CUTS International
www.cuts-international.org

Zoom a Lifeline during Lockdown

But with Security & Privacy Risks

Background

The lockdown imposed due to the COVID-19 pandemic has taken over the natural course of life, and people are making new adjustments in their professional and personal lives. To stay in touch, and follow the meeting and conference schedules, organisations, businesses, educational institutions, government, judiciary, family and friends are using online video conference applications and software, more than ever before. In the past few months, Zoom, a video conferencing application has seen a big surge in its usage, with an increase of around two million users since the beginning of 2020.[1] The Teleconferencing major is now valued more than the combined market capitalisation of US Inc.'s American Airlines, Expedia and Hilton.[2]

While Zoom is proving to be of great help to businesses, the education sector and governments in continuing their work, it is also presenting pertinent privacy and security concerns. Media reports reveal that Zoom had shared personal data of its users with Facebook from its iOS app users, for which a lawsuit has been filed against the company, with the New York Attorney General.[3]

There are many other loopholes found within Zoom's privacy policy, which are coming to light due to the sudden surge in its usage. Zoom's approach to them has been reactive, rather than proactive. These have been elucidated in *Figure 1* and discussed below.

Key Issues

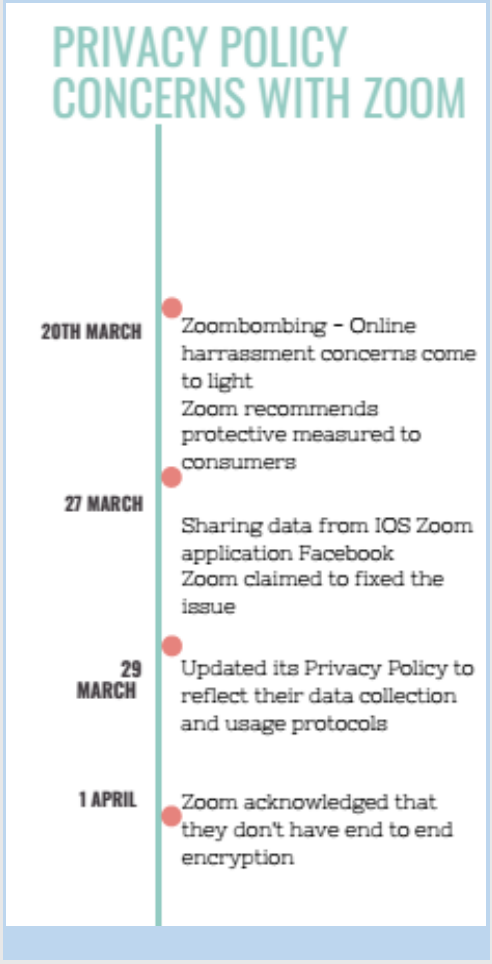
1. 'Zoombombing': Zooms allows for its users to join meetings with passwords. The service provides links to the meetings with embedded meeting ID's and passwords through which anybody with access to the link can join the meeting.[4] While Zoom had enabled default passwords since last year, most users do not opt for this instead of meeting IDs and passwords are widely circulated. This had increased incidents of hacking and infiltration of video chats through unwanted participants sharing their screen-in conferences and meetings and posting of hate speech and explicit content. This is now being called as 'Zoombombing'.

The hacking incidents were also enabled through camera bug in Zoom which facilitates hackers to start webcams and secretly watch users without their knowledge. Zoom installs software to bypass security mechanisms, facilitating the app to launch in a few clicks, but at the cost of security risk. This has led malicious websites to surpass the security feature in Mac computer systems to start cameras without permission.[5] What made this worse is the bug remaining intact and attached to your gadget and systems even if the Zoom application is uninstalled from it.

As several such incidents are coming to light, the Computer Emergency Response Team of India (CERT-In)[6] and Ministry of Home Affairs in India have issued an advisory for users, to check their privacy settings and use strong passwords. The Indian government has also advised ministers and staff to refrain from using Zoom.[7] Additionally, the FBI has also launched an investigation against Zoom, whereas New York, Singapore, UK Ministry of Defence[8] have banned the use of the Zoom by schools amid security concerns.[9].

Figure 1

Source – Zoom Announcements



2. Data Collection, Storage and Consent: According to Zoom's privacy policy, it collects personal data like contact information, email IDs, etc., that users provide while making an account. Zoom's

policy also has a specific category of data called 'customer content' which includes chat logs, files, messages, etc., which can be collected through the permission of the person hosting the meeting. Apart from this, the application also has a unique 'attention tracking' feature[10] which can be activated by the host to track whether Zoom is an active window of the participant at the time of the meeting.[11]

However, there are gaps in the notice and consent framework, along with security loopholes in safe data storage. Zooms privacy policy gives immense power to the host of the meeting in case of recording of the meeting, attention tracking feature and collection of customer content data, as it makes the host responsible for taking consent and informing about the activation of such features to the participants, i.e. there is no default notice and consent mechanism. Additionally, there is a risk of the data stored within the Zoom Cloud through the recording feature being leaked, as its privacy policy does not stipulate security mechanisms used to protect such data. Notably, there have been incidents where links to stored video meetings were leaked online.[12]

3. Data Sharing[13]: Presently, Zoom's privacy policy states that it does not sell user data and neither does it use it to track users nor is it used for advertising purposes. However, it stipulates a separate category 'data we may obtain about you', which includes data that is collected through cookies[14]and is shared with Google analytics for advertising. Concerning other third-party advertising, Zoom gives an opt-out option to its users.[15].

However, media reports reveal that Zoom was sharing data from its iOS app with Facebook for advertising, without informing its users.[16] In another similar incident, Zoom's feature allowed people to access LinkedIn profiles of the participants in the meeting without their knowledge.[17] After these incidents came to light, Zoom has reportedly fixed these issues of data sharing with Facebook, and put its application under a 90 days feature freeze[18], to address all the concerns.[19] Additionally, cookie preferences and opt-out options for data shared with third parties given to users are not explicit and clear, leading them to give consent for sharing their data without being adequately informed about the choices offered to them.

4. End-to-End (E2E) Encryption: Zoom had claimed to be a secured communication platform using E2E encryption. However, such claims have been challenged, leading to a fall in the price of its shares, owing to a class-action lawsuit by shareholders.[20] E2E encryption feature prevents third parties to intercept the conversation or store data, including the service provider itself. An investigation conducted by a cyber-security website on the encryption mechanism used by Zoom revealed that, while the application provides for transport encryption, which

means it prevents third parties from intercepting conversation, however, it does not prevent service provider itself to store or intercept the conversation. This means that Zoom's application can intercept and store video chats.

In another investigation, it was revealed that the 'waiting room feature', which was intended to make the meetings more secure, led the attendees to access and decrypt the meeting key which enabled them to watch the meeting even if they are not approved as participants.[21] This was again enabled due to a weak encryption mechanism.

Furthermore, in a recent report, it has been highlighted that a lot of traffic from Zoom is being directed through China, which has further raised concerns about security and accountability.[22] Notably, Taiwan's government has banned Zoom from public use over fears of communication being intercepted by the Chinese government.[23] Hence, without E2E encryption, and existing lacunas within data sharing and collection protocols, there is a considerable risk of sensitive information such as data of students, or critical discussions by the governments, personal and intimate information about users getting leaked.

While it has been pointed out that ensuring E2E encryption might be technically difficult for video communication application, however, such information must be conveyed to the user to maintain transparency. In the light of this, the officials at the company have claimed that they have fixed the waiting room loophole[24] and are currently working to enable E2E.[25] In the light of the utility derived from E2E encryption, Consumer Unity & Trust Society (CUTS International) is undertaking a study to assess consumer perspective on encryption[26], which can be used by communication platforms such as Zoom to ensure secured communication, considering consumer needs.

Food for Thought

With the increased utility of video conferencing applications in the coming times, concerns towards privacy and security have come to the fore. Concerns highlighted above should be a lesson for all relevant service providers and not just Zoom. There is a need to ensure transparency and accountability of service providers towards users, and investment in mechanisms to ensure digital security. After such concerns being highlighted, Zoom is preparing a transparency report to inform its users regarding its data-sharing practices[27], setting-up an information security council[28], and is also making an effort to ensure the provision of seamless service to its users in these pressing times. Most recently, Zoom has announced that soon paid account holders will be able to select which region their data is routed through.[29] While the company works to revamp its policies, the following recommendations may be adopted to ensure privacy and security.

For Meeting Participants	For Zoom	For Meeting Hosts
• Ensure the host of the meeting is a trustworthy entity. • Users should check what features are activated like recording or attention tracking before they participate in a meeting. • Check their cookie preferences and adjust the settings so that minimal data is shared with third parties. • Businesses that are using Zoom must give employees proper training for their ethical usage to avoid cyber risks.	• Zoom should provide options for locking meetings when all relevant participants have entered the meeting. • Zoom should explicitly state the security protocols and mechanisms it follows within its privacy policy. • Zoom should make passwords mandatory for participating in a meeting and remove the option for embedded passwords within meeting links. • Zoom should make cookie preference and data sharing with third-party as a default option subsequently preventing any sort of explicit data sharing.	• Hosts should ensure that the meetings are only joined by relevant participants. • Hosts should opt for password protection for their meetings. • Hosts should only send the passwords to registered participants right before the meeting to avoid unnecessary circulation. • A host should enable settings in such a way that the least amount of data is shared about the meeting and the privacy of the participants is secured.

Endnotes

1 https://www.cnbc.com/2020/02/26/zoom-has-added-more-users-so-far-this-year-than-in-2019-bernstein.html

2 https://www.moneycontrol.com/news/coronavirus/zoom-is-now-worth-more-than-american-airlines-expedia-and-hilton-combined-5119781.html

3 https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html

4 https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords-

5 https://protonmail.com/blog/zoom-privacy-issues/

6 https://www.outlookindia.com/newsscroll/security-concerns-with-video-conferencing-app-zoom-during-barcs-media-briefing/1788705

7 https://www.livemint.com/news/india/home-ministry-red-flags-zoom-app-for-cybercrimes-11587030646715.html

8 https://www.bbc.co.uk/news/technology-52126534

[9] https://www.theguardian.com/world/2020/apr/11/singapore-bans-teachers-using-zoom-after-hackers-post-obscene-images-on-screens

[10] Zoom claims to have removed this feature, but it still appears within its privacy policy, https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking

[11] https://zoom.us/privacy

[12] https://nypost.com/2020/04/03/zoom-leaves-recordings-of-calls-exposed-on-the-internet-report-finds/

[13] The method of making data used for your research available to others through a variety of mechanisms, https://www.igi-global.com/dictionary/bioinformatics-clouds-for-high-throughput-technologies/6815

[14] Cookies are data collected on the users , as they a use of website or application , specifically with regard to their preferences.

[15] https://zoom.us/privacy

[16] https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html

[17] https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html

[18] No more new features will be introduced in the Zoom application till security and privacy concerns are addressed.

[19] https://techcrunch.com/2020/04/02/zoom-freezes-feature-development-to-fix-security-and-privacy-issues/

[20] https://techcrunch.com/2020/04/08/zoom-sued-shareholder-security/

[21] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[22] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[23] https://www.bbc.com/news/technology-52200507

[24] https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/

[25] https://theintercept.com/2020/03/31/zoom-meeting-encryption/

[26] https://cuts-ccier.org/understanding-consumers-perspective-on-encryption/

[27] https://www.accessnow.org/access-now-urges-transparency-from-zoom-on-privacy-and-security/

[28] https://www.medianama.com/2020/04/223-zoom-information-security-council-alex-stamos/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+medianama+%28Medianama%3A+Digital+Media+In+India%29

[29] https://economictimes.indiatimes.com/magazines/panache/no-more-zoombombing-data-hacking-zoom-rolls-out-new-measures-to-address-security-concerns/articleshow/75198311.cms