DATA PROTECTION AND PRIVACY ISSUES SURROUNDING ZOOMBOMBING

TABLE OF CONTENT

1. INTRODUCTION
2. DEFINING ZOOMBOMBING
3. INCIDENTS OF ZOOMBOMBING
4. DATA PROTECTION AND PRIVACY ISSUES
4.1 THE LEGAL FRAMEWORK OF DATA PRIVACY AND PROTECTION LAWS IN NIGERIA
5. LIABILITY FOR ZOOMBOMBING IN NIGERIA
5.1 LIABLITY AND PUNISHMENTS AVAILABLE FOR THE OFFENCE OF ZOOM BOMBING
5.2 LIABILITY OF CORPORATE BODIES FOR THE OFFENCE OF ZOOMBOMBING IN NIGERIA
6. MEANS OF PREVENTING ZOOMBOMBING
7. CONCLUSION

LIABILITY OF CORPORATE BODIES FOR THE OFFENCE OF ZOOMBOMBING IN NIGERIA

It is no news that a person that commits an offence is liable for such offence. It follows therefore that if a corporate body intentionally neglects it's responsibilities in preventing the incidence of Zoom bombing, it can therefore be held liable for such offence. Also, if such body commits the offence of zoom bombing itself, it shall be held liable.

INTRODUCTION

- The world is technologically advancing in a fast pace, and this results in seemless internet possibilities.
- Remote workplaces, teleconferencing, amongst others, have created a new normal - ‘ a virtual world’
- Zoom is a commonly used app for various businesses and institution, it's unprecedented surge has presented with it certain security and privacy issues which had not been attended to or prioritized prior to this global digital shift, one of which is the issue of "Zoombombing".

DEFINING ZOOMBOMBING

According to Wikipedia, Zoombombing or Zoom raiding refers to the unwanted, disruptive intrusion, generally by Internet trolls, into a video-conference call. In a typical Zoombombing incident, a teleconferencing session is hijacked by the insertion of material that is lewd, obscene, racist, homophobic, or antisemitic in nature, typically resulting in the shutdown of the session.

INCIDENTS OF ZOOMBOMBING

There are a plethora of reported cases of Zoombombing, globally. However, here's a few of them;

- Chipotle, (an American chain of fast casual restaurants) was forced to end a public Zoom chat that the brand had co-hosted with the musician Lauv after one participant began broadcasting pornography to hundreds of attendees.
- Journalists Kara Swisher and Jessica Lessin hosted a Zoom event focused on the challenges women tech founders face. They were forced to abruptly end the event after just 15 minutes of conversation after a participant began broadcasting pornographic content while switching between different user accounts in order to avoid being blocked.

DATA PROTECTION AND PRIVACY ISSUES

- Risk to Users: The interception of meeting links and passwords allows unauthorized individuals to execute automated attacks.
- Sharing of Personal Data: This began in March 2020, and no hint was given in Zoom's privacy policy. Zoom has reacted to criticism with an update which disabled this data sharing.
- - Inefficient Security Systems: Journalists discovered that Zoom had its own definition of "end-to-end encryption." Zoom later apologized for making misleading statements about its encryption methods and provided insight into the actual encryption methods it uses.
- Drastic Control Mechanism: Zoom's "attendee attention tracker" led to a controversy that has arisen over what has been called a drastic control mechanism, this feature has been disabled
- Some organizations have banned the use of zoom, including; Google, SpaceX, Smart Communications, NASA, Australian Defence Force, The New York City Department of Education.
- S 37 of the 1999 CFRN gurantees a right to privacy to all Nigerian citizens. Also, in **Godfrey Nya Eneye v MTN Nigeria Communication Ltd,** the court ruled against a breach of right to privacy.

LEGAL FRAMEWORK OF DATA PRIVACY AND PROTECTION LAWS IN NIGERIA

- The 1999 CFRN: Section 37 of Nigeria's 1999 constitution forms the foundation of data privacy rights and protection in Nigeria.
- Nigeria Data Protection Regulation (NDPR) 2019: The NDPR is a subsidiary legislation. It is the major law specifically aimed at addressing data privacy and protection in Nigeria
- The Freedom of Information Act 2011 : Section 14 of the Freedom of Information Act protects personal data. It restricts the disclosure of information which contains personal information by public institutions except where the involved data subject consents to its disclosure or where the information is publicly available.
- The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 : This Act is Nigeria's

LIABILITY FOR ZOOM BOMBING IN NIGERIA

- Section 6(1) of the Cyber crime Act, 2015
- Section 7 of the Cyber crime Act, 2015
- Section 9 of the Cyber crime Act, 2015.

The provision of the above legislation all sum up to the end that, zoom bombing as it poses a threat to data privacy and security, is a criminal offence in Nigeria.

LIABLITY AND PUNISHMENTS AVAILABLE FOR THE OFFENCE OF ZOOM BOMBING

Having established the fact that zoom bombing is an offence in Nigeria, what punishments are available for the offence of zoom bombing?

- Cybercrime Act, 2015 makes provision for, imprisonment for a term of not less than two years or to a fine of not less than N5,000,000 or to both fine and imprisonment, for offences such as Zoombombing.
- Other enactments on the punishment for zoom bombing and other cyber crimes include;
- Section 7 of the Cybercrimes Act, 2015, Section 9 of the Cybercrimes Act, 2015.

LIABILITY OF CORPORATE BODIES FOR THE OFFENCE OF ZOOMBOMBING IN NIGERIA

It is no news that a person that commits an offence is liable for such offence. It follows therefore that if a corporate body intentionally neglects it's responsibilities in preventing the incidence of Zoom bombing, it can therefore be held liable for such offence. Also, if such body commits the offence of zoom bombing itself, it shall be held liable.

MEANS OF PREVENTING ZOOMBOMBING

- Application Update
- Never use your personal zoom ID
- Disabling the share file feature
- Always set a meeting password
- Kick someone out or put them on hold
- Use Zoom’s waiting room feature
- Mute audio and disable video for attendees
- Make sure that your privacy settings share no more data than is necessary.
- Use email or the phone, rather than Zoom, to discuss strictly

CONCLUSION

Zoom bombing has become the order of the day and has frustrated a lot of meetings, webinar and events. And this actually has posed obnoxious threats. This is a new trend and has been pronounced more due to the COVID 19 pandemic. It is still pertinent that this issue gets the attention of the law and thus will attract regulations and policies to curb this issue most especially the fact that virtual working is now a new normal. We yearn for a Regulation on Video conferencing to be passed by parliament of countries as acts which can become distinct video conferencing laws. As this will help bring a tangible statutory regime for posterity and provide an efficient enforcement and protection system.