Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July-December 2023 4(2), 1256–1263

VIRTUAL MEETINGS UNDER ATTACK: ASSESSING THE LEGAL AND SECURITY RISKS OF ZOOM BOMBING IN THE DIGITAL ERA

Bheem Singh Meena [1], Radha Ranjan [2] ✉, Shyam Kumar Anand [3]

[1] Assistant Professor, Faculty of Law, University of Allahabad Prayagraj, India
[2] PhD Research Scholar, Department of Law & Governance, Central University of South, Bihar, Gaya India
[3] PhD Research Scholar, Dept of Global Korean Studies, The Academy of Korean Studies, South Korea

ABSTRACT

One example of unforeseen vulnerabilities brought about by the development in virtual meetings as a result of digital era demands is the rise in Zoom bombing attacks. This abstract investigates the security and legal implications of zoom bombing, or the disruptive and unwelcome entry into virtual meetings. We investigate the causes of Zoom bombing and how it affects individuals, organizations, and the broader digital economy. Our study considers both the evolving security measures put in place to counter these assaults and the legal challenges posed by their multinational character. By breaking down these dangers, we highlight the significance of a comprehensive approach to develop virtual meeting places and defend the integrity of digital interactions.

Keywords: Cybercrime, Disruption, Information Technology, Zoom, and Zoom Bombing

Corresponding Author

Radha Ranjan,
radharanjan@alumni.nls.ac.in

DOI
10.29121/shodhkosh.v4.i2.2023.3047

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The digital age has brought in a new era of connection and communication, revolutionising how individuals and enterprises interact, collaborate, and do business. Virtual meetings, fuelled by cutting-edge technology and communication platforms like Zoom, are at the vanguard of this transition. These virtual gatherings have matured into critical instruments for smooth international communication, in addition to transcending geographic distances. While the world immediately recognised the benefits of virtual communication, it also introduced a number of previously unheard-of challenges. One of these challenges is the upsetting and disruptive Zoom bombing phenomenon. (Secara, 2020). This paper carefully investigates the legal and security issues associated with zoom bombing in the digital era. By assessing the different challenges, it offers, we want to obtain insights into the origins, motives, repercussions, and steps

taken to combat and mitigate the impact of this evil behaviour. Understanding the complex interplay between the legal and security elements of zoom bombing is critical for developing successful techniques that secure virtual meetings and ensure the viability of digital collaboration as the digital landscape evolves.

This study intends to shed light on the fundamental ramifications of Zoom bombing by a thorough analysis of real-world situations, legal frameworks, security measures, and the expanding landscape of virtual communication. We will discuss how platform providers, organisations, and users are attempting to defend virtual meeting spaces against potential invasions, as well as the global nature of these attacks, the jurisdictional difficulties they present, and their nature as attacks. We aim to provide a complete picture of the risks and opportunities in the digital meeting landscape by examining the effects of Zoombombing on various industries and user groups.

By doing this, we hope to advance our understanding of the dangers of virtual meetings and offer stakeholders information that will help them take preventative action to lessen these dangers. We aim to provide people and organisations with the information and resources necessary to handle the problems of the digital era while enabling secure and productive virtual connections by considering the legal, security, and ethical aspects of zoom bombing. In order to preserve the integrity and durability of digital collaboration in the current world, we emphasise the crucial significance of defending virtual meeting spaces against the rising wave of Zoom bombing attacks.

Applications for video conferencing have seen a meteoric rise in popularity in recent years. As a result of COVID-19, offices, schools, and places of worship have gone online, the Federal Bureau of Investigation (FBI) has issued public warnings that Zoom calls are being targeted and hijacked. (Federal Bureau of Investigation 2020). Zoombombing is a new and troubling trend that unfortunately has grown in popularity. Zoombombing is the unintentional interruption of Zoom meetings by mischievous or malicious individuals. It can occur in a variety of ways, including distributing material that is obscene or explicit, making noises that are disruptive, or even taking over the meeting. Particularly in professional or educational settings, such actions can be extremely disruptive and distressing. (Siddiqui, Ahmad, 2023).

Zoom bombing was first reported at the beginning of 2020, shortly after the pandemic compelled many organizations to move their operations online. (Ling, Balci, et.al., 2020). As Zoom filled in notoriety, so too did the pervasiveness of Zoombombing assaults. Now and again, these assaults have had serious outcomes, like the interference of trials or clinical meetings. Zoombombing poses a significant threat to both individuals and organizations. It brings up concerns regarding freedom of speech, security, and privacy. (Chen, Zou, 2023). The rise of Zoombombing has highlighted the significance of user education in preventing such attacks and exposed flaws in the security measures utilized by video conferencing applications. Zoom and other video conferencing applications have taken a number of precautions to stop Zoombombing. For instance, a waiting room feature that lets the host control who enters the meeting was made available by Zoom. They likewise added elements to assist has with overseeing members, for example, the capacity to quiet or eliminate problematic participants. Also, Zoom has expanded its encryption norms to more readily safeguard client information. Regardless of these endeavours, Zoombombing stays a relentless issue, and clients should stay careful to guarantee that their gatherings are secure. (Secara, 2020).

Due of the issue of Zoom bombing, legislatures and associations all over the planet have gone to different lengths. For instance, in March 2020, the Federal Bureau of Investigation (FBI) issued a warning about the possibility of Zoombombing attacks and urged users to take the necessary safety precautions. (Federal Bureau of Investigation, 2020). In April 2020, the Ministry of Home Affairs of India issued an advisory urging all states to prevent Zoom bombing attacks. (Ministry of Home Affairs, 2020). The National Cyber Security Centre (NCSC) in the United Kingdom issued advice on how to protect applications for video conferencing. (NCSC, 2020).

2. PURPOSE AND OBJECTIVES OF THE RESEARCH

- The purpose of this research dwells upon doing a critical study of Zoom bombing especially during the COVID-19 and post this period.
- To evaluate the reasons of Zoom bombing during virtual meetings.
- To assess the current legislative and enforcement mechanisms to combat zoom bombing.
- To analyse the role of Information Technology Act, 2000 to curb the menace of this crime.

3. METHODOLOGY

The methodology adopted for this study is doctrinal in nature. The article revolves around the concept of Zoom bombing which is a cyber crime committed in the cyber space. It focusses upon how this crime found its relevance during the unprecedented wave of COVID-19 pandemic. An in-depth analysis is made as in what are the different stages of committing zoom bombing. We have gathered data from secondary sources in the form of literature review, articles indexed in SCOPUS and Web of Science, websites and newspapers. Some important legislations have also been referred to which are as follows:

- Indian Penal Code, 1860
- Information Technology Act, 2000
- Constitution of India, 1950
- Indian Evidence Act, 1872
- Digital India Bill, 2023

The judgements have been referred to various High Courts of the country and Supreme court of India, from reliable databases of Manupatra and SCC Online. International legislations and provisions have also been referred too in understanding the different nuances and contours of Zoom bombing in the global scenario.

4. RESULTS AND DISCUSSION

Due of the growing usage of software for video conferencing for socialising, education, and business amid the COVID-19 pandemic, the occurrence of Zoom bombing has grown. As a result of the pandemic, individuals all over the globe have been compelled to stay at home, leading to a surge in virtual work and online schooling. During the outbreak of the pandemic, the kind and number of new Zoom users changed substantially in comparison to those for whom the programme was developed. (Turk 2020).

Zoom bombing, or disturbing or interrupting a Zoom chat with unwanted or obscene information, occurs in phases. Zoom bombing is additionally referred to as *"weaponization of Zoom".* (Lorenz and Alba, 2020). These phases may vary depending on the Zoom bombing method used, but they typically consist of the following:

Designing: The person or group involved for the Zoom bombing finds a target Zoom conference by using openly accessible meeting links or by hacking into a Zoom account. They may also think about the type of information they will use to interrupt the meeting.

Access: The zoom bomber gains entry to the Zoom conference via a publicly accessible connection to the meeting or by hacking into a Zoom account. They may also use computer programmes to determine or break the username and password for the meeting.

Disarray: When a zoom bomber obtains entry to a Zoom conference and transmits improper or offensive information, such as images or profanity, this is what happens. They may also utilise screen sharing to display offensive content to all conference attendees.

Escape: After disturbing the meeting, the zoom bomber may try to avoid discovery by swiftly exiting the room or turning off their gadget.

This increased usage has resulted in an increase in the number of Zoom bombing incidents. This type of behaviour can take several forms, such as distributing unambiguous or unfriendly content, producing troublesome clamours, or, in any case, commandeering the meeting. As a result of the COVID-19 pandemic, the Zoom bombing problem has gotten considerably worse. Attackers have more opportunity to interrupt meetings as the percentage of individuals utilising video conferencing software for education and employment grows. Many anti-black and antisemitic student organisations, for example, participate in "Zoom bombing."(Johnson, 2020) in which video calls are invaded in order to engage in unwanted and disruptive intrusions, which frequently climax in verbal attacks. Similarly, people from marginalised or stigmatised groups typically report negative social interactions on social companionship networks. (Meanley, 2020). Furthermore, the unanticipated trend towards remote work and online training has meant that many

organisations may not have had the necessary security measures in place to prevent such attacks. Zoom bombing in Coronavirus has resulted in a variety of outcomes, including the disruption of studies, clinical meetings, and instructional seminars. This type of activity, especially in professional or educational contexts, has the potential to be exceedingly disruptive and distressing. Furthermore, it may result in legal liabilities as well as an invasion of confidentiality and information security. In several cases, the courts have addressed the problem of unauthorised access to virtual meetings. For example, the Gujarat High Court was forced to postpone an online hearing scheduled for September 2020 because one of the participants started playing a song on his cell phone. The incident prompted the Court to issue guidelines for online hearings, which included a need for members to maintain decency during the proceedings. (Sree Sudha, 2023). Similarly, the Karnataka High Court had to postpone a virtual hearing in May 2020 when an unauthorised person accessed the meeting and began playing music. The incident prompted the Court to issue guidelines for conducting virtual hearings, which included the use of secure passwords and the obligation for members to be cautious about unauthorised access. The Information Technology Act, 2000 doesn't criminalise zoom bombing. Zoom bombing has been made as a federal offence in the U.S.A. which can call for an imprisonment. (Statt, 2020).

Some Zoom bombing cases have been decided by court outside of India. In April 2021, for example, a US district judge in California dismissed a lawsuit against Zoom, arguing that the company had failed to adequately safeguard users against Zoom bombing. (Stempel, 2021). Zoom was deemed to be protected by Section 230 of the Communications Decency Act of 1996, which shields online platforms from liability for user-generated material. However, in a news release, the US Attorney's Office for the Eastern District of Michigan declared zoom bombing to be a federal violation in the United States, punishable by fines and imprisonment. (Devereaux, 2020). In another case, a person in the United States was sentenced to 15 years in prison for hacking into Zoom meetings and sending child pornography. (United States Attorney's Office, 2023). The case highlighted the potential dangers of Zoom bombing as well as the need of people and companies adopting the proper security procedures. Although there aren't too many incidents of Zoom bombing, those that have occurred have compelled judges to provide guidelines for conducting virtual meetings, as well as the necessity for individuals and organisations to take essential security steps. As remote work and online education grow more widespread, stakeholders must be wary of the risks of illegal access to virtual meetings.

The legal reaction to zoom bombing in the context of virtual meetings will probably to be based on existing cybercrime and privacy rules. Courts would evaluate whether unauthorised admission into virtual meetings constituted a violation of privacy, unauthorised access, or online harassment. Legal frameworks would be used to determine the scope of culpability for platform providers and people that carry out Zoom bombing attacks.

- ***Laws Concerning Unauthorised Access and Hacking:*** Zoombombing mainly entails gaining access to virtual meetings without authorization. In order to assess whether Zoombombing involves unauthorised access to computer systems, networks, or data, courts would consider current hacking rules and regulations, opening the door for criminal prosecution against the offenders.
- ***Privacy Infractions:*** If sensitive information is compromised, the intrusion into virtual meetings may also cause privacy problems. Courts would determine whether participants in virtual meetings have a legitimate expectation of privacy and whether Zoom bombing violates that expectation. Privacy laws might apply, depending on the jurisdiction.
- ***Cyberbullying and Harassment:*** Cyberbullying or cyber harassment laws may be relevant if the Zoom bombing incident involved the broadcast of offensive, hostile, or explicit content. Courts would consider if Zoom bombers' conduct violates preexisting legislative prohibitions against such behaviour and whether it amounts to online harassment or bullying.
- ***Jurisdictional Issues:*** Since the internet is a worldwide phenomenon, jurisdictional issues frequently arise in cybercrime cases. Attackers who commit zoom bombing may come from other countries, needing law enforcement agency collaboration as well as perhaps using international laws and treaties.
- ***Platform Provider Liability:*** Depending on the circumstances, platform providers such as Zoom may be held accountable for the safety precautions they implement as well as their duty of care to users. Courts can determine whether they took enough efforts to prevent unauthorised access and reduce the possibility of Zoom bombing.
- ***Educational and Workplace Context:*** In situations of Zoom bombing during educational sessions or workplace meetings, courts may examine the educational institutions' or employers' obligation to provide a safe

atmosphere for participants. If it is discovered that the institution did not implement adequate security measures, proceedings may be undertaken against it.

It's important to realise that judicial verdicts might vary substantially based on jurisdiction, local legislation, and the specifics of each case. The rapidly evolving digital world may result in new interpretations of law or legislative changes over time. If cases involving zoom bombing continue to emerge and grow, the legal position on this issue may become clearer, perhaps leading to more specific legal precedents and suggestions. Legal experts, current court cases, and legal news sources should be consulted for the most current and accurate data on judicial stances and legal developments related to zoom bombing.

5. ISSUES AND CHALLENGES

The rise of virtual meetings has brought forth new hazards and concerns that go beyond the convenience they provide, driven by the demands of the digital world and hastened by the COVID-19 pandemic. This paper explores the numerous problems and difficulties brought on by the frightening Zoombombing phenomena, illuminating the complex security and legal considerations it raises in the context of the internet.

- ***Data breaches and privacy invasions:*** Zoombombing assaults invade participants' privacy by inserting unauthorised and frequently offensive content into virtual meetings. The intrusions disclose critical information shared during meetings in addition to disrupting the flow of business. Finding a balance between effortless collaboration and protecting sensitive data is the difficulty.
- ***Regulatory Complexities:*** When prosecuting Zoom bombing offenders, the global scope of the internet creates jurisdictional difficulties. Coordination between law enforcement agencies and legal systems can be challenging because of the possibility that perpetrators operate from other nations. Harmonising legal strategies and creating a clear framework for international cooperation become essential.
- ***Legal Definitions and Frameworks:*** Zoom bombing blurs the distinctions between the term's cybercrime, hacking, harassment, and privacy breaches as they are currently defined by the law. The difficulty lies in modernising established legal frameworks so that they effectively account for the subtleties of disruptions of virtual meetings.
- ***Platform Operator Responsibility:*** Platforms for virtual meetings like Zoom are accountable for maintaining safe environments. Determining the level of responsibility for Zoom bombing instances is difficult. Clarifying the roles of platform providers and meeting planners in relation to user expectations, technology capabilities, and legal requirements is difficult.
- ***Technology Whack-a-Mole:*** As platform providers improve security controls to stop Zoom bombing, criminals adapt and discover new ways to exploit weaknesses. Maintaining a proactive attitude while regularly discovering and addressing new risks while minimising disruptions for authorised users is difficult.
- ***User Awareness and Education:*** Participants run hazards since they are ignorant of security features and appropriate practises. It can be difficult to instruct users on meeting settings, privacy settings, and how to spot possible Zoombombing, especially in circumstances where users have different degrees of technological expertise.
- ***Cultural Sensitivity:*** Content that is offensive and hateful is frequently used in zoom bombing events. Recognising and resolving the cultural quirks that play a role in the motivations behind such attacks is difficult, and doing so will help to ensure that solutions are appropriate and inclusive in a variety of circumstances.
- ***Rapid digital change:*** Rapid changes in the digital environment result in the introduction of new tools and vulnerabilities. Legal frameworks and security protocols must evolve swiftly enough to keep up with new risks, particularly when virtual interactions continue to change communication standards.
- ***Security and Accessibility:*** It might be difficult to strike a balance between maintaining user-friendly accessibility and implementing strong security measures. Overly lax restrictions can exclude legitimate users, while tolerant conditions might leave meetings vulnerable to Zoombombing hazards.

- ***Enforcement and Dissuasion:*** Effective enforcement measures and suitable penalties are needed to successfully prosecute Zoom bombers and discourage additional assaults. But closing loopholes in legal frameworks and punishments that can effectively deter cybercriminals is a difficult task.

Addressing these problems and problems requires a comprehensive strategy that includes legal reforms, technological innovation, education, and international cooperation in the pursuit of secure and fruitful virtual connections. Stakeholders may establish a safer and more durable digital environment for virtual meetings in the digital age by managing these obstacles.

6. RECOMMENDATIONS

The rapidly changing virtual meeting environment need a diverse strategy to combat the growing threat of Zoombombing. Stakeholders can promote safe and effective virtual interactions by addressing legal, technological, and user-oriented issues. The following suggestions are made in this study to lessen the dangers of zoom bombing:

- ***New technologies:*** Zoom bombers are expected to create additional tools and tactics for accessing and stopping Zoom sessions in the future. Zoom bombers' techniques may evolve to circumvent security measures when zoom and other platforms offer new capabilities.
- ***Coordination at global sphere:*** Zoom bombing is a global problem, international cooperation and collaboration may be necessary to fully address it. Sharing information on Zoom bombing incidents and strategies, as well as establishing uniform criteria for avoiding and responding to Zoom bombing, might be part of this.
- ***Legal Consequence:*** **Cybercrime, data protection, intellectual property, and anti-discrimination laws may all be raised by zoom bombing. Individuals and companies who utilise Zoom may be required to manage these legal difficulties and take appropriate procedures in order to avoid legal responsibility.**
- ***User education and awareness campaigns:*** **To avoid Zoom bombing incidents, organisers and participants should get security training and best practises. Users may actively engage in their own online safety if they have simple access to tools that teach how to safeguard meetings.**
- ***Collaborative Research and Development:*** Academic institutions, cybersecurity specialists, and platform providers should collaborate on research to identify future risks and develop innovative responses. This proactive method can help to maintain resilience to Zoom bombing assaults.
- ***User Reviews and Feedback on a Regular Basis:*** Platform providers should encourage users to leave feedback on security features and report any issues they encounter. User feedback is routinely considered, which can result in more efficient security enhancements.
- ***Transparent Reporting Mechanisms:*** Platforms must provide clear methods for reporting Zoom bombing incidents. Rapid responses to reported situations can help prevent additional disruptions and build user trust.
- ***Ethical Hacking and Vulnerability Testing:*** Ethical hackers should be used by organisations to uncover and report problems in their virtual meeting platforms. Regular vulnerability assessments and bug reward schemes may encourage ethical information sharing while also fortifying platform safeguards against potential attacks.

Implementing these suggestions would help stakeholders improve the virtual meeting defences against Zoombombing attacks, fostering a safe and effective digital collaboration environment. Protecting the integrity of virtual interactions in the digital era requires a comprehensive strategy that includes legal reforms, technology advancements, education, and international cooperation.

7. CONCLUSION

The unparalleled connection of the digital era has revolutionised global contact, with virtual meetings emerging as a critical tool. However, the rise in Zoom bombing, a disruptive and destructive practise, raises worries about the integrity of virtual interactions while also revealing serious legal and security loopholes. Beyond traditional boundaries, zoom bombing poses complex legal, technological, and ethical issues. The hazards range from data breaches to jurisdictional issues, affecting platforms, users, and criminals. To address these difficulties, a collaborative approach is required. Platforms must improve security while allowing for user personalization. Governments and international organisations must collaborate to create a worldwide legal framework that ensures collaboration and speedy action

against criminals. Education efforts that equip users to safeguard virtual areas, spot Zoom bombing indicators, and respond successfully are critical. Promoting cultural sensitivity and appropriate behaviour reduces the spread of offensive information. Adaptability is essential in the ever-changing digital world. Continuous monitoring and research are required in the ongoing race between innovation and harmful methods. Ethical hacking and expert cooperation can deliver cutting-edge insights into dangers. To address the threats of Zoom bombing, a secure digital environment for virtual meetings is required. By embracing proactive security and implementing proposed solutions, stakeholders may prevent Zoom bombing and design a future in which virtual relationships can flourish unfettered. Addressing legal and security problems collectively will determine whether virtual meetings remain a smooth connectivity hub or fall victim to intrusion as the digital era advances.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Bercovitz. (2020, April 20). Prosecuting Zoom-bombing. Lawfare.

Secara. (2021, November 3). Zoombombing – the end-to-end fallacy. https://doi.org/10.1016/S1353-4858(20)30094-5

Mahr., Cichon., Mateo., Grajeda., Baggili. (2021, January 23). Zooming into the pandemic! A forensic analysis of the Zoom Application. University of New Haven. https://core.ac.uk/download/pdf/477677914.pdf

Charles H. Li, Anandh G. Rajamohan, Patricia T. Acharya, Chia-Shang J. Liu, Vishal Patel, John L. Go, Paul E. Kim, Jay Acharya, (2020, June). Why Zoom Is Not Doomed Yet: Privacy and Security Crisis Response in the COVID-19 Pandemic. ELSEVIER. https://escholarship.org/content/qt4hr8h49s/qt4hr8h49s_noSplash_e869e1c0ab8661273ab2570ef659c1d2.pdf

Siddiqui., Ahmad. (2023, February 23). Zoombombing: causes and preventions. E3S Web Conf. https://doi.org/10.1051/e3sconf/202337105026

Linda C. Chu., Anima Anandkumar., Hoo Chang Shin., Elliot K. Fishman. (2020, April 17). The Potential Dangers of Artificial Intelligence for Radiology and Radiologists. Journal of American College of Radiology. https://doi.org/10.1016/j.jacr.2020.04.010

Simeon Vidolov. (2022, March 4). Uncovering the affective affordances of videoconference technologies. Discover Journals, Books & Case Studies | Emerald Insight. https://www.emerald.com/insight/content/doi/10.1108/ITP-04-2021-0329/full/html

Xinyu Hua., Kathryn E. Spier. (2022, March 20). Holding Platforms Liable. TSE | Toulouse School of Economics. https://www.tse-fr.eu/sites/default/files/TSE/documents/sem2022/eco_platforms/spier.pdf

Riana Pfefferkorn. (2020, May 11). Client-side scanning and Winnie-the-Pooh Redux (Plus some thoughts on Zoom). Center for Internet and Society | The Center for Internet and Society is a leader in the study of the law & policy around the Internet & emerging technologies. https://cyberlaw.stanford.edu/blog/2020/05/client-side-scanning-and-winnie-pooh-redux-plus-some-thoughts-zoom

Andrés Martin., Jillian Celentano., Christy Olezeski., Justin Halloran., Brent Penque., Jemel Aguilar., Doron Amsalem. (2022, December 26). Collaborating with transgender youth to educate healthcare trainees and professionals: Randomized controlled trial of a didactic enhanced by brief videos. BioMed Central. https://doi.org/10.1186/s12889-022-14791-5

Sharon Mistretta. (2022, March 28). The Metaverse—An alternative education space. IntechOpen - Open Science Open Minds | IntechOpen. https://www.intechopen.com/journals/1/articles/87

Schwarz, Marius; Scherrer, Aline; Hohmann, Claudia; Heiberg, Jonas; Brugger, Andri; Nuñez-Jimenez, Alejandro. (2020, June 30). COVID-19 and the Academy: It is time for going digital - Research collection. ETH Zurich. https://doi.org/10.3929/ethz-b-000425393

Debarati Halder, K. Jaishankar. (2011, January). Cyber crime and the victimization of women: Laws, rights and regulations. IGI Global: International Academic Publisher. https://www.igi-global.com/book/cyber-crime-victimization-women/50518

K. Jaishankar. (2007, July). Establishing a Theory of Cyber Crimes. International JournalofCyberCriminology. https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf

Ranjan, Radha. Singh Pallavi (2023). Cyber Crime Against Women In Cyber Space: A Critical Analysis of Indian Legislations. Kanpur Philosopher UGC CARE Listed Journal, ISSN No- 2348-8301., 10(1(A), 79–85.

Ayşe Okutan., Yalçın Çebi. (2019). A Framework for Cyber Crime Investigation.ProcediaComputerScience. https://doi.org/10.1016/j.procs.2019.09.054

Mihail Antonica., Ramona Birău. (2015). Financial and non-financial implications of cybercrimes in emerging countries. ELSEVIER. https://10.1016/S2212-5671(15)01440-9

Ranjan, Radha, Singh Pallavi (2022). Sexual Harassment of Women At Work Place: A Study of Indian Legislation And Judicial Approach. Indian Journal of Law and Legal Research, UGC Approved Journal ISSN: 2582-8878.

Cecelia Horan.,Hossein Saiedian. (2021, September 30). Cyber crime investigation: Landscape, challenges, and future research directions. MDPI. https://doi.org/10.3390/jcp1040029

Kristopher Kaliebe. (2017, October). New Technologies, New Laws, New Childhood. Journal of the American Academy of Child & Adolescent Psychiatry Home. https://doi.org/10.1016/j.jaac.2017.07.049

Paul Arnell., Bukola Faturoti. (2022, June 8). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology. https://doi.org/10.1080/13600869.2022.2061888