ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

A CRITICAL ANALYSIS ON CYBER SECURITY AND MOBILE LAWS

AUTHORED BY: BERTILA. A
DESIGNATION: POST GRADUATE STUDENT
INSTITUTION: THE TAMIL NADU Dr. AMBEDKAR LAW UNIVERSITY
SCHOOL OF EXCELLENCE IN LAW, CHENNAI
ADDRESS: NO. 39, MOHANAPURI 2ND STREET, ADAMBAKKAM, CHENNAI 600088
EMAIL: bertilaraj13@gmail.com
CONTACT DETAILS: 9840960006, 9840960001

INTRODUCTION

The current social lifestyle thrives on information technology. A mobile phone always acts as the mini storage and as access to information even when a person is away from his computer, books and libraries or other sources of information. Application wise a mobile is also a very handy tool to wield, there are innumerable applications loaded in the machine beginning from date and time to weather report to GPS systems et al. Until these information system is applied at the right place for the right purpose, mobile is the most advantageous technology at the hands of a man. But, if these information are used undesirably and for cross purposes, they might turn out to be great menaces to the society. In the role of a safety device a mobile is a savior since it can reach the emergency services or the closed ones in no time but, accidents caused due to mobiles also show that cell phones can contribute to unsafe incidents as well.

The law regulating mobile devices, their use, and their adoption is known as "Mobile Law" in basic terms. "Mobile Law" refers to the newly developed legal field and law that affects, relates to, is connected to, or has a relating to convoluted legal difficulties with mobile devices, any type of communication gadget, mobile networks, all data, mobile platforms, laptops and mobile devices, and information that is hosted, whether digitally or otherwise any way, whether generated, sent, received, or transmitted, employing the aforesaid mobile platforms and devices. The rapidly expanding field of mobile law includes, within its purview, complicated legal issues and difficulties that would affect any device, computer, computer system, computer

ISSN: 2582-6433

network, computer resources, as well as data or information in electronic form, within the mobile ecosystem. As the world moves toward more mobile device penetration, adoption, and usage, mobile law has the potential to grow significantly as a legal field.

The question, Do we need mobile laws?

The answer is unequivocally Yes, because this industry represents a new chapter in our life. Mobile phones are more than just communication gadgets. These are extremely powerful computing devices. The device that rules our world indistinctively, the device that aid us from sunrise to sunset and much more powerful than the the computers that were used by NASA to send man to moon. When a new technology emerges there rises a need for specific laws governing it in entirety.

The new law of the future decade is mobile law. Various sophisticated and complex legal concerns will continue to appear in this field of study. These issues will include not only the production, manufacture, sale, marketing, distribution, and related activities pertaining to mobile handsets and mobile devices as well as mobile platforms, but also all issues pertaining to data and information in electronic form that is resident on these mobile devices or is transmitted, sent or received, preserved or retained in the said Mobile devices and mobile platforms.

Mobile Law as a Legal discipline is applicable all throughout the world. Different countries have implemented various rules, regulations, and notifications, as well as laws, all of which have an impact on legal concerns with mobile phones. The majority of these laws are written in an indirect manner. There are very few direct laws governing mobile law. With the increased use of mobile phones in India, the government moved to update the Information Technology Act of 2000. The Information Technology (Amendment) Act of 2008 will put these additional amendments into force. These changes have resulted in the transformation of India's Cyberlaw into India's Mobile Law.

The Information Technology Act of 2000, with subsequent revisions, attempted to cover communication devices, but this was simply the first step. This paper discusses the need for Mobile Laws in today’s scenario, what needs to be done to make this rule truly applicable in the context of mobile apps and their misuse, as well as data collection.

ISSN: 2582-6433

History of Mobile Telephony: Indian Law Enforcement Perspective

In India alone, there are 2.364 million mobile phone subscribers which are growing at a rapid pace. While mobile phones outsell personal computers three to one, mobile phone forensics still lags behind computer. Data acquired from mobile phones continues to be used as evidence in criminal, civil and even high profile cases. However, validated frameworks and techniques to acquire mobile phone data are virtually non-existent.

The Need for Mobile Phone

The following section of the paper will discuss the need for mobile forensics by highlighting the following:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions.
- Law enforcement, criminals and mobile phone devices.

DIFFERENT MOBILE GENERATIONS

1st generation – Analog system
2nd generation – TDMA (Time Division Multiple Access)
3rd generation – GSM 1800 MHz (Global System for Mobile Communications)
4th generation – UMTs 1900 MHz (Universal Mobile Telephone System)

IMPACT OF SMARTPHONES

As the smartphone market grows, there is a corresponding significant growth in mobile applications and online services; driven by both the Government and private players. With rise in smartphone users, there is vast potential to leverage this reach for social and economic development. Mobile apps and web portals as the primary form of service delivery can lead to more efficient process, transparent workings, ease of access to services, citizen participation and inclusion. Recognizing this, the Government has made numerous attempts to cater to the growing demand for digital and mobile friendly services.

COVID 19: ROLE OF SMARTPHONES

Amidst the global Corona pandemic, smartphones have emerged as a multipurpose tool for the government in various ways. By leveraging key features of open ecosystem such as low development time, cost-effectiveness and customization, many state governments have

ISSN: 2582-6433

developed their own apps for a range of services. Owing to open OS's such as Android, the current administration was able to promptly take action and develop apps that would aid various departments in carrying out COVID-19 related functions. This has resulted in over 60 COVID-19 related apps in the Play Store. To prevent the rapid spread of the Corona virus, countries such as India imposed a nation-wide lockdown.

Thus, as the world moves to digital platforms in these physically restrictive times, the role of smartphones is expected to grow in importance and adoption. This may have a cascading and sustainable effect on key sectors such and Education, Health, Finance, etc. With the country in lockdown, citizens are gradually recognizing the value of accessing public services online, through mobile devices. Owing to Google;s efforts to ensure Android compatibility through the AFA/ ACC, smartphones are now one of the Indian government's primary contact tracing tools to battle the coronavirus epidemic. By keeping the public well informed on the ‚do's and donts', well-coordinated steps can be taken to overcome this pandemic. The government has also urged people to come forward and share technology-driven solutions for COVID-19 to arrest its growth. Smartphones are crucial for the government's focus on technology led governance.

AROGYA SETU

- Arogya Setu is an app which is available in 12 Indian languages, with over 9.78 crore users.
- This app is used to monitor the proximity of COVID-19 positive patients within a specified radius. This allows users to distance themselves from active patients and keeps the government updated on corona hotspots and patient symptoms.

WOMEN'S MOBILE-RELATED SAFETY CONCERNS

Mobile has the capacity to transform lives. It can empower women, make them more connected and provide access to information, services and life-enhancing opportunities like health information, financial services and employment opportunities, often for the first time. Mobile is also the main access point to the internet for most of the world's population, especially in low- and middle-income countries. However, while mobile connectivity is spreading quickly, it is not spreading equally. Women are being left behind as various, interconnected barriers keep them from accessing and using mobile at the same rate as men. This unequal access to mobile technology threatens to exacerbate the inequalities women already experience. At the

ISSN: 2582-6433

same time, there is a paradoxical relationship between mobile technology and women's safety. A 2015 GSMA[1] Connected Women survey found that 68% to 94% of female respondents in 11 low and middle-income countries reported feeling safer with a mobile phone or that they would feel safer if they owned one. Among other things, a mobile can provide a way for a woman to contact help if she is in trouble and reassurance when she is out and about. However, research has consistently shown that safety concerns related to mobile are an important barrier to mobile ownership and use, with women perceiving safety as an issue more commonly than men. Mobiles have become conduits for threats that have always existed as well as new ones. Mobile-related safety concerns are wide ranging and include Safety concerns, and a general perception that mobile or internet access and use pose threats, should not however be used as an excuse for denying women access. Rather, their ability to empower women should be emphasised, including the ways in which mobile ownership and access to services can enhance women's personal safety. This report explores women's mobile-related safety concerns, building on previous research by the GSMA and other organisations. It draws on over 30 stakeholder interviews, desk research and primary research in India.

THREE TYPES

1. PHYSICAL WORLD: Threats experienced in the physical world as a result of owning or using a mobile.
2. VOICE AND SMS: Threats experienced via voice calls or SMS.
3. ONLINE: Threats experienced via mobile internet.

CATEGORISATION OF MOBILE-RELATED SAFETY CONCERNS

PHYSICAL WORLD

- Threats experienced in the physical world as a result of owning or using a mobile
- Risk of phone theft
- Harassment when visiting points of sale and subsequent misuse of women's mobile numbers after they share them to top up
- Societal disapproval or harassment as a result of using mobile in public
- Domestic violence triggered by using mobiles at home

[1] GSMA Connected Women, 2015, "Bridging the gender gap: Mobile access and usage in low- and middle income countries", https://www.gsma.com/ mobilefordevelopment/wp-content/uploads/2016/02/ConnectedWomen-Gender-Gap.pdf

ISSN: 2582-6433

VOICE AND SMS

- Threats experienced via voice calls and SMS
- Unwanted calls or messages
- Sexually harassing calls or messages
- Threatening calls or messages
- Scam calls and messages
- Unwanted and harassing marketing calls and messages.

ONLINE

- experienced via mobile internet
- Threats Online/social media harassment or bullying
- Online stalking or use of spyware
- isuse of personal data or images
- Identify theft
- Fraud
- Online scams / viruses
- Exposure to content deemed explicit or inappropriate.

THE CYBER LAW TRENDS AND DEVELOPMENTS OF INDIA

CYBER CRIMES PREVENTION STRATEGY:

Cyber crimes have increased significantly in India in recent years. In response, the Indian government has decided to develop a cybercrime prevention strategy for India. However, the proposed strategy has yet to be developed.

CYBER CRIMES INVESTIGATION TRAINING:

With an increase in cybercrime in India, it was felt that law enforcement agencies in India needed cybercrime investigation training. India must improve its cybercrime investigation capabilities in order to effectively combat cybercrime. Similarly, the modernization of India's police force is urgently required, with a special emphasis on the development of techno-legal skills for them.

ISSN: 2582-6433

ENCRYPTION LAW:

Almost six years ago, the Standing Committee on Information Technology (SCIT) drew the Department of Telecommunications (DOT) over encryption concerns. India's encryption laws and regulations require clarification. The legal risks for website development companies in India would also rise as a result of improper encryption for such websites. A dedicated encryption policy and a techno-legal encryption law in India are urgently required.

BANK ATMS HAVE BEEN COMPROMISED:

On October 20, 2016, it was reported that approximately 3.2 million bank customers' debit cards had been compromised. SBI, HDFC Bank, ICICI, YES Bank, and Axis Bank were among the hardest hit. Banks in India will either replace or request that users change security codes for over 3.2 million debit cards.

E-MAIL POLICY:

Despite repeated warnings from the Delhi High Court, India's e-mail policy has yet to be implemented. The situation is so bad that the Delhi High Court has accused the central government of sitting over India's e-mail policy. The Delhi High Court has also directed the Central Government to issue an electronic signature notification under the Information Technology Act of 2000. India's encryption policy is also lacking, despite the fact that it is urgently needed. However, Madhya Pradesh has legalised email communications between government departments.

ONLINE PAYMENTS:

Over the last decade, India has seen an increase in online and mobile payments. However, various mobile payment providers in India did not take legal and regulatory issues seriously. There are numerous legal issues of e-commerce in India, to which various online payment service providers in India must adhere. In India, it has already specified the cyber law due diligence requirements for PayPal and online payment transferors. Similarly, we have outlined the e-commerce and online business legal compliances for the Indian online payment market.

MOBILE CELL PHONES AND CYBER CRIMES IN INDIA

Telecommunication was first introduced in India in 1882. Following the introduction of the internet and mobile technology in India, telecommunications grew like a weed. On August 15, 1995, India saw the launch of its first non-commercial mobile phone service. The internet was

ISSN: 2582-6433

also introduced in this country on the same day. After the liberation and privatisation of this sector, India did not look back; telecommunications conquered the lives of Indian citizens, and India's telecommunication network quickly became the world's second largest. In May 2019, India had 1909.17 million mobile users. A person is looked at with surprise in this dot-com era if he is not a mobile user.

CYBER CRIMES ASSOCIATED WITH CELL PHONES

BLUE BUGGING:

As the name implies, this is a Bluetooth-based attack on mobile phones. Bluetooth is a common term these days. Bluetooth technology is built into almost every mobile phone. We use Bluetooth to share photos, audio and video files, and so on. Blue bugging enables a hacker to gain complete control of your mobile phone. When you receive a call on your infected mobile phone, the call is forwarded to the hacker, who can listen in on the conversation. Blue snarfing allows a hacker to steal all of the data and information on your mobile phone using his laptop.

VISHING:

This is a mobile tool for committing financial crime. The use of mobile making on mobile phones is increasing. Mobile phones are now used to conduct online shopping and banking transactions. This has made mobile phones an easy target for Vishing. The hacker's motivation is to make quick money. These attacks resemble phishing attacks.

MALWARE:

This is one of the most serious threats to mobile phones. It is a programme (software) designed to carry out malicious activities on the infected device. Malware infiltrates the victim's mobile phone via SMS, file transfer, downloading programmes from the internet, and so on. Malware enters and functions in the victim's mobile device without his knowledge, performing a variety of malicious activities such as the use of talktime.

SMISHING:

The term "SMS" needs no introduction in this day and age. It stands for Short Message Service. It is a common term for text messaging on a mobile phone. This is one of the most popular mobile phone services. As a result, criminals are using it as a tool to satisfy their greed. Smishing is a type of security attack in which the user receives an SMS posing as a lucrative service, luring them into revealing personal information that is later misused. This is also used to install malware on the user's cell phone.

ISSN: 2582-6433

INDIA'S DATA PROTECTION LAWS

The right to privacy has been recognised by Indian courts, including the Supreme Court of India, as an integral part of the right to life and personal liberty, which is a fundamental right guaranteed to every individual under the Indian Constitution. As a result, the Indian judiciary has prioritised the right to privacy, which can only be limited for compelling reasons such as state security and public interest.

LEGAL FRAMEWORK:

MOBILE CELL PHONES AND THE INFORMATION TECHNOLOGY ACT, 2000[2]

Personal liability is created by the section for illegal or unauthorised use of computers, computer systems, and data stored on them. However, the section does not address the liability of internet service providers, network service providers, or entities handling data. As a result, this section does not apply to entities responsible for the safe distribution and processing of data, such as vendors and outsourcing service providers. Section 79 further dilutes the entities' liability by requiring "knowledge" and "best efforts" before determining the quantum of penalties.

This means that if the network service provider or an outsourcing service provider proves that the offence or contravention was committed without his knowledge, or that he exercised all due diligence to prevent the commission of such offence or contravention, he will not be held liable. It should be noted that if a company is accused of violating the IT Act, its key employees are personally liable for any intentional or negligent act that results in a violation of the IT Act.

SECTION 2(I)[3]:

According to the IT Act, mobile phones are included in the definition of a computer. Mobile phones have been used for information exchange.

SECTION 2(R)[4]:

According to the IT Act, "electronic form" refers to information that is generated, sent, received, or stored in media such as magnetic, optical, computer memory, micro film, computer generated micro fiche, or similar device.

SECTION 43 (A), (B), AND (I):

[2] Information Technology Act, 2000
[3] Sec 2 (I) Information Technology Act, 2000
[4] Sec 2 (R) Information Technology Act, 2000

ISSN: 2582-6433

This section states that any person who operates a computer, computer system, or computer network without the permission of the owner or any other person who may be in charge of the computer, computer system, or computer network.

• Gains or maintains access to such computer, computer system, or computer network

• Downloads, copies, or extracts any data, computer data base, or information from such computer, computer system, or computer network, including any information or data held or stored in any removable storage medium.

• Any person who steals, conceals, destroys, or alters, or causes another person to steal, conceal, destroy, or alter any computer source code used for a computer resource with the intent to cause damage, shall be liable for damages.

SECTION 43A[5]:

This section is the bedrock of data protection, and it states that if a body corporate is negligent in implementing and maintaining reasonable security practises and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages in the form of compensation.

SECTION 66A[6]:

The IT Act establishes penalties for sending offensive messages via communication services, among other things.

SECTION 66 C[7]:

This section deals with identity theft and states that anyone who fraudulently or dishonestly uses another person's electronic signature, password, or any other unique identification feature shall face imprisonment for a term of up to three years, as well as a fine.

SECTION 66 E[8]:

This section states that anyone who intentionally or knowingly captures, publishes, or transmits an image of a private area of another person without his or her consent, in circumstances that violate that person's privacy, faces up to three years in prison or a fine.

[5] Sec 43(A) Information Technology Act, 2000
[6] Sec 66(A) Information Technology Act, 2000
[7] Sec 66(C) Information Technology Act, 2000
[8] Sec 66(E) Information Technology Act, 2000

ISSN: 2582-6433

SECTION 67[9]:

Establishes penalties for publishing or transmitting obscene material in electronic form. Whoever publishes, transmits, or causes to be published or transmitted in electronic form any material that is lascivious or appeals to the prurient interest, or whose effect is such that it tends to deprave and corrupt persons who are likely, taking all relevant circumstances into account, to read, see, or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term that may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

SECTION 67(A)[10]:

Penalty for publishing or transmitting in electronic form material containing sexually explicit acts, etc. This is especially important for teenagers. The sharing of pornographic material on cell phones is becoming more popular. Nobody is unaware of the occurrence of indecent MMS. This law punishes anyone who publishes, transmits, or causes to be published or transmitted in electronic form any material containing sexually explicit acts or conduct.

SECTION 72[11]:

States that any person who obtains access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned and then discloses such electronic record, book, register, correspondence, information, document, or other material to any other person violates this section.

INDIAN PENAL CODE, 1860

The Indian penal code makes no mention of data privacy violations. Liability for such violations must be inferred from related crimes under the Indian Penal Code. Section 403 of the Indian Penal Code, for example, imposes a criminal penalty for the dishonest misappropriation or conversion of "movable property" for one's own use.

[9] Sec 67 Information Technology Act, 2000
[10] Sec 67(A) Information Technology Act, 2000
[11] Sec 72 Information Technology Act, 2000

ISSN: 2582-6433

SECTIONS 294, 504, 506, 507, AND 509

The only difference is that the criminal in these sections uses his cell phone or computer to express his offensive feelings. The punishment prescribed by this section is imprisonment for a term of up to three years and a fine. This section includes an explanation that states that the terms electronic mail and electronic mail message refer to a message or information created, transmitted, or received on a computer, computer system, computer resource, or communication device, including attachments in text, image, audio, video, and any other electronic record that may be transmitted with the message. This explanation broadens the scope of this section and ensures that the criminal is held accountable.

NEED FOR A MOBILE LAWS

The new legislation of the future decade is mobile law. Various sophisticated and complex legal concerns will continue to appear in this field of study.

These issues will include not only the production, manufacture, sale, marketing, distribution, and related activities pertaining to mobile handsets and mobile devices, but also all issues pertaining to data and information in electronic form that is resident on these mobile devices or is transmitted, sent or received, preserved or retained in the said Mobile devices and mobile platforms.

As a legal discipline, mobile law is applicable all over the world. Different governments have implemented various rules, regulations, and announcements, as well as legislation that have an impact on legal concerns relating to mobiles The majority of these laws are written in an indirect manner. There are very few direct laws relating to mobile law.

MOBILE LAWS AROUND THE WORLD

- Driving While Using a Cell Phone

The United Kingdom has a restriction on cell phone use while driving, which began as a fine but has since progressed to inflicting points on your driving record. The penalty are $250 for chatting on a cell phone while driving and $100 for texting.

- Gaming on Cell Phones

Many nations have banned cell phone gaming given the fact that online gambling is illegal and that there would be potential for online gambling through mobile broadband. The issue continues to be debated around the world.

ISSN: 2582-6433

- Camera Phone Regulations

The Video Voyeurism Prevention Act of 2004 in the United States prohibits people from taking naked pictures of anyone else with their cell phone camera unless they have obtained consent (and the person is of legal age to give that consent).

- Mobile devices in Schools

Most nations don't have laws governing this, but there is much discussion arguing that there should be placed in place to permit these children to possess their phones but forbidding their use to disturb class time.

- How to Avoid Cell Phone Spam

Spam on cell phones has been on the rise and has become a big issue, prompting governments throughout the world to pass anti-spam legislation requiring those delivering cell phone commercial messages to include a "opt out" option. Cell phone spam should be prohibited, according to Singapore.

CONCLUSION

The new law of the future decade is mobile law. Various sophisticated and complex legal concerns will continue to appear in this field of study. These issues will include not only the production, manufacture, sale, marketing, distribution, and related activities pertaining to mobile handsets and mobile devices as well as mobile platforms, but also all issues pertaining to data and information in electronic form that is resident on these mobile devices or is transmitted, sent or received, preserved or retained in the said Mobile devices and mobile platforms.

The government should start campaigns in promoting literacy about cyber world and cyber crime specifically to make the people more aware about the use and misuse. It is further recommended that cyber illiteracy should start from grassroots level; institutes, computer centers, schools & individuals.