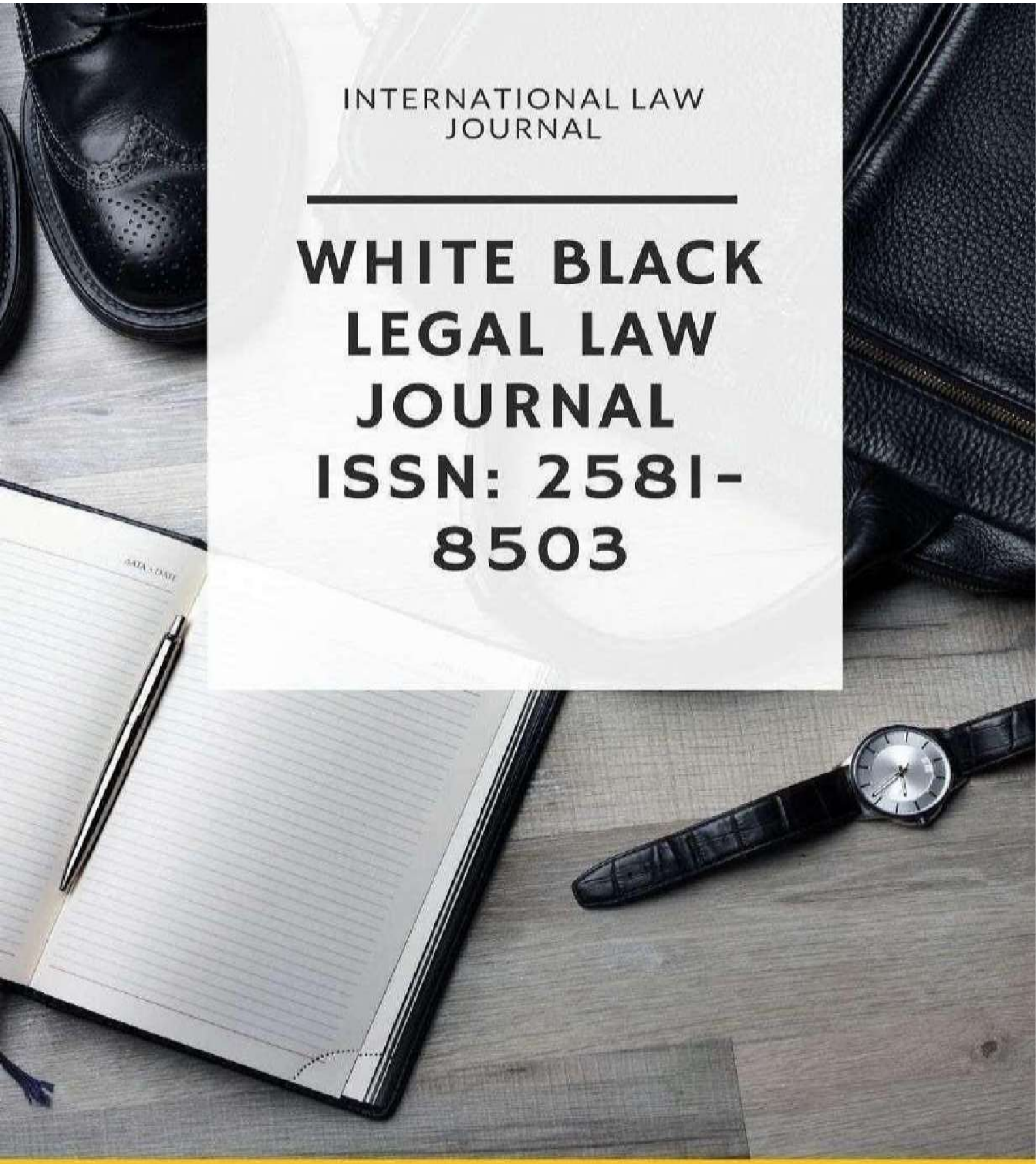

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public a professional Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

LEGAL AND ETHICAL CHALLENGES POSED BY TECHNOLOGY: IS AMENDMENT OF LAW THE ANSWER?

AUTHORED BY – DR. RAJU NARAYANA SWAMY IAS

Concept and Introduction

The interface between law and technology has been summarized in the golden words of Daniel J. Gifford, "Law and technology interact when legal rules foster or retard the development of technology. They also interact when society decides that technology produces undesirable results and employs legal rules to contain or modify those results".

Law, as we are aware, is a set of pre-set rules meant for the purpose of keeping peace and security in society. It is a social engineering which means a balance between the competing interests in society. Technology, on the other hand means the use of scientific knowledge for practical purposes or applications, whether in industry or in our everyday lives.

Industry 4.0 (viz) the digital industry employs a wide range of technologies which include:

a. Robotics
b. Mobile devices and 5 G
c. Internet of Things (IoT) platforms
d. Location detection technologies
e. Advanced human – machine interfaces
f. Authentication and fraud detection
g. 3 D printing
h. Smart sensors
i. Big analytics and advanced processes
j. Multilevel customer interaction and customer profiling
k. Augmented reality / wearables
l. On-demand availability of computer resources (Cloud)
m. Data visualization and triggered "live" training.

However the major components thereof can be classified under the following heads:

I) Cyber physical systems, Cloud computing

II) IOT

III) AI & ML

IV) Big Data

Needless to say, the interface of each of these technologies with the legal framework is complex. The internet infrastructure itself raises myriad legal concerns- ICANN jurisdiction, competition law and policy, network neutrality, infrastructure-sharing and interoperability being the major ones. Similarly AI – powered devices come with a range of challenges, particularly on the fault front. The real dilemma associated with autonomous cars is – who is liable for damages resulting from accidents- maker or machine. Of course, suggestions have been put forth as to how liability of robots can be determined. These range from strict-liability approach (no fault required) to risk management approach (liability of a person who was able to minimize the risks). The legal community is also largely unanimous that liability of robots should be proportionate to the actual level of instructions given to the robot and its degree of autonomy. However, the crux of the issue with A1–powered devices is that as increasingly the decisions that they take become more and more removed from any direct programming and are in turn based more on machine learning principles, it becomes harder to attribute the question of fault.

Herein lies the importance of AI governance – the goal of which is to minimize potential risks from bias and maximize intended benefits. In particular, the legal framework must ensure that AI is

a. fair and impartial
b. transparent and explainable
c. responsible and accountable
d. safe and secure
e. compliant with data and privacy regulations as well as
f. robust and reliable.

In the Indian context, the focus must be on attuning the legal system to the pillars of AI governance (VIZ) AI IP and innovation, AI compute and systems, Skilling in AI, Data for AI and AI ethics. One must be all the more careful about generative AI which can introduce falsehoods into the copy it produces and bias into the text it generates. Needless to say, deep fakes form a big source

of concern. They are the manipulations of facial appearance through deep generative methods. As they leverage powerful techniques from machine learning & AI to manipulate or generate visual and audio content that can easily deceive, dealing with the legal challenges posed by them is easier said than done.

Internet and robotics are not the only innovations where growth of technology brings forth legal puzzles. Another oft quoted example is 3D printing. First, it has serious security repercussions as it enables individuals- including terrorists -to manufacture any weapon comfortably. In fact, 3D printed guns have already been manufactured in US, Japan and Australia.[i] Second, it has significant tax implications. Since product sold (CAD) is in the form of a digital file, it will not be subject to customs duties imposed on physical products. Third, 3D printing may increase the incidence of patent infringement. Consumer will merely need to procure digital file containing instructions for the 3D printer (CAD) and can make infringing copies at home. Fourth, issues of standards and interoperability will come into play here as well.

IoT also raises legal as well as ethical challenges. The first major issue is data security. As smart devices are always connected to the internet for information and system updates, there is a possibility of the devices being hacked. Second, continuous connection to the internet increases the risk of a spontaneous machine malfunction which in case of machines such as household heating can cause physical danger to the user. Third, without sufficient data protection measures, consumer privacy is vulnerable to violation. The devices have access to sensitive information such as present location, preferences and personal information of the user through the connected mobile devices. In the case of some manufacturers, data processing for the equipment is not conducted directly by the manufacturer or a subsidiary. It is in fact outsourced to a third party who may not adhere to the privacy policy sworn by the manufacturer. This leads to the risk of third party infiltration. Fourth, IoT suffers from standardization issues. At present IoT developers are using varied standards. Lack of standards contributes to data insecurity and privacy susceptibility. Fifth, spectrum policy of various countries and ITU will have to accommodate IOT.

Even an innovation like telemedicine raises myriad legal questions. This is all the more relevant, given the fact that medical platforms have witnessed a massive rise since the beginning of the COVID-19 pandemic. The Telemedicine Practice Guidelines were brought forth to bring clarity and certainty in the field. Though these guidelines delineate the liability of platforms with respect to obligations like privacy and due diligence with precision, one major avenue left out is

negligence of doctors on a particular platform. Doctors can face individual sanctions from Medical Councils, but whether there can exist an additional liability on the platform is unclear. This lack of clarity is to be viewed in the backdrop of tort law where Courts have modified the standard test of employer-employee relationship for vicarious liability and hold commercial hospitals vicariously liable for all negligence of their doctors. At the other end of the spectrum is intermediary liability wherein plain application of law results in no liability for any medical platform. All of this is further exacerbated by the sheer variations in business models. While certain platforms like Cure Mantra only provide online appointments and some such as Just Doc and Medimetry provide only online consultations, the majority of platforms (such as M Fine, Zoylo, Img and Practo) provide both online consultation and doorstep medicine delivery. There are also comprehensive care platforms like Bajaj Finserv Health that provide packages to users. Aside from these standard business models, there are creative ones too - a classic example being Lybrate that also provides a forum where doctors can answer user queries. Needless to say, such platforms represent trickier questions when addressing their liability.

In fact, all sharing economies (viz) peer-to-peer based activities of obtaining, giving or sharing access to goods and services pose legal challenges. Fixing of liability in such cases is complicated by their multiparty model. For example, ride- hailing service Uber claims no accountability for behavior of drivers as it is merely an aggregator of taxis. This applies not only to tort but also to criminal liability cases. Again, sharing economies are forcing regulators to re look at licensing and business regulations. This is to be viewed in the light of Airbnb and Uber being able to bypass regulations -ranging from safety restrictions and zoning requirements to tax laws- due to their asset- light business models.

Online entertainment services (Over the top (OTT) Video Streaming services) too come with their bag of legal challenges. The first and foremost in this regard is net neutrality. OTT video streaming is sensitive to the distance from the subscriber as seamless delivery of videos requires higher bandwidth. Therefore such service providers enter into agreements with the ISPs for dedicated channel for their content. This induces ISPs to discriminate between various types of contents delivered by them violating the net neutrality principle. Second, data security and privacy are inextricably involved with these services due to large amount of data collected by the service providers. Third, OTT service providers are not subject to regulatory regimes that apply to operators like Idea, Airtel and Vodafone.

E - payment systems also bring forth challenges in the legal arena. Since e- payment involves

exchange of sensitive information (debit /credit card numbers, banking details, passwords etc.), data security is very crucial for protection of consumer privacy and prevention of theft or fraud. Second authentication is a major concern. Third, determining the relevant law that parties will be governed by in respect of electronic transactions may create problems, especially when the laws in Country A (where the company is registered) permit e-payment contracts whereas those in Country B (where the consumer is located) do not support such contracts. Fourth, legal recognition of digital currencies is a matter of concern given the fact that cryptocurrencies like bitcoin are not recognized in most jurisdictions. Though efforts have been made by the RBI to solve these risks – the recent push for card – on – file tokenisation vide the circular dated January 8, 2019 and the issuance of the Guidelines on Regulation of Payment Aggregators and Payment Gateways on March 17, 2020 being classic examples – they offer only suboptimal methods to solve such risks and do not meaningfully engage with the privacy related dimensions of financial data protection.

Cloud computing is another technological development that raises legal concerns. First, it entails storing of large amounts of data and therefore is automatically subject to data privacy and security concerns. Second, data ownership is a significant question. In the absence of a clear contract, the host can claim ownership over data even after termination of service. Third, extent of liability of the host for any data misuse or breach is a contentious topic. In cases where the client does not have bargaining power or the contract is not negotiable, the host can escape liability completely. Fourth, compliance of regulations related to tax, data protection, damages under contract etc. can be difficult due to absence of onshore facility. These concerns are over and above legal concerns resulting from the current data economy – which range from data protection and data localization to taxation of data flows and jurisdiction applicable to them.

All these legal complexities point out the need for law to ensure level playing field – not only for infrastructure development for the internet and its use, but also for the operation of e-commerce components. Appropriate laws are needed to ensure that the big players (Google, Apple, Facebook, Amazon, Uber, Twitter, Alibaba etc.) do not abuse their market position and that entry barriers for new and small entrants are minimized. A word of caution is however needed here: while some issues need exclusive legal intention, others are better resolved through alternate approaches. So far globally three types of regulatory approaches can be observed - complete freedom (like US), no freedom (like Russia & China) and limited freedom (like EU) for digital business. Which approach must be embarked depends on the current economic and technological structure, nay its

rapidly changing nature.

But the other side of the fence is also equally important. Technology can be transformed into an instrument to assist the enforcement of law.

With the advent of big data analytics, machine learning and artificial intelligence (AI), the fundamental questions of law enforcement and justice are being reconsidered across the globe. Law is based on two important aspects – predictability and precedence and many are of the opinion that AI can greatly help align these processes. While disagreements are galore as to whether these technologies represent a panacea or whether they will further exacerbate social divisions and endanger fundamental liberties, the two camps agree that the new technologies usher in important consequences. In fact, there are three main ways in which technology is already reshaping the judicial system. First and at the most basic level, technology is assisting to inform, support and advise people involved in the justice system (supportive technology). Second, technology can replace functions and activities that were previously carried out by humans (replacement technology) – the concept of online courts being a classic example. Finally, at a third level, technology can change the way that judges work and provide for very different forms of justice (disruptive technology), particularly where processes change significantly and predictive analytics may reshape the adjudicative role. It is at these second and third levels that issues emerge in terms of the impact of technology on the role and function of a judge. Questions raised in this context include

a) Can AI enabled programmes extract the accurate position of law from a mass of precedents?
b) Can robots decide questions of law?
c) Who should be accountable for semi- automated decisions?
d) How should responsibility be allocated within the chain of actors when the final decision is facilitated by the use of AI?
e) Is the "due process of law" denied to the accused when AI systems are used at some stage of the criminal procedure?
f) Can judgements be replaced by data?

These questions are all the more relevant now that AI has made a lot of inroads within justice systems – in Estonia for adjudicating small claims (robot judges), in China, Russia and Mexico for giving legal advice/approving pensions, in Malaysia towards supporting sentencing decisions,

in Austria for sophisticated document management, in Colombia and Argentina for identifying urgent cases within minutes, in Abu Dhabi for predicting probability of settlement and in Singapore for transcribing court hearings in real time- to name a few.

Justice delivery is not the only domain wherein technology is ushering in transformation in the legal arena. Examples in this regard are galore from the spectrum of cyber law- a classic one being end-to-end encrypted (E2 EE) messaging. This form of cryptography allows messages only to be read by senders and their intended recipients. Content shared by users over E2EE channels is inaccessible even to service providers. The main advantage of E2EE is that it can provide individuals with a zone of privacy. But technology comes in here in the context of traceability – in the Indian context in the backdrop of Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. The said rule mandates popular messaging services to facilitate identification of the 'first originator' of any message that is sent through their platforms in response to a court or government order. Implementation of this rule brings forth technological challenges as to how the 'traceability' mandate can be implemented without serious costs to usability, security and privacy.

One among the suggested solutions is storing 'hashes' of all messages. Hashing, it must be mentioned here, is a mathematical operation that converts any piece of information into a unique string of characters. It is computationally infeasible to retrieve the original piece of information from its hash. Service providers will retain the hash of each transmitted message on their servers. In the event of a lawful request to find the originator of a particular message, service providers can compute the hash of that message and compare it to all preciously recorded hashes. This will help them identify the originators of the message.

Another suggested method involves attaching originator information to messages. A submission by Dr. Kamakoti to the Madras High Court described a proposal that service providers could modify their application to attach an additional piece of metadata to messages in the form of information about the originator of a message. Originator information refers to any identifier that can help track down an individual, such as a phone number or device identifier such as IMEI number assigned to cellular phones. This information will travel along with the message as it is forwarded and can subsequently be used to identify the originator.

Technology – law interface comes in when weighing the viability and ease of circumvention of

these alternatives vis-à-vis their limitations which may range from weak attribution and weak identification to geo fencing limitations.

No discussion on law – technology interface will be complete without a reference to copy right law which has exhibited a rather ambivalent attitude and which shares a dialectic relation with technology. In fact, technology challenges copyright law and law tends to react initially by fighting and subsequently by encompassing new ways of exploiting copyrighted works developed by the new technologies, when necessary through reform of law. It triggers a cycle whereby technology enables new practices which are not encompassed within the law but are not excluded by law. On the other hand, law shapes technology by influencing emergence of certain new technologies as well as their design and architecture.

A classic trigger in the recent context is when internet morphed into the World Wide Web 2.0, by reason of availability of broadband connection (mostly wireless) and software programs that enable creation and editing of digital content. But the challenge started much earlier – first with the invention of reprographic technology (photocopier etc.) and later with the arrival of video recorder which was accused of heralding the end of US film industry. In the 1980s, the Hollywood majors united in a campaign against Sony, the corporation that produced and commercialized Betamax technology – which enabled viewers at their own leisure to record onto videotape TV programmes. The challenge was that this permitted copyright infringement. This led to the Sony – Betamax decision in 1984 which set criteria to assess innovative technology in relation to copyright law. Beyond the introduction of the fair use of time – shifting and the reaffirmation of the private copy, the importance of this decision lies in the fact that it is one of a long series of battles between copyright law and technology. It demonstrates how a technology that initially seemed threatening may be transformed into an economic resource for right holders. It spells out that exclusive rights are not granted to block social progress but to promote development of society.

When digital technology met the internet, however, this mechanism became jammed. It generated first, a line of cases that turned the Sony - Betamax principle upside down (from Napster to Grokster), second the adoption of legal provisions (well known legislative responses to the challenges that internet posed to copyright law) and third the spread of DRM systems.

The need of the hour is to understand the state of technology today, its linkage with law and

challenges posed by law – technology interface. What is needed is an analysis in the backdrop of the fact that inherent natures of legal systems and present technology-driven businesses, nay society, are diametrically opposite. To be more specific, laws and regulations are tailored to be stable whereas current technologically driven global environment is in a constant flux. Addressing this dichotomy that has added to the uncertainty wrought by technological revolution is the need of the hour.

To put in simple terms, the road ahead will be a three-fold approach:

a) Creating a legal system which accounts for continually mutating technology.
b) Establishing an equitable ecosystem and ensuring a level playing field.
c) Identifying issues that need extensive legal intervention and sieving out those that are better resolved through alternate approaches.

Only then can a set of frameworks, policies and best practices which ensure that frontier technologies are used in an ethical and responsible way evolve, giving mankind the much needed respite from their evil effects, at the same time yielding the best possible benefits therefrom in a timely fashion. The option before the comity of nations and its denizens, nay netizens is amply clear.

[i] Andy Greenberg, How 3-D printer Guns Evolved into serious weapons in just One year, Wired, 15 May 2014 available at https://www.wired.com/2014/05/3d-printed-guns/.