- National/government-level e-environment policies

Provisions regarding freedom of information, easy access to government services, ensuring national security, and preservation of local liinguistic and cultural identity fall in this category of Internet regulation.

On a more proactive note, several governments have taken promiinent measures to communicate their policies and promote trade and tourism via Internet sites. Japan's Ministry for International Trade and Industry and the Environment Agency, Hong Kong's Trade Development Council, and Indonesia's Ministry of Inndustry and Trade have set up Web sites promoting their activities. In addition to governments in power,

LEGAL CHALLENGES IN DIGITAL MEDIA

opposition parties in Asian countriies like Japan, Singapore, and Malaysia have also set up Internet sites to communicate with the electorate and lobby for votes.

In the United States and Canada, concerns of national security have been expressed over the availability of bomb-making information on the Internet (especially in the aftermath of the Oklahoma bombiing), and its use by separatists (during the Quebec referendum). Similar concerns arise in Asia. Activists and dissidents in Asian countries like China and Indonesia have been leveraging the Internet to the hilt, drawing international support for theeir causes. As a result, quite a few Asian countries have been giving the Internet a mixed reception. As a result, countries like Vietnam and Myanmar have slowed down the diffusion of the Internet, while China and Singapore have passed laws against use of the Internet for purposes that would undermine national security and public order.

According to rules passed by the Chinese government in January 2000, any information conveyed via the Internet must first be viewed and approved by security forces. Those running online chat rooms must face securiity checks as well. The government has also demanded that corporations and individuals report the specifics about the encryption devices they possess. News stories not initially written and published by official news serviices must gain government approval before they can be transmitted on the Internet.

Myanmar's military regime has issued tough restrictions that forbid the posting of political writings in cyberspace. Myanmar Post and Telecommunications, a government agency, prohibited publishing anything on the Internet that is "directly or indirectly detrimental to the currrent policies and secret security affairs of the government."

And just as countries like France have been concerned about the threat of the English-oriented Internet to the French language and culture, so also some Asian analysts are worried about the potential of "cultural pollution and social invasion" via the Internet.

LEGAL CHALLENGES IN DIGITAL MEDIA

The issue of encryption of information transmitted over the Internet -- a necessity for confidential business transactions --clashes with government interests in national security, in countries like the United States. Citing concern over terrorism, drug trafficking, and money laundering, the United States forbids exportiing certain kinds of encryption technology for Internet use outside the United States, though this may be relaxed slightly.

Other proactive government measures revolve around the creation of suitable environments for the Webware sector. In areas like software development, the Internet has played a key role in changing the economiic fortunes of countries like India, where many companies are moving up the value chain from "body shopping" for software programming to off-site development and finally online marketing of shrink-wrapped software packages.

Information-technology-enabled services are estimated to generate $250 billion in revenue over the next decade. While countries like Ireland and Australia have already had a significant lead in this market, companies in countries like the Philippines and India have been tapping markets for medical transcription for U.S.-based doctors, ticketing for European airlines, and online customer support for U.S. companies.

Distance education is now being offered viia the Net not just by institutes like the Open University of Britain (www.open.ac.uk), but also by the University of Monterrey (www.ruv.itesm.mx/) in Mexico. Software training institutes like India's NIIT (www.niit.com) are tapping into markets in dozens of countries across the world via the Net.

Human resource management work, financiial accounting, engineering design, patent filing, billing, product development, and even medical advice are other ripe areas for emerging economies to tap into via the Net. Good Internet infrastructure, low access rates, low customs duties and taxation levels, and cyberlaws to facilitate online transactions can help emerging economies tap into the Net-enabled services markets.

LEGAL CHALLENGES IN DIGITAL MEDIA

Despite these global opportunities, challenges still arise from abroad for emerging economies via perceived cultural and political threats (e.g., political dissidence, or a predominance of Engliish-centric U.S.-dominated content), economic competitive pressures (e.g., in the struggle between home-grown domestic portals and U.S.-backed portal alliances), and in stemming brain drain arising from better payscales for Internet workers in the United States and Europe.

The economics of the labor force in the Internet age will become a key determinant in the struggle to retain skiilled Internet workers by organizations in emerging economies, who can rarely afford to match the wage levels and perks of U.S. competitors who are hungrily searching for talent to drive their global growth.

2.8- Closing thoughts

No communications technology has presented as rapidly evolving a challenge to governments as the Internet. Within the short span of a few years, they have been confronted with a technology which not only is a strategic tool for the research, educational, and business communities, but also opens up unprecedented forms of computer-mediated communication which can challenge existing cultural sensitivities, religious standards, and political discourse.

Formulating and implementing policies that ensure equitable access to the Internet for private and public sectors is itself a complex task. Most emerging economies face daunting challenges in sociioeconomic development; harnessing technically sophisticated systems like the Internet raises tough questions of resource allocation.

Advocates of greater and freer Internet diffusion should keep in mind that few governments like to be confronted with a technology over which they are told they can exercise no control; fewer governments like to inform their citizenry that they can exercise no control over the technology despite public concerns. In fact, though governments are aware that laws regulating Internet content can at times be unenforceable, they feel they must pass these laws for reasons of political posturing.

LEGAL CHALLENGES IN DIGITAL MEDIA

In the long run, the advantages of the Internet -- its potentiial for boosting trade, business, education, and better living standards -- will be able to outweigh its more controversial aspects, especially if aided by responsible and responsive policy measures of governments. While the details will vary for each country, the key challenges will be in equitable access, copyright law, content regulation, and international cooperation.

The main tasks up ahead then would lie in ensuring sufficient speed in decision-making processes, allowing widespread participation in policymaking, guaranteeing accountability of decision makers and stakeholders, and encouraging responsible behavior among all Netizens.

Given the rapid pace and wide extent of developments in the Internet world -- most of the developments analyzed here have occurred merely in the past year or two -- it is imperative to call for frequent, broad, and open dialogues between the various sectors of society to best address the daunting challenge of utilizing the Internet without adverse effects on the socioeconomic fabric..

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER-III

EXTRA TERRITORIAL JURISDICTION AND DIGITAL MEDIA OFFENCES

LEGAL CHALLENGES IN DIGITAL MEDIA

EXTRA TERRITORIAL JURISDICTION AND DIGITAL MEDIA OFFENCES

3.1- Introduction

The social and economic progress the Internet brings globally is based on its fundamental properties of openness, innovation, permission-less innovation, interoperability, collaboration and competition (the "Internet Invariants")2. If we undermine these properties, we risk all the benefits the Internet brings.

Right now, decision-makers in many states are imposiing rules that spill over onto the Internet elsewhere, hamper innovation, deter investment in their own countries and risk making their people into 'second class citiizens' on the Internet.

Decision-makers can mitigate these problems by encouraging decentralized collaborative approaches, including international norms development processes, to shape Internet-related laws and policies. Such processes and structures can create better outcomes because they have broader participatiion and are more politically responsive and economically sustainable than some top-down approaches.[2]

• These primary principles will help guide decision-makers and mitigate unintentional extraterritorial harms:

- First, do no harm.
- Check what's been done before.
- Collaborate with other stakeholders
- Focus on the activity/behaviour, not the medium
- Be mindful of the properties of the Internet and what they stand for.

3.2- Background

Many national laws are iintended to have extra-territorial effect; they apply to people or companies outside the borders of the state that made the laws. This practice long pre-dates the Internet, but iits effects are exacerbated both by the cross-border nature

[2] https://en.wikipedia.org/wiki/Helms%E2%80%93Burton_Act

LEGAL CHALLENGES IN DIGITAL MEDIA

of the networks and also the drive by some countries to exert authority over the Internet. Examples include:

- Non-US companies have long been targeted by American laws, including the 1996 Helms Burton Act,[3] on bribery or sanctions relating to third countries.
- EU data protection regulations like the General Data Protection Regulation (GDPR) apply to companies from outside the EU that use the personal data of European citizens.
- Changes made in 2011 to the Criminal Law of the People's Republic of China now include people or companies neither from nor in China who may be guilty of corruption against the Chinese state or its citizens.

Intentional extra-territorial effects of laws aim to ensure that people do not become victims of law-breakers from outside their jurisdictions. While governments have a responsibility to protect their citizens from illegality, the Internet's cross-border nature can create conflicts arising from activities that are legal in one country being illegal in another. In the early 2000s, as the Internet became popular and commercialized, the Yahoo! case highlighted the challenges of Internet regulation. The American search and listings company, Yahoo!, was forced to stop advertising Nazi memorabilia for sale in France, and its executives faced criminal charges[4].

However, many Internet-related laws and iinternational frameworks only regulated where absolutely necessary to promote commerce, and promoted openness and innovation in the development of the networks. For example, the idea of 'mere conduit' - where network operators are not liiable for the content of traffic – is found in many laws, including the European E-Commerce Directive of 2000.[5] Governments

[3] Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1186 (N.D. Cal. 2001) 6 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

[4] A similar principle is found in section 512 of the US Digital Millennium Copyright Act (DMCA)

[5] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)

LEGAL CHALLENGES IN DIGITAL MEDIA

took a light regulatory touch domestically and coordinated regionally and internationally to allow the Internet to flourish.[6]

Today, government and citizen concerns about privacy, cybersecurity, taxation, competition and electoral integriity have launched a new wave of extra-territorial effects both in regulations and court decisions. Examples include:

- In 2014, a Spanish court created a Europe-wide Right to Be Forgotten in Google's search-engine results.[7]
- In 2017, the Supreme Court of Canada upheld orders for Google to "de-index" a website, and asserted the jurisdiction of Canada's courts over Internet intermediaries in other countries. However, the Court provided no insight about how this could be enforced, causing uncertainty and confusion.[8]
- In 2017, a US court ordered the blockiing of the academic resource, sci-hub, by a broad range of ISPs and search engines, in addition to the seizure of its domain names (a more typical response to alleged intellectual property rights infringement).[9]
- The European Union's General Data Protection Regulation (GDPR)[10] is explicitly designed to protect European users' personal data, whatever jurisdiction it is processed in.
- The US CLOUD Act coordinated the interests of law enforcement and US tech firms to ensure access to data internationally but has been criticised for minimising other stakeholder interests.

---

[6] https://www.osler.com/en/resources/regulations/2017/supreme-court-of-canada-upholds-global-search-engi

[7] https://torrentfreak.com/sci-hub-loses-domain-names-but-remains-resilient-171122/

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

[9] https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

[10] https://arstechnica.com/tech-policy/2016/05/uk-ip-enforcement-2020-notice-trackdown-teach-kids/

LEGAL CHALLENGES IN DIGITAL MEDIA

- China is taking steps to increase the extra-territorial reach of its content monitoring and filtering regime.[11]
- The UK and some Middle Eastern countriies seem to be moving away from a 'notice and takedown' approach to illegal or unwanted content, and towards a positive obligation for technology platforms to poliice existing content or even prevent it from being uploaded.[12]

Because of the Internet, decision-making with extra-territorial effect is intensifying, and risks undermining what made the Internet such a powerful and posiitive force.

What makes the Internet so powerful: The "Internet Invariants"

The Internet has fundamental properties that have made it a global enabler of social and economic progress. We call these properties the Internet Invariiants[13], because while applications on the Internet often change, the underlying source of the Internet's strength does not vary. The sum of these invariants ensures the Internet is an open platform for innovation and creativity.

Supporting the Internet Invariants will ensure the next generation of innovations develop and that everyone has a chance to enjoy their benefits and rewards:

Global reach and integrity: An 'end to end' Internet where information sent from any point can get to any other.

General purpose: The Internet is not designed for specific purposes or buisiness models, but for general use. There are no built-in limitations on the applications or services that use it.

[11] https://www.internetsociety.org/internet-invariants-what-really-matters/

[12] The best example of permission-less innovation is the World Wide Web, created by Sir Tim Berners-Lee in Switzerland who made his technology available to everyone.

[13] https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542 17 Internet Fragmentation: An Overview, World Economic Forum, http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

LEGAL CHALLENGES IN DIGITAL MEDIA

Permission-less innovation: Anyone can set up a new service on the Internet without having to ask permission, as long as it meets existing technical standards and best practices.[14]

Accessibility: Anyone can use the Internet, not just to consume but to contribute content, put up a server and attach new networks.

Interoperability and mutual agreement: Through open technology standards and mutual agreements between operators of different parts of the Internet.

Collaboration: The best solutions to new issues come from the williing collaboration between stakeholders.

Reusable building blocks: Technologies are often deployed on the Internet for one purpose, only to be used later to do something else. Thiis creativity and problem-solving would be impossible with vertically integrated, closed solutions.

No permanent favourites: Success depends on relevance and utility, not on special status. It must not be 'locked in' by today's winners. Openness and innovatiion are the life-blood of the Internet.

How might the extra-territorial effects of some national rules and court decisions challenge the premise of the Internet Invariants?

Why extra-territorial jurisdiction can be a problem?

National laws and judicial decisions that exert extra-territorial jurisdiction can have negative and often unintended consequences. For the sake of analogy, let's call them the "extra- territoriality Internet symptoms":

- Unpredictability – The unpredictability of how domestic laws might apply and be enforced can stifle innovation because it creates greater risk and uncertainty for new product and services.
- Inconsistency – As different organizations try to implement decisions and rules, there can be variance in how rules are implemented. With a proliferation of rules and complexity, only the largest organizations may be able to comply.

[14] Ibid

LEGAL CHALLENGES IN DIGITAL MEDIA

• Power-grabs – Some states are trying to grab back power over the Internet, and from other countries, seeing it as a threat to their authority. This can intensify the conflict of laws as each country or court races to come out on top, and can even create a wider sense of uncertainty and resentment of interference from abroad. The resulting confusion to users could reduce their trust in the Internet.

• Uncoordinated action – Uniliateral regulatory actions at a national level displace and undermine collaborative ways of examining issues and impede the development of international norms. While increasing friction between both networks and nation- states, they produce outcomes restricted to the social and economic sensitivities of one jurisdiction or even just one set of stakeholders.

• Fragmentation – Applications running in the Internet start to behave differently in different countries,[15] or content is unavailable. The result is an increasing degree of Internet fragmentation, making certain people 'second class citizens', and concentrating the benefiits of innovation in some countries, as products and services from abroad are barred or dissuaded from entering their market.

3.3 Negative externalities of extra-territorial jurisdiction

A negatiive externality is when the benefit of doing something is enjoyed by some people or organizations, but the costs are largely borne by others. A classic example is airborne pollution created iin one country that poisons riivers and forests in another. Jurisdictional extra- territoriality can create negative externalities on the networks - by undermining the Internet Invariants - and more broadly on governance and participation in the digital economy.

3.3.1- Externalities on the Internet Invariants

Internet Invariants	**Externalitiies of Extra-Territorial Jurisdiction**
Global reach and integrity: An 'end	**Internet fragmentation**: negates and

[15] Ibid

LEGAL CHALLENGES IN DIGITAL MEDIA

to end' Internet where information sent from any point can get to any other in any network around the world. **Accessibility**: Anyone can use the Internet, not just to consume but to contribute content, put up a server and attach new networks.	challenges the global reach and integrity of the Internet; creates 'second class citizens' where access to information and communication tools is uneven.
General purpose: The Internet is not designed for specific purposes or business models, but for general use. **Reusable building blocks**: Technologies may be deployed for one purpose, but used later or by others to do something new. **No permanent favourites**: Success depends on relevance and utility, not on special status. It must not be 'locked in' by today's winners. **Permission-less innovation**: Anyone can set up a new service on the Internet without having to ask permission, as long as it meets existing technical standards and best practices.	**Inconsistency** - Different stakeholders try to enact decisions and complicated rules that are often not easily enforceable. With a proliferation of rules and complexity, the largest organizations can most easily comply, creating competition issues for smaller firms and even a **new digital divide** between large and established companies, and smaller, potentially more innovative ones. Vertically integrated solutions driven by the legal and cultural backgrounds of the biggest players and countries are favoured, instead of open, reusable technologies that can be repurposed by new players. Instead of being distributed around the world, the benefits of the Internet are increasingly concentrated in the countries with the most international influence and the companies with the resources to comply, turning certain companies into *permanent*

LEGAL CHALLENGES IN DIGITAL MEDIA

	favourites.
Interoperability and mutual agreement: through open technology standards and mutual agreements between operators of different parts of the Internet. **Collaboration**: The best solutions to new issues come from willing collaboration between stakeholders.	**Power-grabs** – States try to grab or reassert power at the international stage, as each races to come out on top, imposing unilateral interests in a top-down, closed way. This intensifies both jurisdictional conflicts and friction between networks. **Uncoordinated action** - Unilateral top-down actions displace and undermine collaborative ways of examining issues. They can negatively affect the development of the network. Because the Internet is a network of networks, if changes are imposed on different networks there is a risk that those networks stop working together. This pulls stakeholders apart instead of bringing them together, resulting in a 'zero-sum game' world where everyone is a loser.

LEGAL CHALLENGES IN DIGITAL MEDIA

3.3.2- Broader externalities

These concern a range of political and economic externalities that affect both governance and how people participate in the digital economy:

- Fragmentation: As well as creating a fragmented Internet, extra-territorial jurisdiction drives both governmental and commercial fragmentation,17 leading to narrow and reduced offerings across various countries.
- Business model disruption as businesses try to cope with the compliance burden of possibly conflicting laws. This creates added uncertainty for companies operating globally and weakens the framework of international trade and investment. It can also drive consolidation and competition issues if only the biggest and best-resourced companies can cope with the legal complexity and business risk of compliance.
- The creation of second class citizens suffering from new digital divides. As technology advances in certain parts of the world, many countries consider regulation as a means to 'catch up' with such progress. Such regulation risks being narrow in scope and reflecting cultural, economic and social sensitivities incompatible with those in other countries. This limits the range of information and services available, creating new digital divides for users in different countries.
- International tension and resentment generated by states imposing their will in other countries. When one state actor is seen as aggressively using domestic law to assert its hegemony globally, we can expect others to react accordingly[16]. Additionally, extraterritoriality undermines international collaboration by diverting attention and resources from developing collaborative frameworks and international norms. Extraterritoriality creates a patchwork of inconsistent rules as

[16] There is precedent: Kenneth W. Dam, Extraterritoriality in an Age of Globalization: The Hartford Fire Case, 1993 SUP. CT. REV. 289, 324; see also Thabo Mbeki, Presi- dent of South Africa, Statement to the National Houses of Parliament and the Nation at the Tabling of the Report of the Truth and Reconciliation Commis- sion (Apr. 15, 2003), http://www.anc.org.za/ancdocs/history/mbeki/2003/tm0415.html

LEGAL CHALLENGES IN DIGITAL MEDIA

different institutions in different countries approach international issues using different laws and procedures.

3.4- Principles for dealing with Internet-related decisions and regulation

We are just beginning the conversation on regulation. Some regulators and judges may be dealing with these topics for the first time. These preliminary principles are intended to help decision-makers to achieve their goals while ensuring the Internet still drives social empowerment and economic growth, both at home and abroad:

3.4.1- Weigh Risks and Benefits.

- The most limited and targeted decisions will create the least unintended negative consequences. Does the decision have to have extra-territorial effect for it to work?
- Actively consider the role and impact of decisions on other stakeholders, including in other countries.

3.4.2- Check what's been done before.

- It's likely other governments or courts have pondered the same challenging questions, Resources to check how others have approached issues may be available from international or regional organizations[17], including regulatory best practices, norms and even suggested legal frameworks.

3.4.3- Be mindful of the properties of the Internet.

- The Internet's unique properties – the "Internet Invariants" - can provide an additional benchmark in determining the effectiveness of regulation. We encourage policy makers to add them as evaluators for sound decision making.

3.4.4- Focus on the activity/behaviour, not the medium.

- Design laws, rules and decisions to deal with the undesirable or illegal activity or behaviour itself, rather than the medium it occurs in. For example, is fraud that

[17] ("[W]e consider it completely unacceptable that matters that are central to the future of our country should be adjudicated in foreign courts which bear no responsibility for the well-being of our country.").

LEGAL CHALLENGES IN DIGITAL MEDIA

occurs online – e.g. phishing - substantively different from offline fraud? While the Internet adds new dimensions or can change the scale or reach of an activity, it doesn't always require rule-making targeted at the Internet itself.

3.4.5- Seek out collaborations with other stakeholders

- Actively seek out opportunitiies to resolve issues with all relevant stakeholders, including at the regional and international level where cooperation and collaboration on norms can be highly effective.

3.4.6- Apply the principle of proportionality

- Has the regulatory measure gone beyond what is required to attain a legitimate goal? Do its claimed benefits exceed the costs?

There is much work to do so the traditional nation-state approach to regulation and the global Internet can continue to evolve. These priinciples are a starting point. There is a need to both acknowledge and resolve some of the differences identified in the legal systems around the world, and to ensure the Internet remains a source of opportunity and a force for good.

Africa				
Country	Statue Name	Year of Adoption	Category	Description of Extraterritorial Effect
Kenya	Computer and Cybercrimes Bill	2018	Cybersecurity, Freedom of Expression	This bill introduces 17 offences intended to prevent and control cybercrime, including imposing penalties on individuals circulating "false, misleading or fictitious data," whom share pornographic content, or whom engage in cyber terrorism. Extraterritorial effect: the bill has a broad scope and Section 42 (2) makes it

LEGAL CHALLENGES IN DIGITAL MEDIA

				clear that this law applies outside of Kenya if an offence is committed by a Kenyan citizen or someone ordinarily resident in Kenya.
South Africa	Cybercrime and Cybersecurity Bill	2017	Cybersecurity	This legislation criminalises cyber-facilitated offences of fraud, forgery, and extortion. Extraterritorial effect: South Africa's jurisdiction will be expanded to "all offenses which can be committed in cyberspace ... to deal with cybercrime which originates from outside our borders" (*extraterritoriality by design*).
	Electronic Communications and Transactions Act	2002	E-Services, Security	This law seeks to enable and facilitate electronic communications and transactions. It also introduced requirements for government agencies to roll out e- services, and criminalises certain cybercrimes like hacking, phishing, and intercepting or interfering with data. Extraterritorial effect: Section 90 of the law states that a court in South Africa has jurisdiction where "the offence has had an effect in the Republic [of South Africa]."

LEGAL CHALLENGES IN DIGITAL MEDIA

Tanzania	Electronic and Postal Communications (Online Content) Regulations	2018	Media Regulation, National Security	This law introduces a requirement for all blogs that contain information about the Tanzanian government to hold a license to do so. Permits can subsequently be revoked if a website publishes content that "causes annoyance, threatens harm or evil, encourages or incites crimes" or jeopardizes "national security or public health and safety." Bloggers must also remove "prohibited content"
				within 12 hours or face fines of not less than five million Tanzanian shillings or a year in prison. Extraterritorial effect: any blog posting information about Tanzania, regardless of where it is hosted in the world or the nationality of the author or publisher, is prior to publication required to obtain a license from the Tanzanian government.
Uganda	Over the Top Services Tax	2018	Internet Freedom	Uganda has imposed a levy of 200 Ugandan shillings per day on citizens who use social media platforms like Facebook, Skype, Twitter, and WhatsApp. Extraterritorial effect: the law applies to all Ugandan citizens, everywhere in the world (at present it is only being

LEGAL CHALLENGES IN DIGITAL MEDIA

				implemented on a national level, with the country's major telecom companies developing special mobile money menus through which users can pay the tax.) Note: this law is still alive as of the date of publication: http://www.theeastafrican.co.ke/business/Ugandan s-raise-volume-on-social-media-tax-protests/2560-4680280-i4ipp0/index.html
Zambia	Cybersecurity & Cybercrimes Bill	2018	Cybersecurity	The bill was adopted to "promote an increased cybersecurity posture, facilitate intelligence gathering, investigation, prosecution and judicial processes in respect of preventing and addressing cybercrimes, cyber terrorism and cyber warfare." Extraterritorial effect: Part XI of the law is extraterritorial, noting that it applies to "any person, irrespective of the nationality or citizenship of the person" who engages in a cybercrime, "directed against equipment, software, or data located in Zambia regardless of the location of the person."
Asia-Pacific				
Country	Statue Name	Year of	Category	Description of Extraterritorial Effect

LEGAL CHALLENGES IN DIGITAL MEDIA

		Adoption		
Australia	Interactive Gambling Amendment Bill	2017	Gambling	This law requires any website which provides or advertises online gambling services, regardless of whether or not the vendor has assets in Australia, to obtain a license from a designated agency if it makes its services available to Australian users. Extraterritorial effect: the law states "this Act extends to acts, omissions, matters and things
				outside Australia" for the purposes of applying civil non-compliance provisions.
	Privacy Enhancement (Enhancing Privacy Protection) Act	2014	Data Protection	This law introduces a set of privacy principles that are intended to see personal data be handled and stored in a more secure manner throughout its lifecycle. Extraterritorial effect: an organization "carrying on business" in Australia must comply with this law even if domiciled in a foreign jurisdiction. This will necessarily include foreign organizations with an online presence,

LEGAL CHALLENGES IN DIGITAL MEDIA

				even if that entity has no physical presence in Australia, if it has customers located in Australia.
	Spam Act	2013	Advertising	This law regulates the distribution of unsolicited electronic communications. Extraterritorial effect: Section 14 of the Act applies where an Australian computer network has received a spam message.
	Therapeutic Goods Advertising Code	2018	Advertising	This regulation introduces new required warning statements that must be displayed or communicated to consumers before medicines can be sold, and clarifies that no advertisement may target a person under 12 years of age. Extraterritorial effect: Section 6 states that the law applies "in Australia and a place outside Australia," if it involves "the promotion of therapeutic goods online" by either an Australian business targeting consumers abroad, or a foreign business targeting Australian consumers.

LEGAL CHALLENGES IN DIGITAL MEDIA

China	Anti-Terrorism Law	2015	National Security	This law requires both Chinese and foreign technology companies to create 'cyber police stations' which provide Chinese law enforcement with surveillance access to any and all data concerning Chinese users. ISPs and platforms are also obliged to block terrorism-related content if asked to do so by designated law enforcement. Extraterritorial effect: the law applies to any data concerning a Chinese national, regardless of where in the world he or she may live.
	Cybersecurity Law	2017	National Security	This law applies to all enterprises that employ networks or information systems in their operations and sets forth significant cybersecurity obligations.

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER IV

GLOBAL INTERNET GOVERNANCE AND ITS IMPLICATIONS FOR DIGITAL MEDIA

LEGAL CHALLENGES IN DIGITAL MEDIA

GLOBAL INTERNET GOVERNANCE AND ITS IMPLICATIONS FOR DIGITAL MEDIA

4.1 Introduction

Today the Internet has seen a radical dramatic shift. In many senses, this dramatic shift is symbolized by the emergent new social media revolution. Social networking websites have taken the imagination of the netizens by storm. Constantly, more and more numbers are thronging on to various established and new social networking sites not only to give vent to their own thought process, ideas, viwe points and perspectives but also to interact with other friends, acquaiintances, business partners and similar minded persons. The emergence Internet after the advent of the World Wide Web and te email.

However the emergence of social media networks have demonstrated that there are a lot of complicated legal issues pertaining to the saiid social networking platforms. These legal issues pertain to a variety of distinct yet diverse subjects.

There are complicated and technical legal issues not only relatiing to user generated content or third-party data that is generated by subscribers on the social networking sites but also with other related apsects.

Issues pertaining to the ownership of the said data is still not clear.

There are issues pertaining to data protection as also violation of privacy.

Further, social networking sites are today increasingly being thronged by cyber criminals and cyber terrorists not only to help facilitate and execute their criminal intentions but also to intermingle with the masses and the huge internet traffic existing on the websites to identify more about the psyche and thinking of the netizen community.

As time passes by, the legal issues surrounding social media shall be of tremendous significance. These legal issues are currently beginning to emerge but are likely to consume sufficient attention and time of the relevant stakeholders over a period of

LEGAL CHALLENGES IN DIGITAL MEDIA

time. At the IGF 4 meeting in Egypt, it has been discussed and decided to set up a 'Dynamic Coalition on Social Media and Legal Issues', in a bid to generate discussions, debates, analysis and awareness about the various legal issues surrounding the use of social media, social networking websites and social media plarforms as also data and information residing therein. The Coalition's objectives are;

- To help identify exiisting legal challenges and issues pertaining to social media.
- To identify existing and potential legal responses to complicated legalities of social media.
- To help provide a global platform for discussion and debate on the nuances and technicalities of legalities surrounding social media.
- To provide a fertile ground for providing debate discussion and analysis of legalities surrounding social media for the relevant stakeholders of social media.

Internet governance is defiined as 'the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet'.

This definition, developed by the Working Group on Internet Governance (WGIG), dates back to 2005, and has remained unchanged ever since. The Internet governance regime has continuously evolved since then, and is now a complex system involving a multitude of issues, actors, mechanisms, procedures, and instruments.

4.1.1 How did the Internet start?

The Internet started as a project sponsored by the US government: in the late 1960, the Advanced Research Projects Agency Network (ARPANET) was developed with the aim to facilitate the sharing of digital resources among computers. With the invention of the Transmissiion Control Protocol/Internet Protocol (TCP/IP) in the mid-1970s, ARPANET network evolved into what is now known as the Internet. In

LEGAL CHALLENGES IN DIGITAL MEDIA

1986, the Internet Engineering Task Force (IETF) was created and it managed the further development of the Internet through a cooperative, consensus-based decision-making process, involving a wide variety of individuals.

4.1.2 What was the DNS war?

In the early days of the Internet, there was no central government and no central planning to guide its evolution. But this decentralised approach began to change as governments and the private sector realised the importance of the Internet as a global network. In 1994, the US National Science Foundation, which at that time managed the key infrastructure of the Internet, decided to subcontract the management of the Domain Name System (DNS) to a private company – Network Solutions Inc. This move lead to the so-called DNS war, which also brought new players into the picture: international organisations and nation states. As a consequence, a new organisation was created in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN), which became the coordinator of the main Internet technical resources.

4.1.3 Who defined Internet governance, and why?

The 2003–2005 World Summit on the Information Society (WSIS) officially placed the question of Internet governance on diplomatic agendas. Several controversies emerged at that point.

On the one hand, some countries wanted a restriictive definition of the term, to only refer to the technical management of critical Internet resources. Others were in favour of a broader definition, to cover policy issues such as e-commerce, spam, and cybercrime.

On the other hand, while several countries supported a priivate-sector led model of Internet governance, others argued that governments should be in charge of Internet governance, in the framework of an intergovernmental body such as the International Telecommunication Union (ITU).

LEGAL CHALLENGES IN DIGITAL MEDIA

These controversies led to the creation of a multistakeholder Working Group on Internet Governance, which came up with the above definition of Internet governance. The definition was then accepted by participants in the second phase of WSIS (Tunis, 2005), and became part of the Tunis Agenda for the Information Society.

Who are the Internet governance actors?

According to the definition, there is no single organisation 'in charge of the Internet', but the various stakeholders – governments, intergovernmental organisations, the private sector, the technical community, and civil society – share roles and responsibilities in shaping the 'evolution and use' of this network.

There are now multiple actors which are involved, in one way or another, in the governance of the Internet, and form the so-called Internet governance ecosystem: from the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF), to the International Telecommunication Union (ITU) and the World Intellectual Property Organisation (WIPO), to the Internet Governance Forum (IGF), Internet companies, and NGOs.

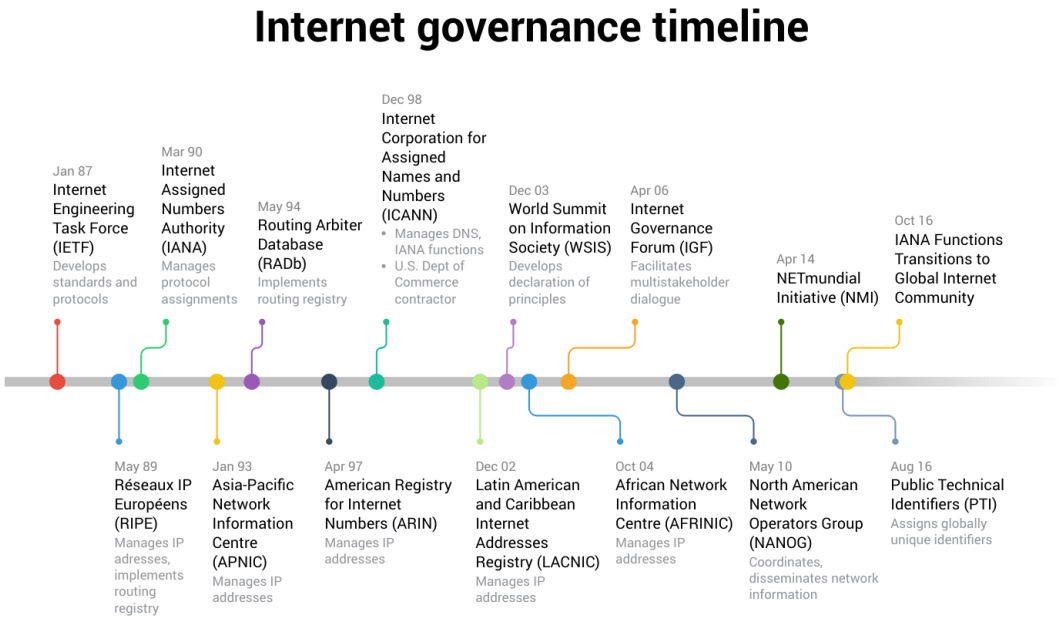
4.2 The Forms of Internet Governance

We say Internet governance and not government because many issues in cyberspace are not and probably cannot be handled by the traditional territorial national institutions. Governance implies a polycentric, less hierarchical order; it requires transnational cooperation amongst standards developers, network operators, online service providers, users, governments and international organizations if it is to solve problems while retaining the openness and interoperability of cyberspace. For better or worse, national policy plays an important role in shaping the Internet, but the rise of cyberspace has produced, and will continue to produce, new institutions and governance arrangements that respond to its unique characteristics.

IGP's analysis of the Internet governance space is informed by institutional economics, which identifiies three broad categories of governance: markets, hierarchies and networks. Markets are driven by private transactions and the price

LEGAL CHALLENGES IN DIGITAL MEDIA

mechanism. Hierarchies govern interactions through orders or compulsion by an authority, such as law enforcement by a state, a biinding treaty, or the organizational control of a firm Networks are semi-permanent, voluntary negotiation systems that allow interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority. Internet governance involves a complex mixture of all three governance structures, including various forms of self-governance by market actors.



The Digital Watch observatory uses the following classification of Internet governance actors: academia/think tanks, business sector, civil society, governments, intergovernmental organisations, technical community, and international organisations. In some instances, the same actor fits under more that one stakeholder group.

Other terms: Digital policy, digital governance, cyber governance, Internet policy

More than 10 years after WSIS, the concept of ‘Internet governance’ remains open and prone to different interpretations.

LEGAL CHALLENGES IN DIGITAL MEDIA

In the public policy debate, other terms are used as well, such as digital policy, digital governance, cyber governance, and Internet policy. Most often, the terms are used interchangeably.

The question of different interpretations arises mainly in relation to the scope of the term, i.e., which issues fall within its remit. Some argue, for example, that cyber security is part of Internet governance, while, for others, this is a separate field in its own. Some say that Internet governance is only about ICANN-related issues (management of domain names and IP addresses). Others extend the coverage of Internet governance to a wide set of Internet-related public policy issues.

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER V

INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS) RULES, 2021

LEGAL CHALLENGES IN DIGITAL MEDIA

INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS) RULES, 2021

5.1 Introduction

With the advancement of sciience, new technologies have provided an opportunity for exponential expansion of print media as well as digital media. The OTT platforms and digital news portals are now establiished and are working well. The problem was that for these new sectors there was no institutional mechanism. When the Press has the Press Council of India and TV has its own self regulation and films have Central Board of Film Certificatiion, these new platforms had no such arrangement. There was a demand for bringiing such parity and mechanism by media experts, filmmakers and industry experts, trade organizations/ bodies and the people at large. These apart, there have been serious griievance from parents and guardians over the adult, violent and such other content which is harmful to children. There is also a need to empower the citizens for their grievance redressal. Due to absence of an institutional set up, citizens do not know where to send their grievances or file complaints or suggestions relating to content on OTT or on digital news. There was demand from all sectors that there must be some arrangement by which a level playing field can be provided to all the media categories.

The Digital Media Ethics Code, under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 establishes an institutional mechanism for digital news portals and OTT platforms.

5.2 Main features of the Rules

The rules establish a soft touch progressive institutional mechanism with a level playing field featuring a Code of Ethics and a threetier grievance redressal framework for news publishers and OTT platforms on the digital media. The OTT platforms would self-classify the content into five age based categories- U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult). Platforms would be required to implement parental

LEGAL CHALLENGES IN DIGITAL MEDIA

locks for content classified as U/A 13+ or higher, and reliable age verification mechanisms for content classified as "A". Publishers of news on digital media would be required to observe Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation) Act thereby providing a level playing field between the offline(Print, TV) and digital media.

5.3 Grievance Redressal Mechanism

A three-level grievance redressal mechanism has been established under the rules with two levels of self-regulation- Level I being the publisher and Level II being the Self Regulatory Body, and the third level being the Oversight Mechanism under the Ministry of Information & Broadcasting. The rules provide for an effective grievance redressal mechanism for receiving, processing, and time-bound disposal of public grievances related to the Code of Ethics. The self regulatory body would be headed by a retired judge of the Supreme Court or of a High Court, or by a person of eminence from the relevant field, and can issue advisories to the publisher. The mechanism is based on the **principles of minimum Government intervention;** however platforms should develop a robust grievance redressal mechanism on their own.

5.4 Benefits of the Rules

The institutional mechaniism established by the Digital Media Ethics Code would provide a stable policy environment to encourage growth in the OTT industry, bring in investments and generate jobs thereby providing a boost to the Champion Audio-Visual Services Sector. Self certiification of content by OTT platforms would ensure artistic freedom for content creators and prevent delays. The Code would also empower the citizens to make informed choices about content, get their grievances redressed in definite time frames, and protect children.

LEGAL CHALLENGES IN DIGITAL MEDIA

The Code of Ethics for news publishers would help to fight fake news on digital media through a mechaniism of accountability of publishers while providing a level playing field between online and offline (Print and TV) news publishers. The rules also open up new avenues for further engagement and coordination with the digital news publishers which would be recognized for the first time under law through the process of furnishing information.

At a time when the digital mediia governance is in a state of flux across the globe, the Digital Media Ethics Code is thus a transformative step which would raise India's stature at an international level and serve as a model for other nations to emulate**.**

Address of Hon'ble Minister for Electronics & Information Technology Shri Ravi Shankar Prasad (25.02.2021) Social Media is welcome to do business in India. They have done exceedingly well, they have got good business, good number of users and they have also empowered ordinary Indians. The Government welcomes criticism and the right to dissent and social media has been used to ask questions too, but it is very important that the users of social media must be given the forum to raise their grievance for resolution against the abuse and misuse of social media . It is very important, with the social media users running into crores, they should be given a proper forum for resolution of their grievances in a time-bound manner against the abuse and misuse of social media. We are empowering the ordinary users of social media. The basic essence of this step is a soft-touch oversight mechanism.

5.5 Key Highlights Of The 2021 IT Rules

5.5.1 Due Diligence by an Intermediary

The definition of 'intermediiary' within the 2021 IT Rules remains the same as provided within the Information Technology Act, 2000 ("IT Act")1, but the 2021 IT Rules now seek to regulate 'sociial media intermediary'2 and 'significant social media intermediary'3 as well. The 2021 IT Rules require all intermediaries to observe "due

LEGAL CHALLENGES IN DIGITAL MEDIA

diligence" while discharging their duties, and as a departure from the 2011 Guidelines, there are certaiin new diligence requirements for intermediaries. For instance, intermediaries are now required to inform users through their privacy policy or user agreements to not publiish or share any information that is: (i) invasive of another's bodily privacy or harassiing on the basis of gender; (ii) patently false or misleading but appearing as a fact; or (iii) false, with the intention of causing injury or to profit.

INDUSLAW VIEW: These incremental additiions to the existing 2011 Guidelines appear to be put in place to check the advent of 'fake news' and 'revenge porn' circulating on numerous platforms. It is pertinent to note however, that terms such as 'harassing on the basis of gender', 'patently false with the intention of causing injury, 'injury', among others, have not been defined, which could be a hindrance in their implementation and could also be a ground for challenging the provision. For instance, in **Shreya Singhal v. Union of India4**, one of the reasons Section 66A of the IT Act was struck down was the observation that as there was no demarcating line conveyed by use of such expressions, it could render the entire Section unconstitutional and vague. Therefore, since the Supreme Court has already criticized the vagueness of similar expressions used in the past, it increases the likelihood that the undefined terms within this Rule could also be similarly challenged on constitutional grounds.

Intermediaries now also have to mandatorily notify users on a yearly basis regarding any non-compliance or change of rules, privacy policy or user agreement, thereby tightening compliance requirements and delegating regulatory responsibilities.

5.5.2 Takedowns

Upon receiving a court order or being notified by the Appropriiate Government5 or its agency regarding unlawful information hosted by the intermediary, the intermediary should immediately ensure that such informatiion is removed from iits platform within 36 hours, in the interest of the sovereignty or security of the State, decency,

LEGAL CHALLENGES IN DIGITAL MEDIA

morality, preventing incitement to an offence relatiing to the above, among others. Further, voluntarily removing information from its platform shall not vitiate the exemption from liability provided to intermediaries under the IT Act.

INDUSLAW VIEW: There have been numerous instances where the Government has sent takedown notices to social media intermediaries for the removal of objectionable or politically-coloured content where, citing the right to freedom of speech and expression and the lack of well-defined law, the platforms have largely not paid heed to such orders. The 2021 IT Rules propose to codify the evolving jurisprudence on this subject. Therefore, in line with the Indian judiciary's interpretation of the safe harbour principles in Section 79 of the IT Act and the 2011 Guidelines, the 2021 IT Rules impose an obligation on the intermediary to take action only upon receiving a court order or a notification from a Government authority. This safeguards the intermediaries from excessive responsibility or liability. The requirement for taking down content by an intermediary only on receiving a lawful order is commendable, protecting the interest of both the intermediary and its users - as it is not practicable for an intermediary to examine all uploaded content to evaluate whether it is liable to remove or disable access. At the same time, the permission to voluntarily take down content to ensure compliance with Rule (3)(1)(b) of the 2021 IT Rules or on the basis of grievance, without any threat to the safe harbour benefit, can jeopardize freedom of speech and expression unless each intermediary implements robust internal controls for self-regulation.

The addition of 'decency' and 'morality' appears to be intended to take full benefit of Article 19(2) of the Constitution as interpreted by the **Supreme Court** in **Shreya Singhal v. Union of India**, when striking down the more looselyworded Section 66A of the IT Act.

5.5.3 Data as Evidence

Under the 2021 IT Rules, intermediaries are expected to store records of any information that has been removed or access to which has been disabled from the platform for a period of 180 days for investiigation purposes or for longer, as opposed

LEGAL CHALLENGES IN DIGITAL MEDIA

to the 90-day requirement under the 2011 Guiidelines. Further, even records of information of users who have withdrawn or cancelled their registration from the platform are expected to be stored for a period of 180 days.

INDUSLAW VIEW: The requirement of storiing records for a longer period for investigation purposes will mean that the intermediaries will have to incur additional costs in preserving and safeguarding user data/records for a longer period, to ensure that there is no misuse or unauthorized access to data during this period. However, retaining information of users who have cancelled their registration from the platform for 180 days appears to be excessive, in light of the extant data privacy framework and global data privacy laws, which require information to be stored for only as long as required. The apparent conflict in treatment of personal data of (for example) an EU resident with the 'right to be forgotten', will need to evolve.

5.5.4 Assisting with Inquiries

In a similar vein, on receipt of a written order, intermediaries have to provide assistance to the relevant Government agency within 72 hours in matters relating to verification of identify, investigation, preventiion of offences, among others6.

INDUSLAW VIEW: The aforementioned Rule does require the order to specify the exact nature of information that is being requested. This may lead to Government agencies fishing for information, thereby exposing the private information of citizens to scrutiny, and drawiing on the technology expertise of the intermediary to help investigate a matter. This may, in turn, create a challenge for intermediaries to strike a balance between complying with the lawful order while safeguarding the right to privacy of its users. In the present case, the scope of this Rule is broader than that conceived under the Code of **Criminal Procedure, 1973**, and has a lower threshold of checks and balances built into it, thus, widening the scope for potential misuse.

5.5.5 Grievance Redressal Mechanism

LEGAL CHALLENGES IN DIGITAL MEDIA

It is pertinent to note that the grievance redressal mechanism has been significantly broadened under the 2021 IT Rules vis-à-vis the erstwhile 2011 Guidelines. Presently, not only should the intermediary publish the name, contact details or mechanism through which a user can complain, but also should acknowledge the complaint within 24 hours and redress it within 15 days of receipt, unliike the one-month period provided earlier. In case the complaint is made in relation to exposure of private parts or impersonation of a person, the intermediary should strive to disable access to such content within 24 hours.

5.5.6 Introduction of Additional Compliances to be Fulfilled by Significant Social Media Intermediaries

A new class of intermediary has been introduced within the 2021 IT Rules, called the **'significant social media intermediary' ("SSMI")** which means a social media intermediary having 5 million or more registered users in India. All SSMIs are required to observe certain additional compliances within 3 months from February 25, 2021, while discharging its duties.

For instance, the SSMI has to mandatorily appoint certain personnel under the 2021 IT Rules, including a (i) Chief Compliance Offiicer; (ii) Nodal Contact Person; and (iii) Resident Grievance Officer. The Chief Compliance Officer is responsible for compliance and can be held liable for contravention of the 2021 IT Rules. The Nodal Contact Person has to be available 24x7 for coordination with law enforcement agencies as required, and the Resident Grievance Officer is in-charge of grievance redressal. A common thread among all these personnel is not only that they are all employees of the respective intermediaries, but also that they have to be resident in India. Moreover, an SSMI is required to have a physical contact address in India to receive communication under the 2021 IT Rules.

INDUSLAW VIEW: The mandate for having a contact address in India and locally present officers in India adds significant legal risk and costs. At the same time, there is greater clarity as to who will be 'on the hook' in case of investigation or non-

LEGAL CHALLENGES IN DIGITAL MEDIA

compliance, and the current practice of summoning country heads or even global heads of organisations may diminish. Further, such requirement may also create permanent establishment risks for certain foreign intermediaries under tax avoidance treaties as global platforms are typically owned and operated in one jurisdiction and other ancillary activities take place physically in the local market. Although the IT Act already provides for extra-territorial jurisdiction, the 2021 IT Rules make it easier for the Indian courts to exercise jurisdiction over intermediaries situated outside India.

5.5.7 Identifying the Messenger

Another decisive addiition made by the Government is the requirement of an SSMI, primarily providing messaging services, to enable the identification of the first originator of informatiion, as required by a court order or as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009. The considerations attached to securing this order are: (i) firstly, for the purposes of prevention, detection or investigation of offences related to the sovereignty and securiity of India, public order, or offences in relation to rape, where the imprisonment is not less than 5 years; and (ii) secondly, as a last resort, when the Government has no other effective means to identify the originator. Further, the intermediary has no obliigation to divulge the contents of the message while identifying the originator. Moreover, in the event the first originator of information is outside Indian territory, then the fiirst originator of information within the territory of India will be considered as the first originator of information for the purposes of the 2021 IT Rules.

INDUSLAW VIEW: Whatsapp, Signal, Telegram and other encrypted messaging services are going to be significantly impacted by the above requirement. This provision appears to have been introduced to cease and curb the nuisance of certain kinds of fake news and conspiracies. To that end, this measure is commendable. Moreover, the requirement of the first originator to be within Indian territory seems to be spurred by the ease of access and ability to hold intermediaries accountable, if they were closer to home. However, as a measure to protect privacy, several of these

LEGAL CHALLENGES IN DIGITAL MEDIA

platforms use end-to-end encryption to ensure that the content of messages shared between two or more people remain priivate. While most messaging platforms are aware of the users' identity (through their mobile number and location), the contents of the messages are usually 'double-encrypted' in that the platform is also not aware of the content. The common belief is that the encryption will need to be broken in order to identify the first originator for the Government; this means that the data from a technology standpoint will be exposed to higher cyber security risk. While the 2021 IT Rules, in not authorising a discovery of content of messages, reflect a nuanced recognition of the extent to which data is double encrypted, the public faith in messaging platforms will be significantly reduced and there is potential for the breach of the fundamental right of speech of Indian citizens. Further, significant costs will need to be incurred in order to have accurate and updated identification records of each user of the platform, in a manner that can be shared with the Government.

The very concept of 'public order' as examined in Shreya Singhal v. Union of India, has a high threshold, where disturbance of public order is to be distinguished from acts directed at individuals which do not disturb the society to the extent of causing a general disturbance of public tranquillity. Therefore, the Government should ensure that for a lawful command on the grounds of 'public order' under this Rule, there needs to be an immediate threat to society as a direct consequence of the messages shared; if not, such messages cannot be said to constitute a disturbance to public order to justify restriction of the freedom of speech. On a related note, offences such as 'murder' do not find their way into the consequences triggering the requirement for identifying first originator of information, and it remains to be seen whether the Government will provide adequate clarification on this front.

The 2021 IT Rules also stipulate that an SSMI should strive to deploy automated tools to proactively identify information that depiicts rape or related offences, as well as information identical to what was previously taken down upon a court order. The automated tools will be periodically reviewed and evaluated in relation to its propensity of bias and discrimination. While the 2021 IT Rules state that only

LEGAL CHALLENGES IN DIGITAL MEDIA

proportionate measures will be taken in relation to this provision, considering the need to ensure priivacy and freedom of speech, the practical implementation of these measures have not been elaborated upon.

INDUSLAW VIEW: The use of such automated tools may arbitrarily, excessively and disproportionately pre-censor information and content, having a chilling effect on an individual's right to free speech. The Government appears to be grantiing interventionist rights to the intermediary directly, and thereby would want to ensure that adequate checks and balances were in place. Indeed, it may be cold comfort to have the Government 'evaluate' artificial intelligence biases within the automated tools, given India's politically charged atmosphere.

5.5.8 Material Risk: flexibility to lower thresholds

The MEITY also has the power to notify any intermediiary, who is not an SSMI, to comply with the additional compliances, in the event the services provided by that intermediary permit transmissiion of information that could create material risk of harm to the sovereignty and security of the country, among other qualifications. 'Material risk' will be determined based on whether: (i) the main services of the intermediary seem to facilitate interaction between users, irrespective of intention; or (ii) the transmission of information is made to a significant number of users, which results in widespread dissemination of information.

INDUSLAW VIEW: This understandably driives a metaphorical stagecoach through the 5 million user threshold for SSMI and affords further unilateral power to the Government in addition to the 2021 IT Rules themselves being outside the formal purview of Parliament.

5.5.9 An Elaborate Censorship Regime for Digital Media

Part - III of the 2021 IT Rules set out the code of ethics, procedure and safeguards in relation to digital media and are applicable to publishers of news and current affairs content, and publishers of online curated content, where such publishers operate in the

LEGAL CHALLENGES IN DIGITAL MEDIA

territory of India or conduct systematic business activity of making its content available in India7.

The 2021 IT Rules provide an inclusive definition of 'news and current affairs content' as well as including "newly received or noteworthy content, iincluding analysis, especially about recent events primarily of socio-political, economic or cultural nature, made available over the internet or computer networks, and any digital media shall be news and current affairs content where the context, substance, purpose, import and meaning of such information is in the nature of news and current affairs content."

'Online curated content' is defined as "any curated catalogue of audio-visual content, other than news and current affairs content, which is owned by, licensed to or contracted to be transmitted by a publisher of online curated content, and made available on demand, including but not limited through subscription, over the internet or computer networks, and includes films, audio visual programmes, documentaries, television programmes, serials, podcasts and other such content."

'Publisher of news and current affairs content' is defined as "an online paper, news portal, news aggregator, news agency and such other entity called by whatever name, which is functionally similar to publishers of news and current affairs content but shall not include newspapers, replica e-papers of the newspaper and any individual or user who is not transmitting content in the course of systematic business, professional or commercial activity."

'Publisher of online curated content' is defined as "a publisher who, performing a significant role in determining the online curated content being made available, makes available to users a computer resource that enables such users to access online curated content over the internet or computer networks, and such other entity called by whatever name, which is functionally similar to publishers of online curated content

LEGAL CHALLENGES IN DIGITAL MEDIA

but does not include any individual or user who is not transmitting online curated content in the course of systematic business, professional or commercial activity."

Part-III of the 2021 IT Rules will be administered by the Ministry of Information and Broadcasting ("MIB").

INDUSLAW VIEW: Considering the fact that the 2021 IT Rules have been issued under Section 87(1) and Section 87(2)(z) and (zg) the IT Act (power of Central Government to make rules)8, empowering MIB to administer a portion of the 2021 IT Rules, namely Part - III, is beyond the scope of implementation of the IT Act. It also seems to be an overreach to use the 2021 IT Rules to expand the regulatory net over digital news publishers.

The 2021 IT Rules reduce the current uncertaiinty surrounding the definition of terms such as 'digital media' and 'news and current affairs', by providing clarity on the scope of such terms. The lack of definition of these terms has contributed to confusion in many spheres of the Indian law, including the foreign exchange management laws in relation to Press Note 4 of 20199. The 2021 IT Rules address the ambiguities that existed within the foreign direct investment poliicy. However, the purview of the IT Act, 2000 does not extend to news media and hence the 2021 IT Rules do not appear to have any legislative backing to regulate news media. Further, there are sufficient existing laws that determine reasonable restrictions on the freedom of press in India.

The definition of 'news and current affairs content' goes beyond the socio-political to cover economic and even cultural news. The net has been cast extremely wide unlike, for instance, the Australian News Media Bargaining Code which focuses on issues of public importance. Moreover, by retaining news aggregators as opposed to original publishers as regulated entities, there is clear signalling by the Government that along with journalistic reporting of news, curation s in itself a regulated activity.

5.5.10 Code of Ethics for Publishers of News and Current Affairs

LEGAL CHALLENGES IN DIGITAL MEDIA

The 2021 IT Rules require the publishers of news and current affairs content to adhere to the Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television and Networks regulation Act, 1995.

INDUSLAW VIEW: The requirement under the Code of Ethiics of the 2021 IT Rules, is an attempt to bring the online news and current affairs publishers on the same footing as the offline news and current affairs publishers.

5.5.11 Additional due diligence to be observed by an intermediary in relation to news and current affairs

An intermediary is mandated to pubilish a clear and concise statement on its website or mobile application, as applicable, informing publishers of news and current affairs that in addition to being governed by the common terms of serviice applicable to all users, these publishers should furnish details of their user accounts on the services of such intermediary to the MIB.

5.5.12 Code of Ethics for Publishers of Online Curated Content

The 2021 IT Rules prohibit the publishers of online curated content from transmitting, publishing or exhibiting any content which is prohibited under any law or by any court of competent jurisdiction. Publishers of online curated content are required to exercise due caution and discretion while featuring the activities, beliefs, practices or views of any racial or religious groups. Publishers of online curated content should classify all content transmitted, published or exhibited by them, based on the suitability of such content for viewers of different ages. The content should also be classified based on the context, theme, tone, impact and target audience of such content as detailed in the schedule annexed to the 2021 IT Rules ("Schedule"). Further, publishers of online curated content should display the rating of any online curated content along with explanation of the relevant content descriptor, in a prominent manner.

LEGAL CHALLENGES IN DIGITAL MEDIA

Publishers should ensure availability of access control mechanism10, including a parental lock to facilitate compliance of age classification of content. Any publisher transmitting, exhibiting or publishing content suitable only for viewers above the age of 18 years, should implement a reliable age verification mechanism for viewership of such content. The publishers of online curated content are further required to take reasonable efforts to improve the accessibility of online curated content transmitted by them to persons with disabilities through implementation of appropriate access services.11

INDUSLAW VIEW: The requirement for the publishers of the online curated content to exercise due caution and discretion with respect to content relating to activities, beliefs, practices or views of any racial or religious groups, is very wide and the term 'exercise of due caution and discretion' creates ambiguity with respect to the responsibility of the publisher. It must be noted that Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television and Networks regulation Act, 1995 do not impose any similar restriction on publishers of news and current affairs content. Though the Norms of Journalist Conduct and Programme Code lay down some guidelines with respect to content relating to religious or communal group, these guidelines are specific and not as wide as the requirement for the publishers of online curated content under the 2021 IT Rules. Considering the difference in the nature of the news and current affairs content and online curated content, it is surprising that the publishers of online curated content are expected to exercise greater responsibility regarding the nature of the content. Imposing such an obligation is an over-reaching exercise of powers over publishers of online curated content.

Though the requirement to implement access control measures to restrict access to content unsuitable for a particular age, is a positive move in protecting the children from inappropriate content, it may be cumbersome for publishers of online curated content to implement these measures, especially for small-scale publishers.

LEGAL CHALLENGES IN DIGITAL MEDIA

5.5.13 Three-Tier Grievance Redressal Mechanism for Digital Media

The 2021 IT Rules provide a three-tier grievance redressal structure for addressing grievances in relation to the Code of Ethics. The publisher shall be the first level of the three-tier structure and is required to set up a self-regulating mechanism and appoint a grievance officer based in India. The publisher is required to issue an acknowledgement for any grievance within 24 hours of its receipt. The grievance officer is required to take a decision on every grievance received by it and communicate the same to the complainant, within 15 days of the registration of the grievance.

At the second level, one or more self- regulatory bodies of publishers will be constituted as independent bodies, by publishers or their associations. The self-regulating body will have a maximum of 6 members, and will be headed by a retired judge of the Supreme Court or a High Court, or an independent eminent person from the field of media, broadcasting, entertainment, child rights, human rights or such other relevant field. Such self-regulating body is required to register itself with the MIB. The self-regulating body has to ensure the alignment and adherence by the publishers of the Code of Ethics, and will hear appeals filed by the complainants against the decision of the publishers. The self-regulating body may then issue guidance or advisory to publishers while disposing a grievance or an appeal against a decision of a publisher.

At the third level, the MIB will develop an oversight mechanism and coordinate and facilitate the adherence to the Code of Ethics by the publishers of news and current affairs content and publishers of online curated content. The MIB will establish an inter-departmental committee (the "Committee"), and an authorized officer appointed by the MIB ("Authorised Officer") will be the Chairperson of such Committee. The Committee will hear complaints arising out of the grievances in respect of the decision taken by the publishers or the self-regulating body, or where no such decision is taken by these bodies within the specified timeline, and complaints referred to it by the MIB. Further, the MIB will also publish a charter, including a

LEGAL CHALLENGES IN DIGITAL MEDIA

code of practice for self-regulating bodies. While disposing a grievance or an appeal, the selfregulating body or the Committee, as the case may be, may issue an advisory or guidance to the publisher in the nature of a warning, censure, admonish or reprimand, or it may require the publisher to submit an apology or to include a warning card or disclaimer. It may also require a publisher of online curated content to reclassify ratings of relevant content, modify the content descriptor, age classification and access control measure or edit synopsis of any content.

INDUSLAW VIEW: While the 2021 IT Rules have introduced a three-tier grievance redressal mechanism involving the publishers, self-regulating body and Committee, the MIB retains the power to refer any complaints directly to the Committee, constituted by MIB, without exhausting either of the first two tiers. It remains to be seen how this will work in practice. The Constitution of India does not grant the executive, the power to judge the suitability of content published by media. At the third level of the grievance redressal mechanism, the 2021 IT Rules have empowered the MIB and the Committee to adjudicate on questions of suitability of the content published by publishers of news and current affairs content and the online curated content. Grant of such adjudicatory powers to an executive branch of the Government, may jeopardize the freedom of the press and media in India. In an event of an emergency, where no delay is acceptable, the Authorised Officer will examine if the relevant content falls within the grounds mentioned under Section 69A(1) of the IT Act12, and whether it is necessary and justifiable to block such content or part thereof. The Authorised Officer will accordingly submit a written recommendation to the Secretary, MIB (the "MIB Secretary").

In the event the MIB Secretary is satisfied that it is necessary and justifiable to block such content, he may issue such direction as an interim measure, after recording the reasons in writing, without providing an opportunity of hearing. In such an event, the Authorised Officer has to seek the consideration and recommendation of the Committee within 48 hours of issue of such direction. The MIB Secretary will pass the final order in accordance with the recommendation of the Committee. In the event

LEGAL CHALLENGES IN DIGITAL MEDIA

the Committee does not approve the blocking of such content, the MIB Secretary shall revoke the interim order

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER VI

JUDICIAL TRENDS

LEGAL CHALLENGES IN DIGITAL MEDIA

JUDICIAL TRENDS

6.1 Introduction

New rules to regulate digital media and online streaming platforms, made official by the Centre on 25 February 2021, are fraught with inconsistencies, ambiguities, go beyond the authority of the government to promulgate and appear to be against constitutional provisions.

The government does not have legislative backing to frame rules to governn OTTs and online publishers of news. Under the IT Act, the government can make rules only for intermediaries and the definition of intermediaries is not broad enough to cover OTTs and online media.

The rules violate rights guaranteed under Part III of the Constitution, and disproportionately impact the freedom of speech and expression, freedom of press, privacy and creative thinking. The apparent vagueness renders the rules unconstitutional and result in a concentration of power in the hands of the Executive by granting it adjudicatory powers.

The new rules were challenged in the Delhi High Court on 6 March by independent website The Wire and The News Minute as posing "profound and serious harms for digital news media… and destructive of their rights". The case is being heard by a division bench headed by Chief Justice DN Patel.

Nithya Ramakrishnan, lawyer for the petitioners, told the court that the new rules, in particular those that relate to the digital news media, "go far beyond anything that is permissible in a democracy". The High Court will hear the case on 16 April.

On 9 November 2020, the central government issued a notification to bring OTT (over the top) or streaming platforms under the ambit of the Ministry of Information and

LEGAL CHALLENGES IN DIGITAL MEDIA

Broadcasting. These regulatiions were notified even though major OTT platforms had already announced a self-regulatory framework, the Universal Self-Regulation Code (USRC), backed by the Internet and Mobile Association of India (IAMAI).

As many as 17 major OTT platforms adopted an 'implementation toolkit' for self-regulation. The government rejected the USRC, remarking that guidelines would be issued soon. On 25 February 2021, the government notified the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, to regulate OTT platforms, such as Netflix and Amazon Prime, intermediaries, such as Whatsapp and Signal, and digital media platforms, such as Article 14.

Not only are the new rules fraught with inconsistencies and ambiguities, they transgress judicial authority, weaken tthe democratic process and open themselves to possible constitutional challenges.

6.2 Govt. Deploys Powers It Does Not Have

The executive has no authority to legislate; it only takes over delegated legislation (delegation of legislative power by the Parliament to the government or agent of lower rank) as per the enabling law or parent act. In KN Guruswamy vs State of Mysore, 1954, the Supreme Court held that any executive action cannot contravene a parent act or exceed the powers granted by the parent act. Justice Vivian Bose remarked that "rules bind state and subject alike".

The new rules are enacted under sections 69A(2); 79(2)(c); 87(1); 87(2)(z) & (zg) of the Information Technology (IT) Act, 2000. These provisions grant the government the power to make rules for an intermediary only.

LEGAL CHALLENGES IN DIGITAL MEDIA

According to section 2(1)(w), an intermediary "means any person who, on behalf of another person, receives, stores or transmits" information. The Supreme Court held in Shreya Singhal v Union of India, 2015, that Internet intermediaries are merely facilitators of content. A 2010 Organisation for EconomicCo-operation and Development (OECD) report, The Economic And Social Role Of Internet Intermediaries , defines intermediaries within the same boundaries explaining that they "do not themselves create or own the content being published or broadcast".

These rules apply to intermediaries, OTT platforms and cover online publishers of news (rule 7), which create and own published content. Since the IT Act grants power to make rules for intermediaries only and the definition of intermediaries is not broad enough to cover OTT and publishers of news, the Rules exceed the authority granted by the parent act and are consequently unconstitutional.

6.3 Fundamental Rights Are Violated

The new rules are rife with provisions that violate fundamental rights guaranteed under P art III of the Constitution.

First, there is a plethora of vague terms in the Rules. For instance, "insulting", "libellous" or "inconsistent". It is a fundamental rule in legal jurisprudence that the governed must be given an opportunity to understand and comprehend what is prohibited. Vague terms lead to an overly broad law that leads to a chilling effect on rights.

The Supreme Court struck down section 66A of the IT Act (the Shreya Singhal case), which too contained the term "insult". Incorporating such terms again in any rule or legislation is an outright rejection of the Constitutional Court's interpretation of fundamental freedoms and the Constitution.

LEGAL CHALLENGES IN DIGITAL MEDIA

Second, since 2017 privacy is a fundamental right in India (Justice K.S. Puttaswamy vs Union of India), yet no data protection law has been enacted to safeguard the rights. Rule 4(2), Part II of the Rules covering Due Diligence by Intermediaries mandates that intermediaries providing services primarily relating to messaging shall enable identification of the first originator of the information.

This implies the termination of end-to-end encryption. Identification of originators is desirable in situations that lead to the disruption of public order; however, it cannot be at the cost of outright violation of privacy.

India does not have data protection legislation or appropriate awareness about the value of privacy. As Chief Judge of the United States Court of Appeals for the Seventh Circuit, Richard Posner, observed in Privacy, Surveillance, and Law (2008), even though "people value their informational privacy.…, they surrender it at the drop of a hat". Posner said people might be willing to reveal information, and in the interest of the nation, they might accept diminished privacy, however, only if it is used for the said purpose.

Third, the rules have a disproportionate penalty for intermediaries who fail to observe "due diligence"—tier III of the regulation calls for an inter-departmental committee that can impose a "take-down order".

If the company or nonprofit in question does not appear before the committee, it can proceed "ex-parte". An important feature of proportionality is the adoption of the least restrictive measure.

The power to impose a take-down order contradicts it directly. Furthermore, the option of proceeding ex-parte is a more blatant violation of the principle. Instead of a notice and take-down procedure, a notice-to-notice procedure would be more appropriate, which means the complainant will send a notice against which the concerned platform can file a

LEGAL CHALLENGES IN DIGITAL MEDIA

counter-notice or remove the content. If the complainant is not satisfied with the counter-notice, he may proceed under appropriate law against the platform. The platfoorm gets a choice and the adjudication, if at all required, will be by the court.

6.4 No Legislative Backing

It might be argued that the state has executive power on matters over which legislation may be passed, as was held in Ram Jawaya Kapur v State of Punjab, 1955. However, this does not mean that the state has unsanctioned power. It is a fundamental concept in constitutional law that state actions affecting fundamental rights must be backed by legislation passed by the Parliament.

The Supreme Court has repeatedly held (here, here and here) that measures that curtail fundamental rights or freedoms must have legislative backing; executive power cannot be used to achieve these ends (State of Madhya Pradesh vs Thakur Bharat Singh, 1967).

Since no legislation permits making rules to regulate OTT platforms or online journalism, the new rules are unconstitutional without an enabling law.

6.5 Powers Concentrated With Bureaucrats

In a constitutional democracy, separation of powers between judiciary and executive is a sine qua non.

As British philosopher A C Grayling writes, the intention is to prevent the concentration of power and prohibit one branch from exercising the core functions of the other.

However, the tier III mechanism establishes inter-departmental committees with representatives from concerned ministers. The constitution of this committee is purely given to the executive, including the chairman, who is an “Authorised Officer” not below the rank of joint secretary.

LEGAL CHALLENGES IN DIGITAL MEDIA

This committee, according to the concept of separation of powers, cannot be granted the power to adjudicate over complaiints regarding the content of OTT, publisher of news or even intermediaries.

Leaving the interpretation of terms in the act, such as “public order”, “insulting”, “inconsistent”, to the executive miight lead to absurd interpretations, even with benevolent intentions. Even if the exercise is effective, the adjudication of disputes is a core function of the judiciary, not the executive.

6.6 Other Concerns

The Rules mandate the appointment of a grievance redressal officer (Rule 10) at level I of the self-regulating mechanism. At Level II, the entities have to constitute an association and then form a self-regulating body; both will be registered. One of the concerns this raises, apart from the cumbersome structure, is the fiinancial burden, especially on platforms that promote independent journalism.

Another flaw is that the tier-III committee of bureaucrats has been given the power to regulate OTT, intermediaries and the media. Publishers of news, in print and online, are already governed by the Press Council of India.

6.7 What Can Be Done Now

It may be argued (here and here) that regulation is necessary. If so, the question is not whether to regulate but how to regulate. Apart from the fact that an enabling law, presented to Parliament, is required to regulate OTT platforms and digital media, not the IT Act, the slippery slopes, ambiguities and concentration of power in the executive must be addressed to maintain India’s democratic character.

LEGAL CHALLENGES IN DIGITAL MEDIA

Regulatory measures could be borrowed from the United Kingdom's Ofcom which regulates telecommunication, broadcasting, radio, mobile phones and other devices that run on airwaves.

Ofcom is paid and funded by the companies it regulates and functions independent of the government. It has monthly meetings and its workings are transparent to the public, uploading as it does the minutes of each meeting on its website.

A feature of deliberative democracy is not just that rules bind the state and subject alike but also that the state and the subject get an equal say in the formation of those rules. The government should have consulted the stakeholders to effectively lay down regulations and not take over independent journalism, freedom of thought, creative thinking and the principles of democracy as a whole

The Delhi HC on Tuesday sought the Centre's response on a plea challenging the new Information Technology rules on digital news media.

A bench of Chief Justice DN Patel and Justice Jasmeet Singh issued notices to the ministry of electronics and information technology and granted them time to file their response on a batch of petitions. The petitioners are Foundation for Independent Journalism and editors of two news websites.

The petitioners argue that the new IT rules issued on February 25 are palpably illegal in seeking to control and regulate digital news media when the parent IT Act nowhere provides for such a remit.

They have sought to declare the "IT rules as void and inoperative insofar as it defines and applies to publishers of news and current affairs content."

LEGAL CHALLENGES IN DIGITAL MEDIA

The petitioners urged the high court to grant them interim protection so that no coercive steps are taken against the digital news media outlets by the authorities till the next date of hearing on April 16.

The HC only said that if any coercive action is taken by the Centre, the petitioners may move the court with an application.

Advocate Nitya Ramakrishnan, representing the petitioners, contended that regulation of news content is not within the Information Technology (IT) Act's purpose. "I am not talking about OTT platforms and social media. I am only concerned with news media and current affairs. The new rules go far beyond anything that is permissible in a democracy," she argued.

The petition assails the new rules as they classify "publishers of news and current affairs content" as part of **"digital media"**, and seek to regulate these news portals under the Rules by imposing government oversight and a "**Code of Ethics**", which stipulates such vague conditions as "good taste" and "decency". The petitioners said they bring out wholly digital news and current affairs publications and are directly affected by this overreach.

One of the major contentions of the petitioners is that the new rules unjustly classify 'news media and current affairs content' as 'digital media', to make them subject to the government's Code of Ethics.

They argue that news portals cannot be classified as 'digital media', because unlike the curated content hosted by digital media, news portals publish news and views. Therefore, the petitioners have restricted the legal challenge to the new rules only to their applicability to news portals and not to OTT platforms.

LEGAL CHALLENGES IN DIGITAL MEDIA

6.8 News Portals Be Regulated Under Information Technology Act

The petitioners argue that the Information Technology Act 'neither intends nor provides' for regulation of news portals. News media can only be regulated under the Press Council Act, 1978, while the Cable TV (Regulation) Act, 1995, provides for a 'programme code' for regulating content on TV networks.

Unlike the Press Council Act, the object and purpose of the IT Act is restricted to legal recognition and authentication of electronic data, electronic commnunication, and receipts of electronic data as evidence.

The Information Technology Act doesn't provide for the regulation of electronic content barring two scenarios:

Defining offences such as cyber-terrorism, sharing of obscene or sexually explicit material, child pornography, and identity theft, and providing punishment for the same.

Issuing a direction to an intermediary under Section 69A for blocking a website in the interest of "sovereignty and integrity of India, defence of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to these".

Can News Portals Be Called 'Intermediaries' Under IT Act?

Section 69 of the Information Technology Act, which proviides for blocking of a website, only stipulates directions to be issued to intermediaries. Petitioners have contended that news portals can't be classified as 'intermediaries' for the purpose of Section 69.

LEGAL CHALLENGES IN DIGITAL MEDIA

The petitioners cite the Supreme Court's judgment in the Shreya Singhal case, where it was held that directions under Section 69 can only be issued either to an 'agency of the government' or an 'intermediary'.

Therefore, the petitioners have argued that news portals can't be included in rules made to regulate content under Section 69 of the Act, as they are neither 'government agencies' nor 'intermediaries'.

In **Shreya Singhal v. Union of India**, the Supreme Court had struck down Section 66A of the IT Act, saying that grounds such as 'annoyance' or 'offensive' are too vague to penalise content. The petitioners argued that by using terms such as 'half-truths', 'decency', and 'good taste' in the new Digital Media Code, the Central government has attempted to use its general rule-making power to unlawfully revive elements of Section 66A.

The government's newly proposed rules also provide for a three-tier Grievance Redressal system.

First, every publisher needs to have a Grievance Redressal Officer to take up complaints by "any person having a grievance regarding content".

Second, publishers or their associations have to create an appellate self-regulating body, with the IT Ministry's approval, which shall have the power to warn or censure, requiring a publisher to apologise or display a warning/disclaimer. This body shall also report non-compliance and certain classes of content to the Tier-3 body.

Third, the creation of another appellate body – an Inter-Departmental Committee, headed by an 'Authorised Officer' of the Government of India, and consisting chiefly of serving officials from various ministries. Apart from being the appellate body, it

LEGAL CHALLENGES IN DIGITAL MEDIA

can also take complaints directly referred to it by the Information and Broadcasting (I&B) Ministry. It can recommend to the I&B Ministry the modification, deletion, or blocking of content in the case of certain perceived dange

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER VII

CURRENT CHALLENGES OF DIGITAL MEDIA WITH RESPECT TO MEDIA LAW AND ETHICS

LEGAL CHALLENGES IN DIGITAL MEDIA

CURRENT CHALLENGES OF DIGITAL MEDIA WITH RESPECT TO MEDIA LAW AND ETHICS

7.1 Introduction

As media influence grows beyond human reach, the fourth pillar of democracy takes pride in being fair, impartial, and presenting the facts. However, as recent events demonstrate, media is confronted with several challenges that jeopardiize its very own function, including the current test of nationalism in the name of religion, hate crimes, and social evils; the media has played a disastrous role, whetherr it is through the propagation of religious ideologies, poor reporting in sensitive cases or investigative cowboy journalism that harmed the media's credibility.

With time, the media's methods of disseminating its views, viiewpoints, evidence, and knowledge have expanded. Nowadays, knowledge is exchanged in a variety of ways– including blogs, Whatsapp groups, YouTube channels, television channels, newspapers, magazines, smart phone and desktop apps. India has grown into one of the world's largest media markets.

There are various unethical media law practices in our Indian journalism sector at present

7.2 Paid News:

It is one of the most serious challenges to media. It is fundamental ethiical media to be truthful and faiir since a vast number of people will eventually see it and shape their opinions based on it

7.3 Possible Solution:

LEGAL CHALLENGES IN DIGITAL MEDIA

Awareness should be there in viewers to identify which journalist propagates one-sided view and does not identify the key issues at present. Thus paid news can be identified easily by way of targeted advertisements or sponsorships or targeting any specific community of the society. Hence viewer's education is a must to deal with this problem.

7.4 Media Trial:

A media trial is a trial similar to a court of law in which the media house declares an individual innocent or guilty before the court's final judgment based on debates and discussions. Additionally, it results in the formation of beliefs in the minds of individuals, thus impacting the case's meritocracy. The media trials were visible in the Jessica Lal murder case and the Sushant Singh Rajput drug case, among others.

7.5 Possible Solution:

Self Regularisation of Media channels by way of ethical codes put forthwith by The News Broadcasting Standards Authority (NBSA) should not only be limited to fines or reprimand but also strict legal actions against the TV channel by suspending them for a temporary period or criiminally charging them in the court of law should be implemented. Repeated offenders of such media channels should also face strict action by the Press Council of India; although it does not have much power at present but more power should be given to such kind of bodies.

7.6 Lack of Diversity in Reportage:

LEGAL CHALLENGES IN DIGITAL MEDIA

There are 800 television channels in India, as well as 36,000 weekly magaziine publications and thousands of web portals. On the surface, there is a dearth of variiety in news coverage as a result of the 'tyranny of distance'.

For instance, many remote areas, such as the northeast, south India, and tier-3 cities, receive little coverage in the national media. With such impediments to journalistic freedom, it is important to consider the strength of the fourth pillar of our democracy's base.

7.7 Possible Solution:

Promoting independent journalism whiich is free from external political influences by increasing their watch time and financially supporting them at our end; for example, Schoop Whoop Unscripted, Quint and other regional media houses have a long way to go in our future journalism industry.

7.8 A Handful Ownership of Media:

Transparency in the inner workings of Indian media organisations is diminishing resulting in the jeopardization of the media's reputation.

The majority of Indian media outlets are owned/ operated either by politically connected individuals or businessman having their political influence inclined towards one political party. For instance, Subhash Chandra, a BJP Member of Parliament, owns the Zee Network, which includes the channels Zee News, Wion, and others

LEGAL CHALLENGES IN DIGITAL MEDIA

7.9 Possible Solution:

According to the European Broadcasting Union (EBU), it was seen that the countries with functioning public media have greater press freedom and less corruption. Thus, establishing a public funding mechaniism for the media can be a step towards enhancing media freedom.

7.10 Attack on Journalist:

With the rising hate crimes and threat calls faced by a journalist in today's era becomes a very serious issue for the media industry to provide fair reporting in any subject matter especially after the death of **Gauri Lankesh** - news reporter; hence it becomes an impediment for the current lot of journalist to provide fearless journalism.

Therefore in any large scale democracy; "dissent is the safety valve of the democracy" as said by Justice **Chandrachud**; but still these ground reporters are faced by NSA (National Security Act), UAPA (Unlawful Activity Prevention Act) wherein they have to face serious legal issues. An example being the Uttar Pradesh incident of ground reporting showing the incompetence of Mid-day meal schemes of state government wherein the reality was as shocking as reported by the media person.

7.11 Possible Solution:

(Independent Judiciary + Independent Media + Citizen Awareness) are the key to tackle such issue legally. Media is the fourth pillar of democracy which needs to

LEGAL CHALLENGES IN DIGITAL MEDIA

complement such issues raised by the public or judiciary at various point of time impartially and not become just a mere spectator or puppet for the government.

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER VIII

DIGITAL MEDIA: THE FOURTH PILLAR OR KILLER OF DEMOCRACY

LEGAL CHALLENGES IN DIGITAL MEDIA

DIGITAL MEDIA: "THE FOURTH PILLAR OR KILLER OF DEMOCRACY"

8.1 Introduction

The media is supposed to exist to maintain the bridge between the government and the people. The press is also called the fourth pillar of democracy. Relyiing on these two statements, the highly important role that the media plays in our day to day life is pretty evident. The media must act as a thiird eye to the government and must keep us aware and informed of what is happening around the world. But things can become very ugly when this media acts as a barrier for the people; when, instead of focusing on the critical issues, it diverts us to another topic.

Sadly this is the reality; this is what Indian media does these days. 2020 has been a bad year for almost everyone, with disasters like high-scale job losses, COVID deaths, economy, GDP, healthcare system, Indo-china clashes and so on. Here, I'll try to explain briefly some topics where the Indian media had failed to do its job.

8.2 Sushant's Case

The suicide case of the actor, Sushant Singh Rajput was the most trending topic in recent past, which started with a perfect objective of demanding CBI inquiry for Sushant's death. But, now, the media has made this case into a real-life circus. Although the movement began with the demand for #JusticeForSSR, no one knows when it turned into "Justice for Kangana Ranaut." The media started this topic with nepotism and ended up with drugs in Bollywood. Right now, the case is under investigation. But the media is debating on this topic every day rather than focusing on real-life issues.

LEGAL CHALLENGES IN DIGITAL MEDIA

8.3 Entrance Exams During COVID

Students from the whole country protested against the exams. Almost every day, the demand to postpone the exams was trending on Twitter, but neither the government nor the media listened. The riisks involved to the lives of lakhs of students in conducting exams were not considered important enough to broadcast on TV channels. At last, no one listened, and the exams did happen.

8.4 Death Rates

We have the data on the number of people dying due to COVID. But no one is looking at the number of deaths and suicides happening nowadays due to job losses, hunger, depression and whatnot. But according to the media, “Sab Changa Si” (Everything is Fine).

8.5 Why Is The Media Doing This?

The answer to this question lies in the present condition of the country, which everybody knows is not stable. GDP growth rate has come down to -23.9%, but now also, the Indian media is puttning its all efforts to distract the people to a diifferent topic.

In a survey, it was found that fake news spreads six times faster than the actual news. So, keeping this in mind, not just the mediia but also the social media trolls try their level best to spread fake news, so that the people must stay diverted from the real issues at hand. Not only the media, but the government is also equally responsible for this ongoing act.

LEGAL CHALLENGES IN DIGITAL MEDIA

Our news channels can question Kangana the whole day on useless topics, but they don't have the guts to question the government regarding the economy of the country. While there are several cases where the media has failed to broadcast accurate news, only a few have been mentioned above. Recently a farmer's protest in Haryana turned violent when police allegedly lathi-charged them. But still, there is no coverage on the news channels. What else can one expect when raising your voice becomes anti-national in a democratic country?

LEGAL CHALLENGES IN DIGITAL MEDIA

CHAPTER IX

CONCLUSION AND SUGGESTIONS

LEGAL CHALLENGES IN DIGITAL MEDIA

CONCLUSION AND SUGGESTIONS

India, which is known to be the largest democracy, has now dropped ten places in the Democracy Index Global Ranking to 51. The media needs to wake up; theiir work is to show the right information to the public and not spread fake news. Instead of staying biased towards a single government, they have to remaiin neutral. Nobody is interested in listening to news that is already irrelevant, and that too from a noisy anchor. This also does not create the right image of the country worldwide. Additionally, along with merely running after TRP, diistracting people from the main topic is not a task worth doing for any respectable journalist.

Leveraging digital media is a necessary marketing strategy for all businesses, but it can be tough to know what kind of media to produce and where to place it. You may have taken care of the basics — settiing up social media accounts and responding to fans online — but you can follow the latest trends to make sure you're in step with where the public is flocking and that your brand is part of the action.

The constriction of immunity enjoyed by intermediaries was long in the making. It remains to be seen how these 2021 IT Rules will play out in practice and whether the Government will indeed adopt a liight touch in exercising its vast powers. There is a case to be made that Indian authorities need more and not less guidance in matters of freedom of speech. The year 2020 was replete with instances of takedowns and blocks without much explanatiion from the Government. The new 2021 IT Rules will now at least mandate reasons for such takedowns to be debated, and provided the three-tier grievance redressal mechanism works, it will provide material for the High Courts and Supreme Court to examine them, in the event Government actions are challenged. Intermediaries now have enhanced due diligence and monitoring burdens, and are also expected to continuously educate users on what can and cannot be posted. This will assist in establishing a trend of self-regulation, especiially in relation to social media intermediaries, thanks to tools provided by artificial intelligence.

LEGAL CHALLENGES IN DIGITAL MEDIA

Invariably, as with implementation of any major legiislation, we can expect a long process of trial and error. It is however undeniable that freedom of speech on the internet may well end up being regulated much more than in the past. The added liabilities for publishers of news and current affairs content and publishers of online curated content are burdensome and will significantly encumber digital media in India.

LEGAL CHALLENGES IN DIGITAL MEDIA

BIBLIOGRAPHY

LEGAL CHALLENGES IN DIGITAL MEDIA

BIBLIOGRAPHY

Books

- Basil S. Markesinis 1999.
- Bing Juris Jon , ‘‘‘Data Protection in Norway’’ 1996.
- Chopra Deepti and Merrill Keith, “Cyber Cops, Cyber Criminals and Internet”, New Delhi :
- I.K. International Ltd., 2002.
- Ghandi,P.R., The Human Rights Committee and the Right ofIndividual Communication: Law and Practice, 1998.
- M.P. Jain, "The Constitution of India", VIIIth Edition, 2012.
- Dr. J.N. Pandey, "Constitutional Law of India", 52nd EDN edition (2015)
- P.M. Bakshi, " Commentary on the Constitution of India: An Exhaustive Article Wise Commentary on the Constitution of India Based on Plethora of Case Law", 2014.
- J.N. Pandey, "Constitutional Law of India", 2016.
- Anderson David A., The Failure of American Privacy Law, in Protecting Privacy, 139
- Ian Hosein and Simon Daviesd, "Liberty on the Line" in Liberating Cyberspace, London: Pluto Press, 1998.
- James, Skone, Copinger and Shone James on Copyright, 13th ed., Sweet & Maxwell, 1991.
- Merrills, J.C. and Robertson A.H., Human Rights in Europe: A Study of the European Convention on Human Rights, 2001,

LEGAL CHALLENGES IN DIGITAL MEDIA

- Miller Arthur R., The Assault on Privacy -Computer Data Banks and Dossiers, 2nd ed., Ann
- Arbor: The University ofMichigan Press, 1971.
- Naikar Lohit D., "77ie Law Relating to Human Rights", Bangalore: Pulani and Pulani, 2004.
- Nirmal, Chairanjivi J. Human Rights in India, Historical, Social and Political Perspective, New
- Delhi: Oxford University Press, 2002.
- Ovey Clare & White, Robin C.A., and Jacobs: European Convention on Human Rights, 2002.
- Radin Margaret Jane et al, "Privacy Online in Internet Commerce: The Emerging Legal
- Framework", New York: Foundation Press, 2002.

ARTICLE /JOURNALS

- Alpa,Guido The Protection ofPrivacy in Italian Law: Case Law in a Codified Legal System,
- Tul.Euro.Civ. LF 1,2 (1997).
- Amelung Tilman Ulrich, Damage Awards For The Infringement Of Privacy - The German
- Approach, 14 Tul. Euro. Civ. LF 15, 19 (1999).
- Beaney Wiliam M., "The Right to Privacy and American Law", 31 Law & Contemp. Probs. 253, 255 (1966)

LEGAL CHALLENGES IN DIGITAL MEDIA

- Bergmann Susanne, Publicity Rights in the U.S. and in Germany: A comparative Analysis, 19 Loy. L.A. Ent. L.J. 479, 480 (1999).
- Bryniczka Peter M, Irvine v. Talksport Ltd.: Snatching victoryfrom the jaws ofdefeat—English law nowoffers betterprotection ofcelebrities ' rights, 11 Sports Law. J. 171, 193 (2004).

WEBSITE :

- http://articles economicstimes.indiatimes.com/2010-06-27/news/27596832-1-data-double- taxation-avoidance-agreement-check-tax-evasion
- https://www.efforg/node/56457.
- http:// law. berkeley . edu/privacycensus.html.
- http://crypto.stanford.edu/—dabo/pubs/abstracts/privatebrowsing.html.
- https://www.privacyrights.org/print/fs/fs18-cyb.htm visited 29th January 2017.
- http://supportgoogle.com/accounts/bin/answer.py?h1=en&answer=32050.
- http://searchsecurity.techtarget.com.
- http://searchwebservices.techtarget.com.
- http://searchmobilecomputingtechtarget.com.

LEGAL CHALLENGES IN DIGITAL MEDIA

- http://vvww.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times¬per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html?hpid=z2
- http://cis-india.org/internet-goveniance/publications/privacy-it-act.docx/