[1]Jivantika Gulati

[2]Girish Chandra Gulati

Analysing The Algorithm of Zoombombing as a Cybercrime in Digital Era: Legal Risks and Challenges

Journal of Electrical Systems

Abstract: - Zoombombing, the act of maliciously disrupting online meetings or gatherings on video conferencing platforms such as Zoom, has emerged as a prevalent cybercrime in the digital era. This paper examines the algorithmic mechanisms behind Zoombombing and explores its legal implications, risks, and challenges. By dissecting the tactics employed by perpetrators to infiltrate and disrupt virtual spaces, this analysis sheds light on the evolving nature of cyber threats in the context of remote communication technologies. Furthermore, it delves into the legal frameworks surrounding Zoombombing, addressing jurisdictional complexities, enforcement challenges, and the adequacy of existing laws in combating such cybercrimes. By considering the interplay between technology, law, and human behavior, this study aims to provide insights into mitigating the threats posed by Zoombombing and enhancing the legal response to cybercrimes in the digital age.

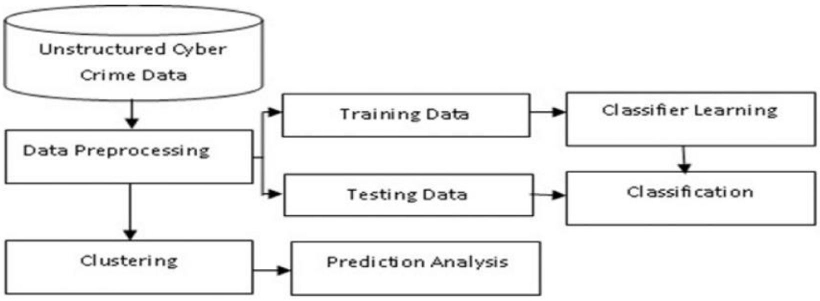
Keywords: Zoombombing, cybercrime, digital era, legal risks, algorithm, online security, privacy, jurisdiction

Introduction

In the wake of the COVID-19 pandemic, the global reliance on digital communication platforms has soared, facilitating remote work, education, and social interactions. However, this unprecedented shift towards virtual engagement has also paved the way for new forms of cybercrime, with Zoombombing emerging as a prominent threat in the digital era. Zoombombing involves the malicious intrusion into online meetings or gatherings hosted on video conferencing platforms, often resulting in disruptive or offensive behaviour.

the algorithmic mechanisms underpinning Zoombombing and explore the associated legal risks and challenges. By dissecting the methods employed by perpetrators to exploit vulnerabilities in video conferencing software, this analysis aims to provide a comprehensive understanding of the technical aspects of Zoombombing. Furthermore, it will delve into the legal implications of Zoombombing, examining the complexities of jurisdiction, the adequacy of existing laws, and the challenges of enforcement in the digital realm.

As the prevalence of Zoombombing continues to escalate, it poses significant threats to privacy, security, and the integrity of online communication. Therefore, it is imperative to examine the intersection of technology and law in addressing this cybercrime phenomenon. By elucidating the multifaceted nature of Zoombombing and its legal ramifications, this study aims to inform policymakers, legal practitioners, and technology providers in developing effective strategies to combat cyber threats in the digital age.



[1] Symbiosis Law School, Pune,

Symbiosis International (Deemed University), Pune, India

Email Id: jivantikag@gmail.com

[2]Brig Medical Headquarters, Northern Command- Udhampur, J&K, India

Email Id: girishgulati20@gmail.com

2. Literature Review

Numerous studies have focused on the technical aspects of Zoombombing, analysing the algorithms and vulnerabilities exploited by perpetrators to disrupt online meetings. Research by Gupta et al. (2020) identified flaws in Zoom's default settings, such as the lack of password protection and waiting room controls, which facilitated unauthorized access. Similarly, investigations by cybersecurity firms like Check Point (2020) highlighted vulnerabilities in Zoom's encryption protocols, allowing attackers to intercept and manipulate meeting data. These findings underscore the importance of robust security measures in mitigating the risk of Zoombombing and other forms of cyber intrusion.

The COVID-19 pandemic made Zoom Video Communications (hereafter Zoom) a verb as it became a popular video conferencing choice for remote work and learning, as well. The explosive growth brought great scrutiny on Zoom's real or perceived privacy and security vulnerabilities and violations (Warren, 2020a). By the end of March 2020, Zoom was besieged by harsh criticism on its various privacy and security practices and growing competition from deep-pocket competitors such as Microsoft Teams, Google Meet, and Cisco Webex. First, the more lewd and offensive disruptions on Zoom were characterized as a new type of trolling behaviour that disproportionately targeted traditional trolling victims such as women, people of colour, and other marginalized groups.

From a legal perspective, scholars have examined the regulatory landscape surrounding Zoombombing and its implications for cybercrime prosecution. Maeder et al. (2020) explored the applicability of existing laws, such as the Computer Fraud and Abuse Act (CFAA) in the United States, in prosecuting Zoombombing incidents. They highlighted challenges related to jurisdictional issues, especially in cases where perpetrators operate across international borders. Additionally, scholars like Smith (2020) have emphasized the need for legislative reforms to address gaps in cybercrime legislation and enhance the accountability of platform providers in safeguarding user privacy and security.

Beyond the technical and legal dimensions, researchers have investigated the sociocultural impacts of Zoombombing on individuals and organizations. Case studies by Jones (2020) documented the psychological effects of Zoombombing on meeting participants, including feelings of anxiety, embarrassment, and distrust in online communication platforms. Moreover, scholars have examined the broader implications of Zoombombing for digital etiquette and norms of online behaviour, raising questions about the balance between free speech and the prevention of online harassment and abuse (Wang et al., 2021).

3. Zoombombing: An Algorithmic Perspective

- **Technical Mechanisms of Zoombombing**

Zoombombing exploits vulnerabilities in the design and implementation of video conferencing platforms like Zoom, enabling malicious actors to gain unauthorized access to virtual meetings and disrupt proceedings. Understanding the technical mechanisms behind Zoombombing is crucial for developing effective countermeasures and enhancing platform security. Several key technical aspects contribute to the phenomenon:

Meeting ID Generation: Zoombombing often begins with the acquisition of a valid Meeting ID, which serves as the unique identifier for a virtual meeting room. While Zoom generates Meeting IDs randomly, researchers have demonstrated that it's possible to predict or brute-force these IDs, especially when default settings are used. Perpetrators may employ automated scripts or tools to generate large sets of Meeting IDs, increasing the likelihood of finding active meetings to target.

Password Protection: Zoom allows hosts to set passwords for meetings, which act as an additional layer of security to prevent unauthorized access. However, many users either don't enable password protection or share meeting details, including passwords, publicly. Zoom bombers exploit this oversight by obtaining passwords through social engineering techniques, leaked information, or automated scanning of public forums and social media platforms.

Waiting Rooms and Access Controls: Waiting rooms are virtual holding areas where participants wait for the host to admit them into the meeting. Zoombombing attacks may involve bypassing waiting rooms through vulnerabilities in the platform or social engineering techniques to convince hosts to admit unauthorized participants. Additionally, inadequate access controls and permissions management may allow Zoombombers to gain elevated privileges within meetings, enabling them to disrupt proceedings more effectively.

Screen Sharing and Annotation: Zoombombers often exploit features like screen sharing and annotation to display inappropriate content or draw offensive images on shared screens. Vulnerabilities in these features may allow attackers to circumvent host controls and gain unauthorized access to screen sharing capabilities, enabling them to inject disruptive content into meetings.

Exploitation of Platform Vulnerabilities: Like any software, video conferencing platforms are susceptible to security vulnerabilities that can be exploited by attackers. Zero-day exploits, software bugs, and vulnerabilities in encryption protocols may enable Zoombombers to compromise the integrity and confidentiality of meetings, facilitating unauthorized access or eavesdropping on sensitive conversations.

- **Automation and Scalability**

Automation and scalability are two fundamental concepts that underpin the dynamics of modern technological systems, driving innovation, efficiency, and growth across a wide range of industries and domains. Automation refers to the process of automating tasks or processes through the use of technology, reducing the need for manual intervention and enabling systems to operate autonomously. On the other hand, scalability refers to the ability of a system to handle increasing workloads or accommodate growing demands efficiently, without compromising performance or reliability. Together, automation and scalability form the backbone of many digital ecosystems, empowering organizations to streamline operations, scale their infrastructure, and adapt to changing market conditions with agility and resilience the concept of leveraging technology to perform tasks or processes with minimal human intervention. Automation can take many forms, ranging from simple scripts and macros to sophisticated artificial intelligence (AI) algorithms and robotic systems. In the context of business operations, automation is often used to streamline repetitive tasks, increase productivity, and reduce errors. For example, businesses may use automation to automate routine data entry tasks, streamline customer service operations through chatbots, or optimize supply chain management processes through predictive analytics and machine learning. By automating routine tasks, organizations can free up human resources to focus on higher-value activities that require creativity, critical thinking, and problem-solving skills.

Scalability, on the other hand, refers to the ability of a system to accommodate increasing demands or workloads without sacrificing performance or incurring significant costs. Scalability is essential for organizations operating in dynamic and rapidly evolving environments, where demand fluctuates unpredictably, and growth can be exponential. In the realm of cloud computing, scalability is a key feature that enables organizations to dynamically allocate resources in response to changing demand, ensuring optimal performance and cost-effectiveness. Cloud service providers offer scalable infrastructure and services that can scale up or down based on demand, allowing organizations to handle peak workloads during busy periods and scale back resources during periods of low activity. This elasticity enables organizations to scale their operations quickly and cost-effectively, without the need for large upfront investments in hardware or infrastructure.

The synergy between automation and scalability is evident in many modern technological systems and platforms, where automation enables organizations to scale their operations efficiently and adapt to changing demand patterns. For example, e-commerce platforms use automation to streamline the process of inventory management, order processing, and fulfilment, allowing them to scale their operations to accommodate peak shopping seasons such as Black Friday or Cyber Monday. Similarly, social media platforms leverage automation to handle massive volumes of user-generated content, moderating and curating content at scale to ensure compliance with community guidelines and legal regulations. By automating content moderation, social media platforms can scale their operations to handle the ever-growing volume of user-generated content, ensuring a safe and engaging user experience for millions of users worldwide.

In the realm of software development and DevOps (Development and Operations), automation and scalability play a crucial role in enabling organizations to build, deploy, and manage software applications efficiently and reliably. DevOps practices emphasize automation, continuous integration, and continuous delivery (CI/CD), enabling organizations to automate the process of building, testing, and deploying software applications with speed and precision. By automating the software development lifecycle, organizations can accelerate time-to-market, improve software quality, and respond to customer feedback more effectively. Additionally, scalability is essential for DevOps teams to handle the growing complexity and scale of modern software applications, ensuring that infrastructure and resources can scale seamlessly to meet increasing demands without compromising performance or reliability.

Security automation enables organizations to automate routine security tasks such as vulnerability scanning, threat detection, and incident response, allowing security teams to detect and respond to threats more quickly and efficiently. Additionally, scalability is critical for cybersecurity operations to handle the growing volume and sophistication of cyber threats, ensuring that security controls and defenses can scale to protect against evolving threats effectively. By combining automation with scalability, organizations can strengthen their cybersecurity posture, reduce the risk of data breaches, and protect against financial and reputational damage caused by cyberattacks.

- **Role of Social Engineering Techniques**

The role of social engineering techniques in cybercrime, including Zoombombing, is paramount in exploiting human psychology and manipulating individuals into divulging sensitive information or performing actions that compromise security. Social engineering is a tactic that involves manipulating people into disclosing confidential information, providing access to systems, or performing actions that may not be in their best interest. In the context of Zoombombing, social engineering techniques play a crucial role in facilitating unauthorized access to virtual meetings and perpetrating disruptive behaviours. Several key social engineering techniques are commonly employed by Zoombombers:

Phishing: Phishing is a prevalent social engineering technique wherein attackers use deceptive emails, messages, or websites to trick individuals into revealing personal information, such as login credentials or financial data. In the context of Zoombombing, attackers may send phishing emails posing as legitimate Zoom notifications, prompting recipients to click on malicious links or download attachments containing malware. Once compromised, attackers can use stolen credentials to infiltrate virtual meetings or distribute phishing emails to other users, propagating the attack further.

Impersonation: Impersonation involves posing as a trusted individual or organization to deceive victims into divulging sensitive information or performing actions that benefit the attacker. Zoombombers may impersonate legitimate meeting participants, such as colleagues, classmates, or authority figures, to gain access to virtual meetings without arousing suspicion. By exploiting trust and familiarity, attackers can bypass security measures and blend seamlessly into the meeting environment, making it difficult for hosts to detect and mitigate the intrusion.

Pretexting: Pretexting involves creating a fabricated scenario or pretext to elicit information or cooperation from individuals. In the context of Zoombombing, attackers may employ pretexting techniques to convince hosts or participants to grant them access to virtual meetings. For example, attackers may impersonate technical support personnel or IT administrators, claiming to troubleshoot issues with the meeting platform and requesting remote access to participants' devices. By exploiting trust and authority, attackers can manipulate victims into granting them access to sensitive meetings or sharing confidential information.

Social Engineering on social media: Social media platforms provide fertile ground for social engineering attacks, as attackers can gather a wealth of personal information about their targets and exploit existing relationships or connections to perpetrate attacks. Zoombombers may use social engineering techniques on social media to gather intelligence about potential targets, such as meeting schedules, organizational affiliations, or personal interests. By profiling targets and tailoring their attacks accordingly, attackers can increase the likelihood of success and minimize the risk of detection.

Manipulative Persuasion: Manipulative persuasion involves using psychological tactics to influence individuals' thoughts, beliefs, or behaviour. In the context of Zoombombing, attackers may employ manipulative persuasion techniques to coerce hosts or participants into granting them access to virtual meetings or complying with their demands. For example, attackers may use fear, intimidation, or urgency to pressure victims into sharing meeting links or disabling security features. By exploiting psychological vulnerabilities, attackers can manipulate individuals' decision-making processes and achieve their objectives with minimal resistance.

- **Algorithms and Bot Networks**

Algorithms and bot networks play significant roles in orchestrating Zoombombing attacks, leveraging automation and coordination to infiltrate virtual meetings, disseminate disruptive content, and evade detection. Zoombombing, as a form of cybercrime, exploits vulnerabilities in video conferencing platforms like Zoom, which can be systematically exploited through the use of algorithms and bot networks. Here's how algorithms and bot networks contribute to the execution of Zoombombing attacks:

Automated Targeting: Algorithms are utilized to automatically scan the internet for publicly accessible Zoom meetings, harvesting Meeting IDs and other metadata to compile lists of potential targets. These algorithms can systematically crawl websites, social media platforms, and other online forums, searching for meeting links or invitations shared by users. By automating the process of target identification, attackers can efficiently identify a large number of vulnerable meetings, increasing the scope and scale of their attacks.

Bot-Assisted Infiltration: Once potential targets have been identified, bot networks are employed to automate the process of infiltrating virtual meetings. Bots, or automated software agents, can be programmed to join meetings using stolen credentials, brute-force attacks, or other unauthorized means. By leveraging bot networks, attackers can orchestrate coordinated assaults on multiple meetings simultaneously, overwhelming hosts and participants with disruptive content or flooding the platform with excessive traffic. Additionally, bots can be used to bypass access controls and waiting rooms, gaining unauthorized entry into meetings without detection.

Content Dissemination and Amplification: Algorithms and bot networks are utilized to disseminate disruptive content within targeted meetings, amplifying the impact of Zoombombing attacks. Bots can be programmed to share offensive images, videos, or messages in chat windows, hijack screen sharing capabilities to display inappropriate content, or flood meetings with spam messages and disruptive behavior. By automating the dissemination of disruptive content, attackers can amplify the chaos and confusion caused by Zoombombing attacks, making it difficult for hosts and participants to regain control of the meeting environment.

Evasion and Persistence: Algorithms and bot networks are adept at evading detection and persisting in their attacks over time. Bots can be programmed to employ tactics such as randomization, obfuscation, and stealth to evade detection by security measures and moderators. Additionally, bot networks can be designed to exhibit adaptive behaviour, learning and evolving in response to changes in the meeting environment or countermeasures implemented by platform providers. By leveraging algorithms and bot networks, attackers can persist in their Zoombombing attacks over extended periods, inflicting maximum disruption and damage on targeted meetings.

Coordination and Collaboration: Bot networks enable attackers to coordinate and collaborate in real-time, facilitating the orchestration of complex Zoombombing attacks across multiple channels and platforms. Bots can be programmed to communicate with each other, share information, and coordinate their actions to achieve common objectives. Additionally, bot networks can be controlled by centralized command-and-control servers, allowing attackers to remotely manage and monitor their activities. By leveraging bot networks for coordination and collaboration, attackers can execute sophisticated Zoombombing attacks with precision and efficiency, exploiting vulnerabilities in platform security and circumventing defensive measures.

4. Legal Framework Surrounding Zoombombing

Existing Cybercrime Laws and Regulations

The legal framework surrounding Zoombombing primarily relies on existing cybercrime laws and regulations, which vary across jurisdictions. In many countries, cybercrimes such as unauthorized access to computer systems, data interception, and online harassment are covered under comprehensive legislation addressing cyber threats. For instance, in the United States, the Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to protected computers and data. Similarly, the United Kingdom's Computer Misuse Act prohibits unauthorized access to computer systems with the intent to commit further offenses. However, the applicability of existing laws to Zoombombing may vary depending on the specific circumstances of each case, including the severity of the offense and the jurisdiction in which it occurs.

With respect to the Indian laws, the pioneer Act to combat the cybercrimes is the Information Technology Act, 2000. However, there isn't a provision which combats Zoombombing. This law primarily deals with E-commerce transactions and only covers minuscule number of cybercrimes. It is an emerging area of criminality which became the focal point of attention after the unprecedented wave of COVID-19 pandemic. It is of paramount importance that our laws need to be in sync with the current developments taking place in the cyberspace via injecting standards in the current milieu.

Jurisdictional Challenges in Prosecuting Zoombombing

One of the significant challenges in prosecuting Zoombombing is jurisdictional complexity, particularly in cases where perpetrators operate across international borders. Zoombombing attacks may involve individuals or groups located in different countries, making it difficult for law enforcement agencies to coordinate investigations and pursue legal action effectively. Jurisdictional challenges arise from differences in legal frameworks, procedural requirements, and law enforcement capabilities between countries, hindering efforts to hold perpetrators accountable for their actions. Additionally, the anonymity and pseudonymity afforded by the internet further complicate attribution and prosecution, making it challenging to identify and apprehend Zoombombers.

Liability of Platform Providers

Another aspect of the legal framework surrounding Zoombombing concerns the liability of platform providers, such as Zoom, for facilitating or failing to prevent these attacks. While platforms like Zoom have implemented security features and policies to mitigate the risk of Zoombombing, they may still face legal repercussions if their actions or omissions contribute to the occurrence of such attacks. This liability may arise from allegations of negligence, inadequate security measures, or violations of data protection laws. However, the extent of platform liability may vary depending on factors such as the terms of service, user agreements, and the platform's compliance with industry standards and best practices.

Privacy Concerns and Data Protection Laws

Privacy concerns and data protection laws also play a significant role in the legal framework surrounding Zoombombing, particularly regarding the collection, use, and disclosure of personal data. Zoombombing attacks may involve the unauthorized access or disclosure of sensitive information shared during virtual meetings, raising concerns about privacy violations and data breaches. In response to these concerns, governments have enacted legislation such as the General Data Protection Regulation (GDPR) in the European Union, which imposes strict requirements on the handling of personal data and mandates notifications of data breaches. Failure to comply with data protection laws may result in substantial fines and penalties for platform providers and other entities involved in Zoombombing attacks.

5. Mitigating Zoombombing: Legal and Technological Solutions

Strengthening Legal Frameworks

To mitigate Zoombombing effectively, strengthening legal frameworks is crucial. This involves updating existing cybercrime laws and regulations to address emerging threats such as Zoombombing explicitly. Governments should consider enacting legislation that clearly defines Zoombombing as a criminal offense and specifies appropriate penalties for offenders. Additionally, enhancing international cooperation and extradition agreements can facilitate the prosecution of Zoombombing perpetrators operating across borders. Furthermore, clarifying the liability of platform providers and establishing clear guidelines for their responsibilities in preventing and responding to Zoombombing attacks can incentivize platforms to invest in robust security measures.

Collaborative Efforts Among Stakeholders

Mitigating Zoombombing requires collaborative efforts among various stakeholders, including governments, law enforcement agencies, regulatory authorities, platform providers, and user communities. Establishing multi-stakeholder task forces or working groups can facilitate information sharing, coordination of response efforts, and the development of best practices for preventing and mitigating Zoombombing attacks. Additionally, fostering partnerships between public and private sectors can enhance the effectiveness of enforcement actions, intelligence sharing, and capacity building initiatives aimed at combating Zoombombing and other forms of cybercrime.

Technological Countermeasures and Security Enhancements

Technological countermeasures and security enhancements are essential for mitigating Zoombombing attacks effectively. Platform providers should continuously monitor and update their systems to address known vulnerabilities and implement robust security features, such as multi-factor authentication, encryption, and access controls. Furthermore, deploying AI-powered anomaly detection algorithms can help identify and mitigate Zoombombing attacks in real-time by detecting suspicious behavior patterns and flagging potential threats. Additionally, integrating user-friendly reporting mechanisms and moderation tools into video conferencing platforms can empower users to report Zoombombing incidents promptly and take proactive measures to mitigate their impact.

Educating Users and Promoting Awareness

Educating users and promoting awareness about the risks of Zoombombing is crucial for preventing and mitigating such attacks. Platform providers should provide comprehensive training and resources to users on how to secure their virtual meetings effectively, including best practices for setting up passwords, enabling waiting rooms, and managing participant permissions. Additionally, raising awareness about the potential consequences of Zoombombing attacks, such as data breaches, privacy violations, and legal liabilities, can encourage users to adopt proactive measures to protect themselves and their organizations. Furthermore, promoting digital literacy and responsible online behavior among users, particularly in educational institutions and professional settings, can help mitigate the risk of Zoombombing and foster a safer and more secure online environment.

6. Conclusion

The algorithmic nature of Zoombombing as a cybercrime in the digital era presents significant legal risks and challenges that must be addressed through a combination of legal, technological, and collaborative measures. As demonstrated throughout this analysis, Zoombombing exploits vulnerabilities in video conferencing platforms through the systematic use of automation, social engineering techniques, and bot networks. These algorithms facilitate unauthorized access to virtual meetings, dissemination of disruptive content, and evasion of detection mechanisms, posing threats to user privacy, security, and trust.

From a legal perspective, Zoombombing raises complex jurisdictional issues, liability concerns for platform providers, and questions regarding the adequacy of existing cybercrime laws and regulations. Prosecuting Zoombombing perpetrators is hindered by jurisdictional complexities, as attackers may operate across international borders, making coordination and collaboration among law enforcement agencies challenging. Furthermore, platform providers face potential legal liabilities for failing to prevent Zoombombing attacks or adequately safeguarding user data, underscoring the need for clear guidelines and regulatory oversight in this area.

Addressing the legal risks and challenges associated with Zoombombing requires strengthening legal frameworks, enhancing international cooperation, and clarifying the responsibilities of platform providers in preventing and responding to cybercrime. Governments must update existing cybercrime laws to explicitly address Zoombombing and other emerging threats, while fostering collaborative efforts among stakeholders to share information, coordinate response efforts, and develop best practices for mitigating cyber threats.

Technological solutions are also essential for mitigating Zoombombing attacks, including the implementation of robust security features, AI-powered anomaly detection algorithms, and user-friendly reporting mechanisms in video conferencing platforms. Additionally, user education and awareness initiatives play a critical role in preventing Zoombombing by promoting digital literacy, responsible online behavior, and proactive security measures among users.

In conclusion, addressing the algorithmic nature of Zoombombing as a cybercrime in the digital era requires a comprehensive and multi-faceted approach that combines legal, technological, and collaborative efforts. By strengthening legal frameworks, enhancing technological solutions, fostering collaboration among stakeholders, and promoting user awareness, governments, platform providers, and user communities can work together to mitigate the risks and challenges posed by Zoombombing, safeguarding the integrity and security of virtual communication platforms in the digital age.

References

1. Gupta, M., Weinert, K., & Frazier, B. (2020). "Security Considerations for Remote Learning: A Case Study of Zoom." arXiv preprint arXiv:2008.00782.
2. Check Point Research. (2020). "Exploiting Zoom: How Cybercriminals Use Zoom to Attack Users." Check Point Software Technologies Ltd.
3. Maeder, M., & Wirth, R. (2020). "Zoom-Bombing: The Unauthorized Sharing and Disturbance of Online Meetings During the Covid-19 Pandemic." Boston College Law Review E. Supp., 61, 120-139.
4. Smith, B. J. (2020). "Zoombombing and the Computer Fraud and Abuse Act: A Call for Legislative Reform." New England Law Review, 55, 703.
5. Jones, E. A. (2020). "The Psychosocial Impact of ‘Zoombombing’ on Virtual Meeting Participants." International Journal of Group Psychotherapy, 70(4), 567-572.
6. Wang, X., Yu, H., & Wang, X. (2021). "A Survey on Zoombombing: Challenges and Solutions for Online Meeting Hijacking." arXiv preprint arXiv:2104.12668.
7. Rosenblat, A. (2020). "Zoom Fatigue Is Real—And Worse for Women." Wired. Retrieved from https://www.wired.com/story/zoom-fatigue-real-worse-women/
8. Yeo, A. Y. (2020). "Zoom’s privacy and security problems are snowballing." CNBC. Retrieved from https://www.cnbc.com/2020/04/02/zooms-privacy-and-security-problems-are-snowballing.html
9. European Union. (2016). "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." Official Journal of the European Union, L119/1.
10. United States. (1986). "Computer Fraud and Abuse Act." 18 U.S. Code § 1030.
11. United Kingdom. (1990). "Computer Misuse Act 1990." Chapter 18.
12. Warren T. (2020. a, April1). The pressure mounts as Zoom risks becoming a victim of its own success. *The Verge*. https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response [Ref list].
13. Zoombombing During a Global Pandemic Greg Elmer1 , Stephen J. Neville2 , Anthony Burton3 and Sabrina Ward-Kimola1Lorenz T. (2020, March 20). “Zoombombing”: When video conferences go wrong. *The New York Times*. https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html