Cullen | Dykman

Zoom Enters Agreement with NY Attorney General to Implement New Protections for Users Amid Cybersecurity Concerns

May 27, 2020

The COVID-19 pandemic has caused businesses worldwide to quickly shift to a remote working environment. With most employees now working from home, many institutions have turned to various video conferencing programs to conduct virtual face-to-face meetings. Zoom quickly became one of the most popular video conferencing platforms for both business and social use, likely due to its ease of use and ability to host up to 100 participants in a free video chat. In the early weeks of the COVID-19 pandemic, the app was seemingly ideal for various types of institutions, providing a platform to connect users with varying technology skills. However, as Zoom's popularity grew, so did scrutiny over the app's security protocols and data sharing policies.

Concern over Zoom's protections and safety protocols became significant enough for some organizations, including the New York City Department of Education, to ban the use of Zoom for official meetings and instead require the use of other video conferencing platforms. On March 30, 2020, the New York State Attorney General's Office announced it was launching an investigation into Zoom and its security measures to determine what new protections, if any, Zoom put into place to deal with its drastic increase in popularity. On May 7, 2020, the New York Attorney General's Office announced that its investigation was complete after Zoom agreed to implement certain new protections and security measures designed to maintain the privacy and security of all its users.

Concerns About Zoom's Security

One of the most prevalent issues associated with conducting meetings through Zoom was a practice that became known as "Zoom Bombing." Zoom Bombing involves a hacker impermissibly joining a Zoom video conference and interrupting the session with inappropriate images or sounds. This act has been particularly prevalent in online classes conducted by high school teachers and college and university professors. For example, a Massachusetts high school reported that during an online class, an unknown number of individuals entered that class' Zoom conference and disrupted the class by yelling profanity.

In addition, even before the sudden rise in Zoom's popularity at the outset of the COVID-19 pandemic, the company that created the video conferencing platform was already under fire for its privacy policies and certain lesser known features. One feature that has caused controversy and scrutiny allows a Zoom conference host to identify whether the app is active on a participant's screen. Zoom was also forced to admit in March that some

calls initiated using the platform were mistakenly routed through China which has much fewer data privacy laws and could have allowed Zoom to decrypt otherwise encrypted calls.

Zoom has also faced scrutiny for its data collection practices. It was discovered that Zoom may collect user data to be distributed to Facebook, regardless of whether a user has a Facebook account. This practice caused an uproar, calling for Zoom to change its policies related to user data collection and sharing.

Agreement with the New York Attorney General

In response to these security concerns, the New York Attorney General's Office launched a month-long investigation into Zoom's security protocols and practices. The New York Attorney General's Office announced the conclusion of its investigation on May 7, 2020 after an agreement was reached with Zoom to enhance its protections for its end users.

As part of their settlement with the New York Attorney General, Zoom agreed to designate a Head of Security to report directly to the company's Chief Executive Officer on a quarterly basis and its board of directions on a semi-annual basis. The Head of Security will be responsible for implementing and maintaining a comprehensive information security program that is designed to protect the "security, confidentiality, and integrity of personal information that Zoom collects receives or processes."[1] The Head of Security will also be responsible for identifying internal and external risks to the company's security as well as designing and implementing reasonable safeguards to control the identified risks. Zoom's information security program will be continuously evaluated and adjusted in light of the results of testing and monitoring. Zoom also agreed to employ and keep up to date encryption and security protocols, including encryption of all personal information stored by Zoom on its cloud servers.

In addition, the company is now required to offer educational materials about privacy controls for certain types of users including consumers, students, and universities. The New York Attorney General will also require Zoom to offer user facing controls for those who create free accounts and K-12 education accounts that may be used to host meetings for students. Controls must be included to allow users to control access to a specific video conference by requiring a default password or waiting room before access is granted. Moving forward, Zoom must also implement controls related to private messages in a meeting and the ability for hosts to limit screen sharing and the number of participants to those with specific email domains. These measures are designed to eliminate the ability for hackers to "Zoom Bomb" meetings.

The New York Attorney General is also requiring Zoom to maintain reasonable procedures to enable users to easily report violations of Zoom's Acceptable Use Policy. This includes complaints related to users who engage in abusive conduct during meetings. Zoom is also required facilitate external monitoring of its platform to address complaints and bugs associated with any of their systems.

Public Reaction to Settlement

Following the New York Attorney General's announcement of its settlement with Zoom, the New York City Department of Education reversed its stance related to its staff's use of Zoom and will now allow teachers and

administrators to use the video conferencing platform for classes and meetings. It remains to be seen whether other institutions that had previously banned their employees or members from using Zoom will reconsider their stance in light of Zoom's increased security measures. However, the increased security measures and protections outlined in Zoom's settlement with the New York Attorney General should, at the very least, provide increased peace of mind for those who choose to use Zoom as their video conferencing platform.

If you have questions regarding cybersecurity risks and how it may impact you and your business, feel free to contact Ariel E. Ronneburger at (516) 296-9182 or via email at aronneburger@cullenllp.com, Roxanne L. Tashjian at (516) 357-3704 or via email at rtashjian@cullenllp.com, or Ryan Soebke at (516) 357-3784 or via email at rsoebke@cullenllp.com.

Footnote

[1] Letter Agreement between Zoom and the NYAG, May 7, 2020, *available at* https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf (last accessed May 25, 2020).

Practices

- Cybersecurity and Data Privacy

Attorneys

- Ariel E. Ronneburger
- Roxanne L. Tashjian
- Ryan M. Soebke