UNIQUE LEGAL

THE MAGAZINE FOR CYBER TECH
JULY 2021

"A data breach is about both privacy and security. And security becomes very, very important because you can't have privacy unless you have good security. And if someone tries to say otherwise, they are crazy people!"

Pegasus spyware: Making allegation is not enough, proof of surveillance is needed.

UNIQUE LEGAL

Editorial Board

UNIQUE LEGAL

TABLE OF CONTENT

ALL ABOUT UNIQUE LEGAL

Behind every start-up to be successful it is important to verify the needs of the targeted audience and then the solution which fulfils the need. It is important that the need which we are fulfilling and the idea is not being copied by anybody else.

So, the basic need is to equip the future generation of law students, young advocates and common people who want to seek legal education and increase their legal acumen.

One thing in this world is constant and that is change. Change in the only constant. In this era where people have become smarter and technologically advanced, there has been changes taking place whether it's lifestyle, education, culture etc. With these changes in mind as well as "Start-up India" it's our objective to better equip and build a strong background for the future generation of law aspirants, students, legal professionals. Our aim is to make the upcoming generation more versatile and professional.

Problem: Weak legal base/knowledge of students resulting to their academic performance. The youth of our nation who are opting to get admission in law school are not aware about how to conduct legal research activities and somewhere lack in developing their skills. The students in law school go through a lot of pressure because memorizing the laws with different cases is very difficult and it happens with a good percentage of students who aren't able to do so. Once the students don't pay attention to what is taught in the class, they make last day project and assignments assigned by college, become an introvert and it weakens their communication skills. The students from the start of college should start making a strong base of law otherwise it will affect their academics.

Problem: Theoretical law is different from the application of law which means once a law student graduates and is ready to practice law, they see that what they have studied is totally different when it comes to practice.

Problem: Law students, young advocates, legal professionals lack in legal research and writing. They don't exactly know how to conduct a healthy legal research. A healthy research includes a research question which is being administered. Instead of this they use internet sources and look for readymade research papers, material, definitions.

Problem: Each and every citizen is not aware about their rights and duties leading to lack in legal education and then breaking of the law. The law abiding citizen should obey the supreme law of the land and don't do any such activities which will hamper their well-being.

Problem: In the field of law, we believe the students should be provided with consultation services so that they can have a clear idea before entering the law school and after entering how to perform in academics and other aspects related to skill development. There are no firms, institutes who provide consultation to law students from different parts of the world.

Need: Law is a very important subject and every citizen should be aware of the laws which include certain rights and duties which should be followed by the common people. People who don't have a legal background should also be keen to know about the different and important laws related to the urgency of the situation, only then they can understand and act accordingly.

ELECTORAL BONDS

Electoral bonds are planned as conveyor instruments like Promissory notes that convey no data about the proprietor except for respect the holder or carrier of the bond. The subtleties of the contributor are not disclosed however are accessible just with the bank.

- **It can be bought by an Indian resident or a body incorporated in India.**
- **An ideological group (Political party) enlisted under RoPA, 1951 that gets something like one percent of votes surveyed in state races or Lok Sabha races will be allocated a record by the Election Commission of India, into which the bonds can be recovered inside 15 days of procurement.**
- **Donations made through these bonds are excluded from charges.**
- **The bonds will be given in products of Rs 1000, Rs 10,000, Rs 1 Lakh, Rs 10 Lakh and Rs 1 Crore and can be purchased by the giver with a KYC agreeable record.**
- **They can't be bought by paying money. The greatest sum that an ideological group can get as gift in real money is covered at Rs 2000. Appointive bonds in this way license them to raise higher totals. For what reason is Electoral bonds required**
- **They give a straightforward system to ideological groups to bring funds up in request to meet political race uses. Since the contributor purchases constituent bonds in the wake of outfitting KYC subtleties to the bank, it is a more straightforward device than cash.**
- **The ADR (Association for Democratic Rights) expresses that 69% of political financing in India comes from obscure sources. In this unique circumstance, Electoral securities give another, straightforward course for gatherings to raise reserves.**
- **It additionally safeguards secrecy of benefactors which is fundamental as they should be secured against any post-survey terrorizing or provocation by political rivals.**

Concerns raised against Electoral Bonds

- **RBI self-rule the public authority needed to revise RBI act to give these bonds as carrier bonds have the qualities of cash notes which are given exclusively by the national bank. The alteration anyway will add up to dividing of the notes giving force of the RBI especially when its self-rule is being addressed over its inferred acknowledgment of Demonetization.**

- **No Transparency: The bonds are not enlisted for the sake of a particular individual accordingly gifts through constituent bonds keep on giving secrecy to contributors.**
- **Could be utilized as channel for tax evasion and storing dark cash Since these bonds keep on giving secrecy to holders, they can be abused similar as the Indira Vikas Patras skimmed as advancement bonds in 1987 that fell into unsavoriness inferable from comparable reasons.**
- **These will likewise work with round stumbling that is rerouting of illegal assets that begin in India, back into the country through an assessment asylum. Here, it should be noticed that India positions at 19 in a rundown of 180 nations that figured in the Paradise paper releases that rattled off people and organizations that moved funds to seaward areas to dodge charges. Discretionary bonds offer mystery and will empower such tax avoidance.**
- **Anti-majority rule Law Commission in its 255th report brought up that mystery and obscurity give rich grounds to campaigning and catch of governments by large benefactors. Discretionary bonds consequently will be instruments that guarantee legislature of the trivial few.**
- **Non-divulgence to Election Commission While RoPA,1951 determines that gifts got by ideological groups in aggregates more noteworthy than Rs 20,000 be unveiled to the duty specialists, the Finance Bill,2017 unequivocally gives an exception from this statement to electing bonds. This damages the actual motivation behind tidying up appointive money.**
- **Not enough mystery: Another worry raised by ideological groups against discretionary bonds is that the occupant government can undoubtedly discover benefactor subtleties utilizing KYC subtleties imparted to banks. This could make the instruments disliked.**
- **Further the plan was presented through Finance bill,2017 and as such was not bantered in the upper house.**

What further changes are required in Indian Electoral Finance?

- **The cap of Rs 2000 for cash gifts gives a chance to stream of dark cash into decisions. This ought to be disposed of by and large. Political race Commission hosts recommended that gatherings be made to reveal commitments got in real money for more modest aggregates in the event that they surpass 20% of complete assets raised. This can be thought of.**
- **An meddling investigation of political race consumption caused by gatherings and up-and-comers is required to guarantee location of dark cash in the framework.**

- **To keep parties from mocking consumption standards, Election commission should allow higher use limit for competitors.**
- **A more limited mission period will restrict costs brought about by parties. Concurrent races ought to likewise be investigated for similar reasons.**
- **National Electoral Fund, as proposed by previous Chief Election Commissioner S.Y Quraishi, to which everything givers can contribute is another conceivable other option.**
- **To welcome all gatherings on a level battleground and to make private gifts less applicable, state subsidizing of decisions can likewise be investigated.**

Discretionary bonds are unique instrument acquainted in the country with tidy up the political framework. While they raise concerns, they are superior to cash and present more straightforwardness in discretionary money. The need is to combine them with different changes required in the discretionary framework to cut down the job of cash power in Indian legislative issues.

JUHI CHAWLA CASE ANALYSIS "THIS IS A CLASSIC TEXTBOOK CASE OF, HOW NOT TO DRAFT"

DISCLAIMER: The information contained in this observation is intended for educational purposes only and does not constitute legal opinion, legal advice or any advertisement. This is indicative and not directory. This is not intended to make any allegations or address the circumstances of any particular individual or corporate body. The content of the Delhi HC Order dated: 4th June, 2021 must be read and understood for the purposes of this observation, please do not amend or misuse the content. Any resemblance to any entity or person, living or dead, is purely coincidental.

DELHI HIGH COURT

Juhi Chawla and others v Science and Engineering Research Board and others

CS(OS) 262/2021 & I.A. Nos.6904/2021, 6906/2021, 6907/2021, 6908/2021

OBSERVATION OVER THE ORDER DATED 4th June 2021

CORUM: HON'BLE MR. JUSTICE J.R. MIDHA

"This is a classic textbook case of, how not to draft a plaint, which should be taught in law colleges and to young lawyers so that such bloopers in drafting of pleadings, damaging to one's own client, are avoided",

The High Court observed in the judgment:

Indeed, these perceptions were made by a seat of Justice Rajiv Sahai End law with respect to another case. A seat of Justice J R Midha, which considered Chawla's suit, said that these perceptions are completely relevant to her suit also.

No case for grant of leave to institute the suit is made out under Section 91(1)(b) of the Code of Civil Procedure or to sue in representative interest under Order I Rule 8 of the Code of Civil Procedure or to maintain the suit without the aforesaid leave/permission, as the plaintiffs' suit is defective and not maintainable for the following reasons: -

- **Order VI Rule 2(1) of the Code of Civil Procedure provides that the plaint shall contain statements of material facts in a concise form but no evidence by which they are to be proved. However, the plaintiffs have not complied with Order VI Rule 2 of the Code of Civil Procedure as**
- **The statement of plaintiffs is not in concise form and**
- **The plaintiffs have incorporated the evidence in the plaint.**
- **Order VI Rule 9 of the Code of Civil Procedure provides that the contents of any document shall not be set out in the plaint unless the precise words of the document or any part thereof are material. However, the plaintiffs CS(OS) 262/2021 Page 15 of 19 have not complied with Order VI Rule 9 of the Code of Civil Procedure and have reproduced the documents in the plaint.**
- **The plaint is stuffed with unnecessary scandalous, frivolous and vexatious averments which are liable to be struck down under Order VI Rule 16 of the Code of Civil Procedure.**
- **The plaintiffs have joined 33 defendants in this suit. However, the plaint does not reflect the compliance of Order I Rule 3 of the Code of Civil Procedure in joining 33 defendants in one suit.**
- **The plaintiffs have joined various causes of action without complying with Order II Rule 3 of the Code of Civil Procedure.**

- **The plaintiffs have not verified the plaint which is mandatory under Order VI Rule 15 of the Code of Civil Procedure.**

- **In the affidavit filed along with the plaint, the plaintiffs have deposed that only para 1 to 8 of the plaint are true to their knowledge whereas paras 1 to 169 of the plaint are based on information and legal advice, meaning thereby that the plaintiffs have no personal knowledge of any of the averments made in the plaint. The suit totally based upon information and legal advice is not maintainable.**
- **Since the plaintiffs have no personal knowledge of any averments made in the plaint and the whole plaint is based CS(OS) 262/2021 Page 16 of 19 on information and legal advice received, it appears that the plaintiffs want an inquiry to be conducted by this Court into the averments made in the plaint which is not permissible in law in these proceedings.**
- **Section 34 of the Specific Relief Act, 1963 deals with declaratory suits. A person entitled to any legal character can institute a suit against another person who denies or is interested to deny his right. In the present case, the plaintiffs never approached the defendants claiming any right and therefore, there was no occasion for the defendants to respond or deny to the plaintiffs alleged rights. In the matter, the maintainability of the declaratory reliefs sought by the plaintiffs is doubtful.**
- **Section 39 of the Specific Relief Act, 1963 deals with mandatory injunctions. The twin requirements of Section 39 are the existence of an obligation of the defendant towards the plaintiff and the breach thereof by the defendant. Both these requirements are not fulfilled the maintainability of the mandatory injunctions sought by the plaintiffs are, therefore, doubtful.**
- **The plaintiffs have not valued the suit properly for the purpose of Court-fees.**
- **The plaintiffs have not given the mandatory notice under Section 80(1) of the Code of Civil Procedure.**

The plaintiffs filed this suit on 28thMay, 2021 in which the Registry raised an objection to the maintainability of the suit. The plaintiffs, instead of explaining how the suit is maintainable, requested the Registry to list the suit as it is with defects and the plaintiffs undertook to bear the cost and consequences of the same, whereupon the Registry listed this matter, subject to objections, before the Court.

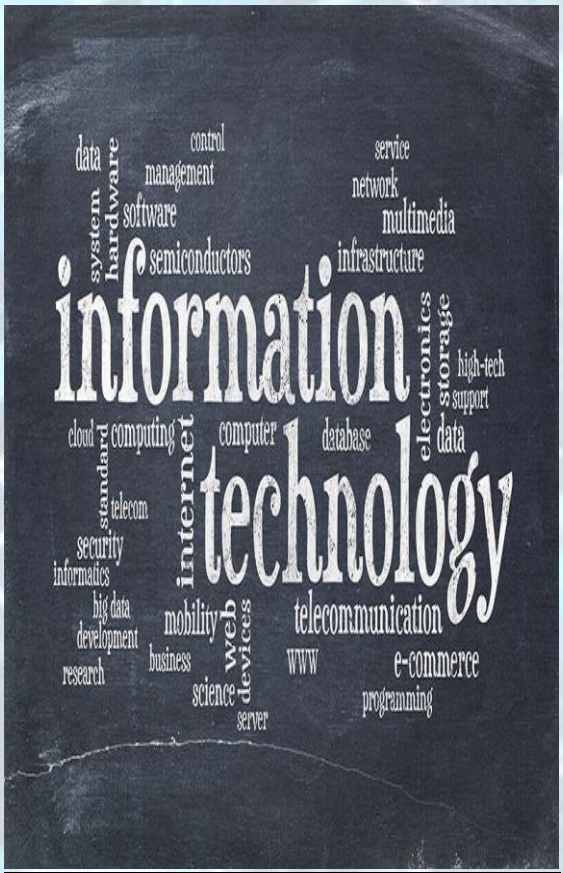
The entire suit filed by the plaintiffs is under Section 91of the Code of Civil Procedure read with Order XXVII-A and Order I Rule 8 of the Code of Civil Procedure. However, no application was filed along with this suit to seek the leave of the Court to institute the suit.

The Court termed the suit an "abuse of process of law" which resulted in wastage of judicial time. Therefore, a cost of Rs 20 laksh

was imposed, which was directed to be deposited before the Delhi Legal Services Authority. Also, the balance court fee payable of Rs 1,95, 594/- was also directed to be deposited. DSLSA shall utilize this cost for the cause of the victims of road accidents.

The Court further ordered:

"It appears that the plaintiffs have filed this suit to gain publicity which is clear from the fact that plaintiff No.1 circulated the video conferencing link of this Court on her social media accounts, which resulted in the repeated disruption of the Court proceedings.



MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (LEGAL POSITION)

The Ministry of Electronics and Information Technology is an executive agency of Government of India. It was set up in 2016 after being separated from Ministry of Communications and Information Technology. Shri Rajeev Chandrasekhar is the current minister of this particular ministry.

It performs various functions relating to cyber, IT and technology like promotion of internet, IT and IT enabled services, Unique Identification Authority of India (UIDAI), Matters relating to Cyber Laws, administration of the Information Technology Act. 2000, National Informatics Centre (NIC), Assistance to other departments in the promotion of E-Governance, E- Commerce, E- Medicine, E-Infrastructure, Promotion of Standardization, Testing and Quality in IT and standardization of procedure for IT application and Tasks, Initiatives for development of Hardware/Software industry including knowledge– based enterprises, measures for promoting IT exports and competitiveness of the industry etc.

It has also provided great services like Digi Locker etc. and introduced programs like Digital India, Technology Incubation and Development of Entrepreneurs (TIDE 2.0), Digi Dhan Mitra chatbot etc.

Social media platforms and the ministry

After the introduction of the new privacy policy of WhatsApp, Ministry of Electronics and Information Technology claims that such a policy violates the privacy of individuals along with the data security which is not in the good interest of the citizens and wants the court to declare such policy null and void. Also, such a policy is violative of Indian laws of Constitution, Information Technology Act, 2005 etc. The decision on this case is still awaited though.

OTT and Social Media Platforms and the regulation by the ministry

With the increase in growth of users on OTT platforms and social media users which in turn led to increase in cyber issues, there was a need to introduce laws relating to the same. The Government of India came up withthe Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, in order to regulate the content on the social media and OTT platforms like Netflix, Amazon Prime etc. All the rules of this act have been framed in accordance with the powers provided under the provisions of Section 87 (2) of the Information Technology Act, 2000.

Rationale and Justification for New Guidelines:

- **In Prajwal case of 2018, the Honourable Supreme Court had observed that the Government of India may frame necessary guidelines to banish child pornography, rape and gangrape imageries, videos in content hosting platforms and other applications.**
- **In 2019, the Supreme Court ordered the Ministry of Electronics and Information Technology to give the highlights and timeline of process competition of notifying the new rules.**
- **During the Calling Attention Motion on the misuse of social media and spread of fake news in the Rajya Sabha in 2018, the Minister conveyed to the house, that necessary actions will be taken to strengthen the legal framework and certain laws will be introduced to make social media platforms accountable.**
- **The Ad-hoc committee of the Rajya Sabha laid its report on 03/02/2020 after studying the alarming issue of pornography on social media and its effect on children and society as a whole and recommended for enabling identification of the first originator of such contents.**

Facebook and its intermediaries like Twitter, WhatsApp had for a timing refused to comply with the rules of abovementioned act and afterwards agreed to comply with the same demanding for a time period of six months to make compliance which they have failed due to the corona pandemic. If these social media platforms fail to comply with the rules, criminal proceedings could be initiated against them according to the provisions of Information Technology Act, 2000 and which could lead to their

departure from the country. The Ministry of Electronics and Information Technology is required to maintain a track record of the progress on compliance. These rules basically require WhatsApp to identify the real origin and originator of any message on its platform and Facebook and Twitter to pull down any content on its platform that would be unlawful according to the officers of ministry.

OTT Platform and Censorship Law

- **Online streaming portals like Netflix, Hotstar and Amazon Prime will now be subjected to the same censorship laws.**
- **Reason being objectionable content should be removed and OTT platforms violates Art. 19(2) of constitution.**

Conclusion: The position which the ministry maintains and the way it handles the particular issues and the legal duties which it has got to play, has got a very important position in the functioning of the cyber technology in the country. It has been endowed with the biggest and the most prestigious responsibility of the present times i.e., to maintain the cyber security and prevent cyber-attacks because of the increasing use of technology and IT. The Ministry is on its development path and is trying to make best use of technology in the country.

ALL ABOUT PEGASUS

Leaks associated with Israeli cyber-intelligence firm NSO Group's spyware Pegasus have created global headlines and sparked political controversies lately. Pegasus is spyware developed by the Israeli cyber arms firm NSO Group that can be covertly installed on mobile phones (and other devices) running most versions of iOS and Android. Pegasus exploits undiscovered vulnerabilities, or bugs, in Android and iOS. This means a phone could be infected even if it has the latest security patch installed. A previous version of the spyware from 2016 infected smartphones using a technique called "spear-fishing": text messages or emails containing a malicious link were sent to the target. It depended on the target clicking the link—a requirement that was done away with in subsequent versions.

By 2019, Pegasus could infiltrate a device with a missed call on WhatsApp and could even delete the record of this missed call, making it impossible for the user to know they had been targeted. Once installed on a phone, Pegasus can intercept and steal more or less any information on it, including SMSs, contacts, call history, calendars,

emails, and browsing histories. It can use your phone's microphone to record calls and other conversations, secretly film you with its camera, or track you with GPS.

In late 2019, Facebook initiated a suit against NSO, claiming that Pegasus had been used to intercept the WhatsApp communications of several activists, journalists, and bureaucrats in India, leading to accusations that the Indian government was involved. Phone numbers of Indian ministers, opposition leaders, ex-election commissioners, and journalists were allegedly found on a database of NSO hacking targets by Project Pegasus in 2021. Independent digital forensic analysis conducted on 10 Indian phones whose numbers were present in the data showed signs of either an attempted or successful Pegasus hack. The results of the forensic analysis threw up shows sequential correlations between the time and date a phone number is entered in the list and the beginning of surveillance. On different occasions, the Indian Government has been questioned on the Pegasus issue. On 17.07.2021, in response to the questionnaire which was sent to the MeitY by the consortium of journalists, the ministry said that the questions had already been answered. "Considering the fact that answers to the queries posed have already been in the public domain for a long time, it also indicates poorly conducted research and lack of due diligence by the esteemed media organizations involved ". On 19.07.2021, when the Pegasus issue was raised in Parliament, Mr. Ashwini Vaishnav, the Minister for Communications, Electronics & Information Technology and Railways, dismissed reports about the use of Pegasus for spying on journalists, activists, and opposition leaders. He said without technical analysis, it was not possible to say whether or not there had been an attempted hack.

For years, the spyware/surveillance software industry has operated discreetly, occasionally being exposed for their wrongs committed against human rights activists, journalists and researchers. The scale of misuse and human rights violations across the world that have been facilitated by Pegasus is quite staggering. Governments around the world must rise to the occasion to address this problem and they must collaborate and restrict the sale of surveillance tools and technologies. It is disheartening to see that the same issue has surfaced yet again in India and begs the same questions which have remained unanswered and unaddressed by the Indian Government.

Technology has played a vital part in boosting India's multifaceted growth. In the wake of the pandemic, the importance of technology is ever increasing. With the unwarranted power that it possesses, it is necessary to lay down proper laws in place that prevents abuse of technology to befit immoral and unethical practices. The need for well-defined restrictions in the IT sector stems from the necessity to limit the occurrence of cybercrimes while dealing

with technology that gets sophisticated by the minute.

IT LAWS IN INDIA- A HISTORY

The emergence of IT laws in India can be traced back to the resolution of the General Assembly of United Nations dated 30th January 1997 that gave birth to the Information Technology Act. This led to the adoption of Modern Law on Electronic Commerce on International Trade Law by the Indian polity. India became the 12th country to legitimize cyber regulations. The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 when the new IT Ministry was formed. After some required alterations to comply with the suggestions from the World Trade Organisation (WTO), the bill was referred to the 42-member Parliamentary Standing Committee following demands and suggestions from the Members. Post the initial draft created by the e-Commerce Act led by the Ministry of Commerce in 1998, the revised Information Technology Bill was passed in May 2000.

Finally, things came under control, with the inception of the Information Technology Act, back in October 2000. This Act intricately traced each trifling activity or transaction on the internet, cyberspace, and the World Wide Web. Each minuscule action, as well as its reaction in the global cyberspace, imposed severe legal implications and penalty angles.

The Act swiftly amended the traditionally-set Indian Penal Code 1860, the Bankers' Books Evidence Act 1891, the Indian Evidence Act 1872, and the Reserve Bank of India Act 1934. These amends aimed to tone up all electronic transactions/communications bringing them under the radar by granting strict legal recognition.

Regulatory Framework of IT laws in India

1. Information Technology Act, 2000

Activities in the cyber world in India are governed by the Information Technology Act enacted in 2000. The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 June 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to e-Commerce, facilitating registration of real-time records with the Government. But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed. The ITA, enacted by the Parliament of India, highlights the grievous punishments and

penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cybercrimes. In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format.

This Act deals with cybercrimes rigorously, and has brought about changes in the pre-existing laws of the country to incorporate penalty for acts overriding cyber security. The IT Act is the supreme law of India with regard to cybercrimes and related activities. A few sections of the Act claim immense importance in guiding the cyber world of our country-

- **Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.**
- **Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.**
- **Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.**
- **Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.**
- **Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.**

The Act has undergone amendments to suit the needs of the society from time to time. A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism. The

amendment was passed on 22 December 2008.

One major step towards driving people to indulge in digital transactions to increase its popularity and ease of use was the inclusion of digital signatures. This had far broader ambitions covering other tech-driven authentication forms like bio-metrics. Further, the popularity of electronic fund transfers and electronic data storage attested to the need and success of the futuristic vision behind the IT Act.

2. Indian Penal Code, 1860

The IPC, 1860 has been a prominent legislation in curbing cybercrimes and associated activities. Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000. The primary relevant sections of the IPC cover cyber frauds:

- Forgery (Section 464)
- Forgery pre-planned for cheating (Section 468)
- False documentation (Section 465)
- Presenting a forged document as genuine (Section 471)
- Reputation damage (Section 469)

Along with amendments to the IPC, certain provisions of the Evidence Act were also amended to include digital signatures in all relevant sections.

Several other legislations pertaining to the administration and governance of corporate businesses and commerce have also been amended to be inclusive of possibilities that may arise out of cyber security concerns. The Companies Act, NIST Compliance etc. have taken into account the necessary implications that cyber tech will pose and have ensured proper safeguards against it.

IT laws and need for change

It has been over two decades since the IT Act, 2000 was implemented for the first time. Several changes have taken place in the digital arena since then. There are vast areas that do not fall under the purview of this Act like Artificial Intelligence and Machine Learning, which drives an immense amount of information and communication in the digital sphere today. Significant technological, policy, and legal developments have taken place that subsequent amendments have not been able to completely account for. The ubiquity of smartphones and internet technology in modern life calls for a new paradigm of regulation on diverse subjects such as Artificial Intelligence and Machine Learning technologies, electronic financial services, and online gambling.

The Act has undergone amendments in 2006 and 2018 to incorporate various technological developments. Section 67BA is inserted by the 2018 Bill stating that whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is repugnant to well established cultural ethos, that person shall be punished on first conviction with imprisonment of either description for a term which may extend to

six months and with fine which may extend to two lakhs INR. Also, with respect to online gaming specifically, sections 67BB and 79B are inserted.

Specialists have opined that the amendments are toothless legislation and are not really compelling in awarding punishment to the culprits. There are several areas where IT laws can be improved like spamming, protection of users of internet banking etc.

One major type of cybercrime we see today is intellectual property infringement in the form of pirated movies, games etc. This is a widespread infringement of copyright laws; however, the numbers of culprits are so large that a successful measure cannot be taken to check it. So, to check the developing threat of digital violations, government through measures frequently deny access to sites. The Government of India was compelled to issue the Information Technology (Intermediaries Guidelines) Rules, 2011 which mandate an intermediary to observe due diligence while discharging its duties and not knowingly host or publish any information which infringes the Intellectual Property Rights of anyone. But the guidelines would not stop the piracy because of the vastness of the domain.

A key development is the emergence of progressive data protection paradigms. In its judgement in Shreya Singhal v. Union of India, the Supreme Court struck down section 66A as unconstitutional, stating that the provision was vaguely drafted and significantly violated the right to free speech guaranteed under articles 19, and 21 of the Indian Constitution. In light of the Supreme Court's judgement in Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors, provisions of the Act that relate to privacy, such as section 69, to accommodate the proportionality standards laid down in the aforementioned judgement.

Recommendations

Information Technology is an area that never loses its momentum to grow. It is only imperative that adequate measures to cope with its super paced advancement to prevent any to its users and to prevent abusers from profiting out of it. New laws have to be devised to replace these draconian laws that do not do justice to a lot of activities today. Privacy is of the utmost concern among users of digital media today. There have been incessant debates on the topic of how to deal with this issue but without any fruition. The unprecedented growth of artificial intelligence and machine learning also calls for proper checks so as to demote people from misusing it. Hopefully, lawmakers will consider these issues to bring about much needed amendments in the existing laws so as to incorporate all these up-and-coming digital avenues.

Sources

1. https://www.appknox.com/blog/cybersecurity-laws-in-india

2. https://thedailyguardian.com/two-decades-of-the-information-technology-act-2000-way-forward/
3. https://internetfreedom.in/it-act-amendments/

LAWS RELATING TO PORNOGRAPHY IN INDIA

Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.

Cyber pornography is banned in many countries and legalized in some. In India, under the Information Technology Act, 2000, this is a grey area of the law, where it is not prohibited but not legalized either.

Under Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment upto 3 years and fine upto 5 lakhs:

1. Publication- which would include uploading on a website, whats app group or any other digital portal where third parties can have access to such content.

2. Transmission- this includes sending obscene photos or images to any person via email, messaging, WhatsApp or any other form of digital media.

3. Causing to be published or transmitted- this is a very wide terminology which would end up making the intermediary portal liable, using which the offender has published or transmitted such obscene content. The Intermediary Guidelines under the Information Technology Act put an onus on the Intermediary/Service Provider to exercise due diligence to ensure their portal is not being misused.

Section 67A of the Information Technology Act makes publication, transmission and causing to be transmitted and published in electronic form any material containing sexually explicit act or conduct, punishable with imprisonment upto 5 years and fine upto 10 lakhs.

An understanding of these provisions makes the following conclusions about the law of cyber pornography in India extremely clear:

1. Viewing Cyber pornography is legal in India. Merely downloading and viewing such content does not amount to an offence.

2. Publication of pornographic content online is illegal.

3. Storing Cyber pornographic content is not an offence.

4. Transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence.

In a very recent case, a 21-year-old Engineering student was arrested for sending obscene pictures by WhatsApp to a woman.

In the infamous Bazee.com case, the CEO Avinash Bajaj was arrested for an advertisement by a user to sell the DPS sex scandal video. The video was not uploaded on the portal, despite that Avinash was arrested under Section 67 of the Information Technology Act. It was subsequent to this case that the Intermediary guidelines were passed in 2011 whereby an Intermediary's liability would be absolved if they exercised due diligence to ensure obscene content is not displayed on their portal.

However, there is one case in which viewing Cyber pornography is punishable with imprisonment upto 5 years and fine upto 10 lakhs. Where the content contains children engaging with one another or with adults in sexually explicit acts.

Browsing or downloading Child pornography online is also a punishable offence under the Information Technology Act. The creation of child pornography is also punishable under the Act.

The act of collecting and storing cyber pornography is not an offence, but if the content involves minors, then it is punishable with imprisonment upto 5 years and fine upto 10 lakhs.

World over online child pornography is illegal. One of the biggest publicized catches of child pornography perpetrators was launched in May 2002 and called Operation Ore. After the FBI accessed the credit card details, email addresses, and home addresses of thousands of pornographers accessing a British child pornography site, the particulars were given to the British police for investigation. The arrest of a computer consultant in Texas led to an international investigation that jailed Thomas Reedy for 1,335 years for running the pornography ring. About 1,300 other perpetrators were also arrested, including teachers, child-care workers, social workers, soldiers, surgeons, and 50 police officers. As a result, 40 children, 28 of them in London, were placed under protective care.

To conclude, Cyber pornography has not been legalized in India, however, it's browsing has not been prohibited either except in the case of child pornography

NATIONAL AND INTERNATIONAL NEWS RELATED TO TECH, CYBER AND IT

DOJ Solar Winds hackers breached emails from 27 US Attorney's office. The Russian hackers who orchestrated the Solar Winds supply chain attack pivoted to the internal network of the US DoJ, from where they gained access to Microsoft Office 365 email accounts belonging to employees at 27 state attorneys offices Node.js fixes severe HTTP bug that could let attackers crash apps Node.js has released updates for a high severity vulnerability that could be exploited by attackers to corrupt the process and cause unexpected behaviours, such as application crashes and potentially remote code execution(RCE). Microsoft Shares More Information on Protecting Systems Against PetitPotam Attacks PetitPotam is the name assigned to a vulnerability that can be exploited by an unauthenticated attacker to get a targeted server to connect to an arbitrary server and perform NTLM authentication Indian nearly lakh cyber-attacks in 2020, I1 Ministry tells Parliament The Ministry of Electronics and Information technology said proactive tracking by CERI - in and improved cyber security awareness among individuals and organisations across sectors has led to increased reporting of incident ne Indian computer Emergency response team (CERT-n) has reported 49, 455. 50,362, 53.117. 208,456, 394,499 and 646,938 cyber security incidents airing the year 2015, 2016, 2017, 2018, 2019 and 2020 (till August) respectively. the MelTY said while responding o an unstarred question in the Lok Sabha regarding cyber-attacks on Indian citizens and India-based commercial and legal entities. Apple Introduces UPL RuPay, Net banking as Additional Payment Options on App Store, iTunes How to Us hem Apple advise users to be on the latest version of ioS IPados, or MacOS to be able to see these new payment Options UN Security Council Confronts Grouing Threat of Cyber Attacks the Security Council has addressed the subject in the past, but only informally. both in public or behind closed doors. -India s Offensive Cyber Capability Pakistan-Focussed and Not Tuned Towards

China, Study Claims he 182 page study by the International institute for Strategic Studies talked about the key areas where India lags when it comes to cyber security India, Australia To Expand Cooperation In Digital Economy, Cyber Security India Australia Ties The two sides discussed a range of issues relating to emerging technologies in the cyber domain at the first meeting or the India- Australia Joint Working Group JWG) on cyber security cooperation according to the Ministry of External Affairs (MEA Security Of Government Computers Breached, E-Mail Traced To Bengaluru he computers broken into also stored data relating to National Security Advisor Ajit Doval, Indian citizens and senior government functionaries.

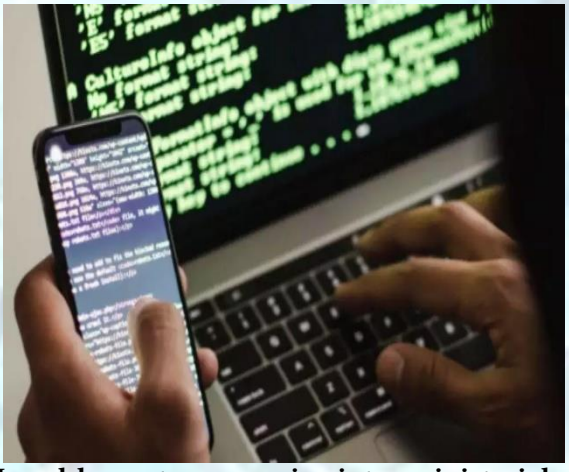
National and International news Cyber technology

International News:

- **Cybersecurity firm Kaspersky warns users about the presence of fake Windows 11 downloaders that can infect your computer with malicious software.**

With Microsoft announcing the new Windows 11 operating system, you may be all excited to upgrade your PC. However, before you click the install button, the biggest mistake you can make is to not verify the source of the Windows 11 update. Kaspersky is warning users about the presence of fake Windows 11 downloaders and claims to have "defeated several hundred infection attempts". A large portion of these threats consists of downloaders, whose task is to download and run other programs.

- **Israel's National Security Council 'looking into' NSO spyware allegations.**



Israel has set up a senior inter-ministerial team to "look into" proliferating allegations that spyware sold by an Israeli cyber firm has been abused on a global scale, an Israeli source said on Wednesday, while adding that an export review was unlikely. The team is headed by Israel's National Security Council, which answers to Prime Minister Naftali Bennett and has broader areas of expertise than the Defence Ministry, which oversees exports of NSO Group's Pegasus software, the source said. "This event is beyond the Defence Ministry purview," the source said, referring to potential diplomatic blowback after prominent media reports this week of suspected abuses of Pegasus in France, Mexico, India, Morocco, and Iraq. On Wednesday, French Prime Minister Jean Castex said French President Emmanuel Macron had called for a series of

investigations to be carried out into the Pegasus spyware case.

- Amid China's military pressure, Taiwan prepares for cyberwar.

Cyber-attacks are a growing global threat and several countries are now focusing on the mounting threat of cybercrimes, Taiwan being at the forefront amid China's military pressure and crippling cyberattacks. Taiwan's head of cybersecurity told CNN Business this month that it is using dramatic measures to guard against technological vulnerabilities including employing roughly two dozen computer experts to deliberately attack the government's systems and help it defend against what Taiwanese authorities estimate are some 20 million to 40 million cyberattacks every month. Taiwan says it has been able to defend against the overwhelming majority of attacks. Successful breaches number in the hundreds, while only a handful are what the government classifies as "serious."

National News:

1. 2 lakh tech support scams detected in India in Q1 2021: Report

Cybersecurity researchers reportedly said that they have detected and blocked more than 200,000 tech support scam attacks in India in the first quarter of this year. In tech support scams, fraudsters use scare tactics to trick innocent individuals into purchasing overpriced and unnecessary "support services" to fix an alleged computer, device, or software problem. Once granted access, bad actors can also install malware, or other malicious programs that damage the data housed on devices, or even worse, harvest personal information. According to a report by cybersecurity company Avast, tech support fraud remains a massive issue in India. "Tech support fraud is increasingly common and targets some of the most vulnerable individuals. Criminals exploit victims through money or personal information," said Alexej Savcin, Senior Malware Analyst, Avast.

2. Pegasus Controversy: India Inc fear of being snooped put mechanisms in place

Days into the Pegasus spyware saga a large Indian conglomerate is working with a cyber security firm to hand out 150 special phones to its key executives across companies. These phones would not be able to download any applications or surf the internet. And every message or phone call received or sent would go through a protected server. Call it the Pegasus effect. From upping their

internal security to creating centralized servers and from getting vulnerability tests to sensitizing the senior management about cyber risks, the Pegasus spyware incident has brought the spotlight on rapidly emerging enterprise threats from cyberspace. "Many business organizations have woken up to cyber-forensic and business risk emanating from Pegasus' kind of surveillance. There is a consequential and existential risk of loss of key business information assets and compromise of personally identifiable information for business organizations," said Kartik Radia, managing partner, Mazars India, a professional services firm.

AMENDMENTS

The Information Technology (IT) Act has undergone amendments to ensure that it covers almost all of the up-and-coming advancements of the cyber world. Several other legislations have also been laid down to cater to the needs of the growing tech savvy world.

1. **IT Amendment Act, 2008**

   The IT Amendment Act brought in some notable changes such as:

   - **Focus on data privacy,**
   - **Introduction of information security practices,**
   - **Definition of cybercafé,**
   - **Responsibility on companies to implement reasonable security practices to protect information from unauthorized access, damage, use, modification, disclosure, or impairment.**
   - **Computer related offences**
   - **Power of interception- The scope of the information intercepted was broadened to include its transmission, generation and storage, as opposed to just transmission in the original provision.**
   - **Critical information infrastructure- The Amendment Act introduced the term 'critical information infrastructure' ("CII") i.e., a computer resource whose destruction will have a huge impact on the national security, public health and safety and economy.**

This amendment also ensured that draconian provisions of the law are replaced with more relevant and necessary safeguards. It also imposes both civil and criminal liability for data theft.

2. **National Cyber Security Policy, 2013- In July 2013, the erstwhile Ministry of**

Communication and Information Technology notified the National Cyber Security Policy ("NCSP"). Based on the objectives envisioned in the NCSP 2013, the following strategies/initiatives were introduced by the Indian government:

- **Designation of the NCIIPC as the nodal agency to undertake measures to secure the country's CII.**
- **Cyber Swachhta Kendra initiative under the CERT-In to combat and analyse any malicious**
- **Infections/attacks that damage computer systems.**
- **Development of multilateral relationships in the area of cyber security.**
- **Setting up of the National Cyber Coordination Centre ("NCCC") to create situational awareness about cyber security threats and enable timely information sharing for preventive action by individual entities.**

3. **The Personal Data Protection Bill, 2019- It was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. The Bill proposes to supersede the Information Technology Act, 2000 (Section 43-A) deleting the provisions related to compensation payable by companies for failure to protect personal data. The PDPB inter alia, prescribes the manner in which personal data is to be collected, processed, used, disclosed, stored and transferred.**

4. **National Cyber Security Strategy 2020- The Indian government has proposed to come out with the National Cyber Security Strategy ("NCSS") 2020. The NCSS aims to examine various facets of cyber**

security under three pillars- securing the national cyberspace; strengthening the structures, people, processes, capabilities; and synergizing the resources including cooperation and collaboration. The government had sought comments and suggestions on different aspects of the NCSS by 10th January 2020 and is currently in the process of framing the policy.

Sources-

1.https://www.ikigailaw.com/cyber-security-framework-under-the-it-act-in-india/

2.https://blog.ipleaders.in/changes-and-developments-in-crimes-in-cyber-world-since-indian-independence/

3.https://internetfreedom.in/it-act-amendments/

4.https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019

QUIZ

Question 1: App permissions in your mobile phone can cause trouble as some apps may secretly access your OTPs or details of contacts from your phone

(a) True

(b) False

Question 2: Keeping which of the following functionalities activated all the time can cause serious threat to the security of your mobile phone?

(a) Flashlight

(b) Bluetooth

(c) Rotation

(d) All of the above

Question 3: Which of the following password is more secure?

(a) Boat123

(b) WTh!5Z7

(c) into*48

(d) 123456

Question 4: Is any website whose URL starts with https safe to access?

(a) Yes

(b) No

Question 5: Which of the following can be considered as a cybercrime as per Indian IT Act?

(a) A criminal activity that involves usage of a communication device like mobile phone

(b) Unauthorized access of information on a server

(c) Both

Question 6: Is violation of privacy a cybercrime as per Indian IT Act?

(a) Yes

(b) No

Question 7: Smishing is a type of attack done over

(a) Email

(b) SMS

(c) Wi-Fi

(d) Pen drive

Question 8: Which among the below is not a correct example of multi-factor authentication?

(a) Password + SMS OTP

(b) Password + PIN

(c) Password + Face recognition

(d) Entering PIN for a card transaction while withdrawing money at ATM

We are open for suggestions of the next issue of the magazine.

THANKYOU!!!