BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

"Zoom Bombers" -- Illicit Privacy Concerns as the Nation Goes Virtual

By Anne Luquette, J.D. Candidate 2022 | April 13, 2020

Throughout the nation, companies and universities have responded to the coronavirus pandemic by transitioning to virtual classes and meetings. One crucial platform aiding this transition is Zoom, a video conferencing application whose userbase has skyrocketed in the past few weeks. The platform saw a surge in upwards of 200 million daily users in March. Unfortunately, the platform was not entirely prepared for the onslaught of users and security concerns that followed.

Although there are several privacy concerns associated with the rapid growth of Zoom, the recent trend of "Zoombombing" is particularly harmful. Zoombombing has taken the form of simple pranks and coordinated large-scale harassment/disruption efforts. The New York Times recently reported that they discovered "153 Instagram accounts, dozens of Twitter accounts and private chats, and several active message boards on Reddit and 4Chan where thousands of people had gathered to organize Zoom harassment campaigns, sharing meeting passwords and plans for sowing chaos in public and private meetings."

This chaos includes the projection of pornographic and violent images as well as the use of racial, misogynist, anti-Semitic, threats, and vulgar slurs. Zoom Bombers have utilized other platforms to share Zoom links and create further harmful disruptions. There have been a significant amount of disruptions and threats to Alcoholics Anonymous meetings as well as support groups for trans and nonbinary youth.

Government response to these issues is constantly evolving, but the FBI has attempted to enact harsh penalties to deter Zoombombing. The incidents have been classified as cyber-attacks. A teen in Connecticut was "charged with committing fifth-degree computer crime, fifth-degree conspiracy to commit a computer crime and breach of peace" for a Zoombombing incident. The difficulty comes with the nature of these attacks, as it is often difficult to trace the user or halt the attack once the user has access to the link.

While the platform undoubtedly needs to do more to increase security, there are a few things Zoom hosts can do to increase the safety of their meetings. The following steps, recommended by the FBI, can be taken to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
- Lastly, ensure that your organization's telework policy addresses requirements for physical and information security.
- Report any abuse to the FBI's Internet Crime Complaint Center at ic3.gov.
- For a specific threat during a teleconference, please report it at tips.fbi.gov or call the FBI Boston Division at (857) 386-2000.