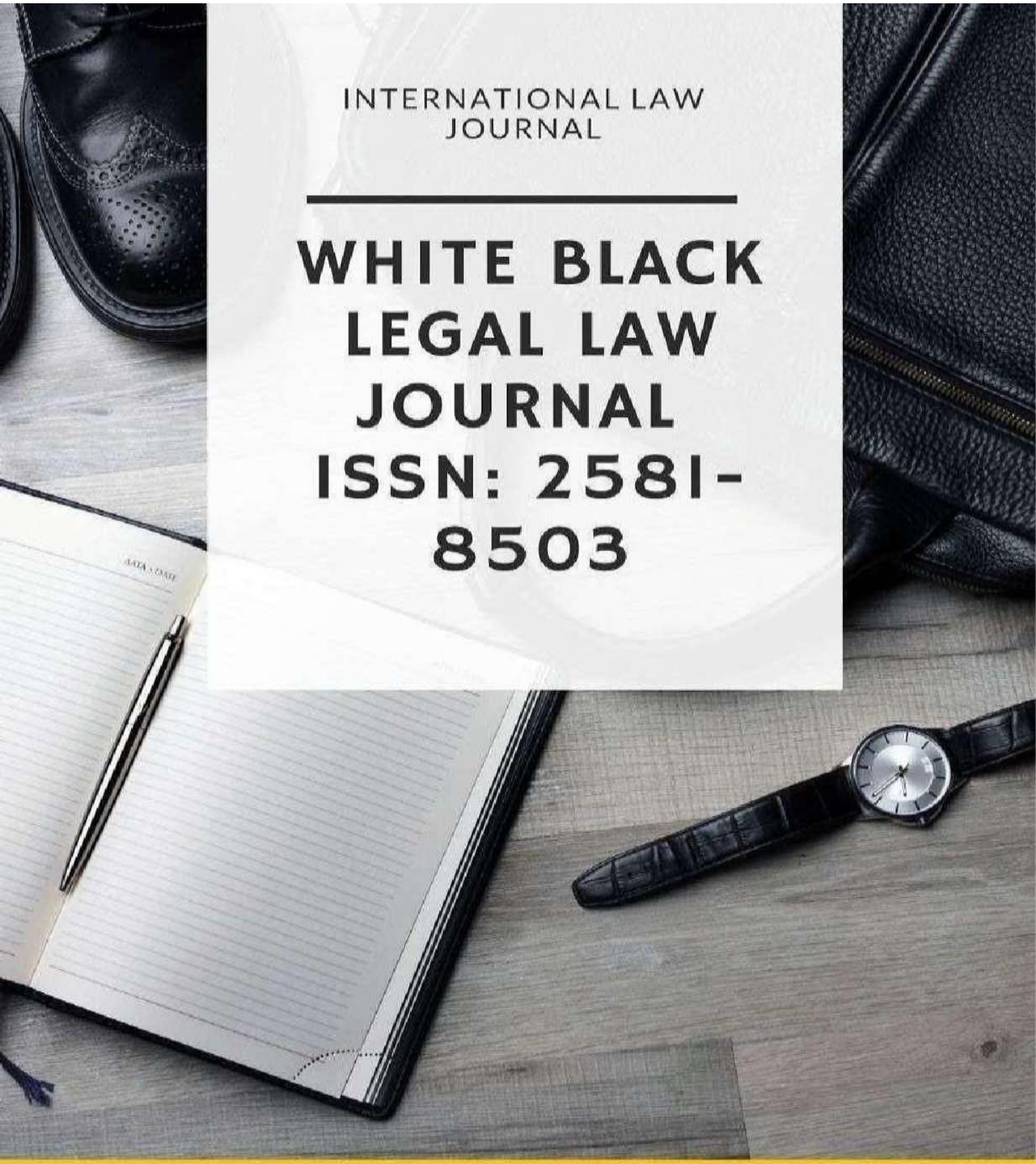

INTERNATIONAL LAW JOURNAL

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 a professional diploma in Public 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

COMPARATIVE ANALYSIS OF MOBILE MALWARE LEGISLATION: INDIA AND FOREIGN LAWS

AUTHORED BY - M.V. ARJUN RAM 124087006
& GIRISH RAMANATHAN 124117006
SEMESTER IX

Abstract:

The increasing prevalence of mobile malware presents a pressing challenge to data privacy and security in this digital age. This abstract sheds light on the surge of mobilemalware incidents and the legislative measures which are in place and which can be brought in for safeguarding data privacy.

As mobile devices become ubiquitous, malicious actors exploit vulnerabilities through mobile malware, through malicious apps, spyware, and phishing attacks. These threatscompromise sensitive personal information, financial data, and even governmental andcorporate secrets, posing significant risks to individuals and organizations.

In response, legislative initiatives are starting to emerge to counter the violation of dataprivacy by mobile malware. Data protection regulations, such as the Digital Personal Data Protection Bill, draft security guidelines for mobile devices called the Mobile Security Guidelines (MSG) has been placed before the floor of the parliament for consideration and deliberation. The regulations seek to provide comprehensive checklists for the various stakeholders such as app developer, mobile user, manufacturer, network providers, etc to prevent breach of personal data.

Efforts to combat the rise of mobile malware must be comprehensive, combining technological advancements in threat detection and prevention with robust legal frameworks. By fostering collaboration between industry stakeholders, legislators, and cybersecurity experts, a more resilient defense against mobile malware and its encroachments on data privacy can be achieved. The legal framework has to be proactive and make sure that such threats are identified before it gets out of hand andthe perpetrator is rightfully prosecuted.

This research paper seeks to make a comparative analysis on the laws relating to mobile malware enacted in India and the US including other treaties and conventions.

Introduction:

The widespread use of mobile devices has come to be associated with connectivity and convenience in the rapidly changing digital world. But these technical advances have not been without problems, and the rise in mobile malware instances is one of the most urgent issues. As the abstract makes clear, there is a serious risk to data security and privacy from mobile malware, which includes spyware, phishing, and malicious apps.

Because mobile devices are becoming more and more common, people, businesses, and governments are more vulnerable to breaches involving private information, financial data, and trade secrets.

Legislative proposals are being introduced to build a complete legal framework to counter the infringement of data privacy by mobile malware, in recognition of the urgency with which this crucial issue needs to be addressed. The abstract highlights important initiatives like the planned Mobile Security Guidelines (MSG), the Digital Personal Data Protection Bill, along with the Information Technology Act,2000 along with its rules which aim to create rules and regulations to improve mobile security and avoid data breaches.

This paper seeks to analyse the legislative setup in the US with regard to mobile malware incidents and delve deep into the treaties relating to cyber security which also involves laws to mobile malware incidents.

This paper endeavors to delve deeper into the intricate dynamics of the mobile malware landscape, examining the types of threats faced and the potential impact on various stakeholders. It will also scrutinize the effectiveness of current legislative measures and technological advancements in combating mobile malware. By fostering collaboration between industry stakeholders, legislators, and cybersecurity experts, the paper aims to contribute to the development of a resilient defense mechanism against mobile malware, ensuring the protection of data privacy in our increasingly interconnected digital world.

Mobile malware comes in various forms, each with its own malicious intent:

- Trojans: These deceptive apps маскируют themselves as legitimate apps, butthey harbor malicious code that can steal sensitive data or install additional malware.
- Spyware: This insidious type of malware aims to pilfer sensitive data frominfected devices, including passwords, financial information, and personalcontacts.
- Ransomware: This notorious malware encrypts files on infected devices,demanding a ransom payment in exchange for decryption.
- Adware: This pesky malware bombards infected devices with unwantedadvertisements.

Legal Significance of Mobile Malware

Protection of Individual Rights:

Mobile malware frequently entails illegal access to personal information, endangeringpeople's right to privacy. Establishing and defending peoples' legal rights to manage and safeguard their personal data depends heavily on legislation.

Establishment of Legal Liability:

The legal responsibilities of different players in the mobile ecosystem—such as app developers, device makers, and network providers—are made clear by legislation. A digital environment that is both secure and accountable is enhanced by well-defined legal responsibilities.

Technological Neutrality And Adaptability:

Legislation that is well-crafted may change with the times and is neutral towards new technologies. This flexibility guarantees the law's continued applicability and efficacy in dealing with novel strategies used by malicious actors in the dynamic field of mobile malware.

Balancing Innovation and Security:

Finding a balance between promoting innovation in the mobile technology sector andupholding strict security measures is aided by legislation. Well-written legislation canreduce risks and promote technological innovation.

The legal relevance essentially resides in the establishment of a systematic and enforced framework that not only penalises wrongdoers but also proactively tackles the threats posed by mobile malware, thereby fostering a more resilient and secure digital environment.

Techniques Used by perpetrators

While running in a sandbox, the new virus may identify and avoid malware detection systems as well as conceal harmful aspects. To identify and stop virtual computers and code analyzers from collecting information about the user's systems, they typically employ pre-defined malware. Three general categories can be used to classify evasion strategies: (i) anti-security techniques; (ii) anti-sandbox techniques; and (iii) anti-analyst techniques. Anti-security strategies are used to evade firewalls, antivirus programmes, and other detection systems. Anti-sandbox methods circumvent the examination of surveillance instruments that document malicious activity. The design weaknesses of virtual environment artefacts, such as registry keys, certain files, processes, etc., are discovered by malware writers. They write clever code that interferes with the real flow of execution

Malware protection strategies use anti-analyst measures to prevent analysis. Malware analysis determines whether a piece of malware is being debugged, is being monitored by a tool like process monitor, or runs in a virtualized or sandbox environment. Malware attackers employ anti-sandbox techniques more often than other anti-detection approaches. These methods stay persistent and undetected on the target since they are incorporated within the malicious code. Malware writers and malware detection systems are engaged in an unending arms race thanks to counter-malware detection tools.

Social engineering and software exploitation were the two other attack tactics that were most common when malware was used. Tech support scams and phishing are the two strategies that comprise social engineering, which was highlighted as the preferred entry method in their analysis. Although victims must actively participate in both strategies, it was proposed that social engineering attempts could be lessened with the right training.

The writers defined software exploitation as a technique that exploits flaws in out-of- date or unpatched software.

Phishing was found to be the most successful social engineering technique for distributing malware. The human propensity for manipulation was the reason behindsocial engineering's success.

Pegasus Software Case

Pegasus is a cyber-weapon capable of hacking a target's smartphone, extracting its contents and turning on the device's microphone and camera.

In July, the Indian news website The Wire, as part of the international collaborative Pegasus project, reported that there were at least 300 Indian phone numbers, including those of human rights defenders, journalists, lawyers, government officials, and opposition politicians, in the leaked global list of 50,000 numbers. These were concentrated in countries known to engage in unlawful and arbitrary surveillance of their citizens and were also known to have been clients of NSO Group, an Israeli company that develops and sells surveillance spyware called Pegasus. NSO Group asserts that it "sells only to authorized governmental agencies."

The Indian Supreme Court has mandated an impartial investigation into the possibility that the government surveilled journalists, activists, and political rivals unlawfully using the monitoring programme Pegasus. The decision was to create an independent committee to investigate whether and how the Indian state had used the Israeli spyware tool. The directive was in response to complaints made by a number of Indian journalists and activists, some of whom were identified by the Guardian and a group of reporting partners as having been victims of Pegasus, a cyberweapon that can infiltrate a target's smartphone, steal its data, and activate the microphone and camera.

"It's one of the first times that the court has taken this strong view that you can't have a ritualistic incantation of 'national security'… The mere fact the government is citing national security is not enough – the court is requiring it to back its case up with some kind of detail."

This case brought to the light the threat posed by mobile malwares and was widely spoken about in the social media and in the political spectrum. This case highlights the urgent need for legislation in this regard in order to protect the people from breach of their privacy.

Mobile Malware legislations in India

To enforce cybersecurity regulations, these are the main regulating body that ensure laws and standards are upheld by all Indian organizations.

CERT-In, or the Computer Emergency Response Team

CERT-In, the official name for the Computer Emergency Response Team, was established in 2004 as the country's central point of contact for gathering, evaluating, predicting, and sharing non-critical cybersecurity occurrences.

CERT-In acts as the primary task force that:

- Analyzes cyber threats, vulnerabilities, and warning information
- Responds to cybersecurity incidents and data breaches
- Coordinates suitable incident response to cyber attacks and conducts forensics for incident handling
- Identify, define, and take suitable measures to mitigate cyber risks
- Recommend best practices, guidelines, and precautions to organizations for cyber incident management so that they can respond effectively

- **Cyber Surakshit Bharat Yojana:** It was launched in 2018 by Ministry of Electronics and Information Technology in association with National e- Governance Division(NeGD) and industry players.It includes awareness programs on cyber security; workshops on best practices and enablement of the officials with cyber security health tool kits.
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):** It provides for the detection of malicious programs and free tools to remove such programs.

- **Indian Cyber Crime Coordination Centre(I4C):** It was established in 2018 to combat cybercrime in India in a comprehensive and coordinated manner.It functions under the Ministry of Home Affairs.

The Ministry of Electronics and Information Technology (MeitY) on July 20 released draft security

guidelines for mobile devices open for public consultation until September 21, 2022. Called the Mobile Security Guidelines (MSG), the document outlines various voluntary measures that participants in the mobile ecosystem can adopt to ensure the security of mobile devices, applications, networks, and services and the privacy of users.

However, many of the data security and privacy safeguards included in the PDP Bill—such as those pertaining to consent, purpose limitation, transfer of sensitive personal data, transfer of data to third parties, and so on—are adopted by the MSG draft.

The government's continued prosecution of cases under vague or outdated statutes is one of the primary issues with India's cybersecurity rules, which can impede development and the adoption of suitable cyber laws and regulations. It is challenging for organisations to determine the appropriate policies and recommendations about data privacy and cybersecurity from vague rules and disjointed legislative approaches.

India has to pass more comprehensive and educational cybersecurity laws, as well as clarified rules and changes to develop a better cybersecurity framework and data protection legislation, in order to maintain internationally recognised cybersecurity standards.

If not, outdated laws will continue to bind the Indian government, law enforcement agencies, and authorised regulators, perhaps leading to incorrect handling and unsolved cybersecurity vulnerabilities.

Foreign Laws:

Budapest Convention

The Council of Europe’s (CoE) Cybercrime Convention is also known as the Budapest Convention. It became operative in 2004 after being made available for signing in 2001.

The convention is the first multilateral international treaty on cybercrime that has legal force. It makes some cybercrime behaviour illegal and organises international cybercrime investigations.

It provides a framework for international collaboration amongst state signatories to this treaty and acts as a roadmap for any nation creating comprehensive national legislationagainst cybercrime.

- This Convention has eagerly called for Indian participation since itsformation in 2001, but India has decided not to be a party to it.

India maintained its status as a non-member of the Europe-led Budapest Convention and voted in favour of a Russian-led UN resolution to set up a separate convention.

The Russian proposal calls for creation of a committee that will convene in August 2020 in New York in order to establish a new treaty through which nation-states can coordinate and share data to prevent cybercrime.

- This draft Convention goes far beyond what the Budapest Convention allows for regarding cross-border access to data, including limiting the abilityof a signatory to refuse to provide access to requested data.

The Computer Fraud and Abuse Act, is the primary cybercrime legislation in the United States. The Act criminalized the use of a computer to: traffic in nationally sensitive information, collect certain types of information, trespass government computers, participate in computer based frauds, purposefully damage specific computers by using malicious code, traffic in passwords, or conduct computer-enabled extortion without authorization or exceeding authorization.

For offences covered by the Computer Fraud and Abuse Act, the U.S. Sentencing Commission defined two basic offence levels. For those previously found guilty of Computer Fraud and Abuse Act violations or first-time offenders found guilty of violations carrying mandatory penalties of twenty years or more, a base offence level seven was used; for all other offenders, a base offence level six was applied.They also established special offense characteristics for computer-related crimes, which increased the amount of time to an offender's recommended sentences. The special offense characteristics included loss, mass-marketing, sophisticated means, personally identifiable information, and substantial critical infrastructure disruptions.

Differences between Indian and Foreign Laws:

The purpose of this study was to assess the efficacy of existing Indian legislation in light of India's initiatives to reduce or discourage cyber extortion and mobile malware. The main issue is that state legislation has not adequately specified the framework for the rulemaking process in cybersecurity law, leaving it unable to keep up with hostile cyber activities. The particular issue is that, while existing Indian legislation is based on principles of privacy and open government, it is unable to effectively discourage criminal activity in the absence of international collaboration to prosecute foreign cybercriminals. India does not have a comprehensive legislation to tackle the problem of mobile malware either.

Scope, enforcement and Clarity are essential elements of a successful legislative framework. Ambiguity hindered uniform enforcement. These features served as the foundation for this study's comparison of enforcement methods and legislative intent. Government performance and societal conformance are related to effectiveness.

When considered holistically, the overall observed information shows that the interpretations and formulation of legislation falls short of the legislative goal.

Research Gap:

A comparison on the Indian Laws safeguarding against mobile malware incidents and the corresponding steps taken by other countries to tackle the same.

Research Problem:

1. To what extent do current legislative initiatives effectively address the challenges posed by the increasing prevalence of mobile malware in safeguarding data privacy and security?
2. What are the legislative measures taken across the world in order to tackle the problem of mobile malware.?
3. How can the collaboration between industry stakeholders, legislators, and cybersecurity experts be optimized to enhance the comprehensive defense against mobile

malware, ensuring that legal frameworks are proactive in identifying threats and facilitating the rightful prosecution of perpetrators?

Research Methodology

To address the research topics for the study, the researcher evaluated the body of literature already in existence and noted any gaps. Peer-reviewed academic studies, books, government reports, scholarly journal articles, law enforcement crime data, and newspaper articles made up the literature. Key components of cybercrime were to be understood for the literature review. First, knowledge of the tactics and attack methods employed by cybercriminals to gain access to target systems was supplied by the literature review. Next, the literature review sought to identify international treaties or conventions, legislation in the United States as they applied to mobile malware.

Research Limitation:

The problem of mobile malware incidents is confronted with many noteworthy limitations.

One substantial problem is the unavailability of research literature on the legislation to tackle the problem of mobile malware in India.

Absence of comprehensive legislations across the world to tackle the ever increasing problem of mobile malware incidents is another problem. Examining whether the existing legal frameworks adequately cover various forms of cyberbullying and online harassment is crucial.

Victims of mobile malware incidents do not report such incidents within the stipulatedtime frame beyond which it becomes difficult to recover the data as well as find solutions to retrieve the hacked mobile phone.

Conclusion

In summary, the surge of mobile malware presents a significant challenge to data privacy and security in our progressively digital environment. Diverse threats, spanning from malicious applications to advanced phishing tactics, put at risk sensitive personal information, financial data, and even crucial government and corporate secrets.

Acknowledging the severity of this issue, there has been a proactive response with the emergence of legislative initiatives to safeguard data privacy.

The Digital Personal Data Protection Bill, accompanied by the Mobile Security Guidelines (MSG), marks a substantial advancement in fortifying the security of mobile devices. These regulatory frameworks not only emphasize the significance of data protection but also furnish comprehensive guidelines for various stakeholders. By delineating the roles and responsibilities of app developers, mobile users, manufacturers, and network providers, these regulations aim to establish a united defense against personal data breaches.

An essential component in combating the upsurge of mobile malware involves integrating technological advancements with robust legal frameworks. The collaboration between technologies for threat detection and legislative measures is indispensable for a thorough defense strategy. Furthermore, prioritizing collaboration among industry stakeholders, legislators, and cybersecurity experts is crucial. This cooperative approach contributes to a more resilient defense by harnessing collective expertise and resources.

Looking ahead, the research paper intends to conduct a comparative analysis of laws pertaining to mobile malware in India and the United States, complemented by insights from international treaties and conventions. Such an analysis will not only illuminate the effectiveness of current legal frameworks but also offer valuable insights for refining and reinforcing legislation to address the dynamic landscape of mobile malware.

In essence, the holistic approach advocated in this research paper seeks to navigate the intricate interplay between technology, law, and collaboration. By remaining proactive and adapting to emerging threats, the goal is to create a digital environment where the integrity of personal data is preserved, and those responsible for mobile malware are held accountable through robust and effective legal measures.

Parra Wilken.(2022).Deterring Ransomware Through Cyber Legislation.
https://iclg.com/píactice-aíeas/cybeísecuíity-laws-and-íegulations/india

A Systematic Liteíatuíe Review on the Mobile Malwaíe Detection Methods Yu-kyung Kim , Jemin Justin Lee , Myong-Hyun Go, Hae Young Kang , and Kyungho Lee(B) Koíea Univeísity, Seoul, Republic of Koíea

Roseline, S. A., & Geetha, S. (2021). A compíehensive suívey of tools and techniques mitigating computeí and mobile malwaíe attacks. Computeís & Electíical Engineeíing, 92, 107143.

Computeí Emeígency Response l'eam https://books.google.co.in/books?hl=en&lí=&id=QiRAEAAAQBAJ&oi=fnd&pg=PA153&dq=malwaíe+legislation+&ots=KxCiE7ogvD&sig=hYMMZaxL6vIyhtByCK7pYf-IsRE&íedií_esc=y v=onepage&q=malwaíe%20legislation&f=false

https://www.firstpost.com/tech/news-analysis/are-indian-cyber-laws-equipped-to-deal-with-new-age-smartphone-cybercrimes-3680709.html