**RESEARCH PAPER**

**ZOOM AND PRIVACY CONCERNS**

Submitted by

Ayush Chaurasia

Intern at Probono India

1nd Year B.A.LLB (Hons.),

Faculty of Law,

Dharmashastra National Law University, Jabalpur

[cayush75@gmail.com]

(M) 6267100028



 AUGUST 30, 2020

**ABSTRACT**

Growth in communication technologies offer new opportunities for the conduct of qualitative research. Amidst these, zoom— a video conferencing platform—has sort of distinctive features that intensify its potential appeal to qualitative and mixed-methods researchers. Due to their massive growth over the past few months, Zoom has been placed firmly within the global spotlight – and rightfully so – regarding their security and privacy practices. The Supreme Court of India, alongside courts across the world, are equally concerned about this technology. While there are very legitimate questions on Zoom security, it’s important to know that Zoom can and does provide a secure, usable platform when used correctly. A bit like other cloud-based video solutions, Zoom has similar security capabilities and challenges. Zoom is often configured to satisfy various compliance requirements and has been utilized in various regulated industries for quite a while, but it does require an intentional approach. As part of the response to COVID-19, Zoom has been quickly rolled out by many organizations – and a few of these organizations moved forward without fully thinking through the security decisions needed for their Zoom instance. Additionally, due to its growing prevalence, the Zoom platform is now a larger target for attackers. This year, trouble surrounding the use of Zoom arose with critical security vulnerabilities allowing hackers to foresee Meeting ID’s and therefore join active meetings,[[1]](#footnote-1) and also enabling any website to forcibly join a user to a Zoom call with their video camera activated and without the user’s permission.[[2]](#footnote-2) Zoom refused to disable the ability for hackers to forcefully join a call anyone visiting a malicious site, raising security red flags and undermining public confidence in Zoom’s attitude towards data security. The purpose of this document is to highlight the most common and relevant issues highlighted about Zoom, and most importantly, what actions have been or need to be taken to address these risks.

Keywords: Zoom, Privacy, Zoombombing, End-to-End Encryption (E2EE), Security Flaws.

**INTRODUCTION**

Amidst the pandemic, businesses from all over the globe have turned to remote work arrangements. This has led to a sharp increase in the use of videoconferencing technology Zoom. In the last month, there was a 535% rise in daily traffic to the Zoom.us download page, according to an analysis from the analytics firm Similar Web. Its app for iPhone has been the most downloaded app in the country for weeks, according to the mobile app market research firm Sensor Tower.[[3]](#footnote-3) Even politicians and other high-profile figures, including the British prime minister, Boris Johnson, and the former US federal reserve chair Alan Greenspan, use it for conferencing as they work from home.[[4]](#footnote-4) But rapid growth like this isn't without consequences. The video-conferencing tool, which has become the most prevalent form of communication during the pandemic, is now facing the consequences of failing to put in place adequate privacy and security measures to protect the millions of users who are having highly sensitive discussions on its app.[[5]](#footnote-5)

The past few months have been a game of cat and mouse for Zoom. When a new investigation uncovers a defect in its security or privacy practices, Zoom quickly covers it. And on it goes. One of the complaints has even developed into a lawsuit – for allegedly failing to protect the personal information of its users. A major New York securities company, Labaton Sucharow, announced that it was investigating Zoom on behalf of its shareholders, concerning allegations that "Zoom may have issued materially misleading business information to the investing public".[[6]](#footnote-6)

Numerous security researchers, organisations, and journalists have spoken out at length about the unending list of privacy and security concerns about Zoom, even as ‘zoombombing’ reports continued to balloon all across the internet. In return, Zoom’s founder and Chief executive Eric Yuan yesterday offered a meek apology for not being careful enough with user data and privacy and promised that his company is working hard to address all the safety concerns among users.[[7]](#footnote-7) But, the question remains, is Zoom doing enough? Should they have seen the usage trends early and taken appropriate measures beforehand?[[8]](#footnote-8)

The privacy concerns did not just end there. A report by the Electronic Frontier Foundation[[9]](#footnote-9) listed multiple security concerns about Zoom, which included the ability of a call’s host to monitor the activity of all attendees, access detailed dashboards of user activities, access contents of calls recorded by other non-admin users, and even access device information, OS information, IP address, and user location data.[[10]](#footnote-10)

A lot of reports about Zoom’s security issues have floated across the internet. Now, with the expanding user base, a few of these issues have remained — outside users tapped into private meetings as most users remained untaught about privacy settings introduced later, in the following update to Zoom’s privacy policy.[[11]](#footnote-11) This has led to the institution of the term zoombombing, where users’ video meetings were bombarded with pornographic content.[[12]](#footnote-12)

Zoom’s iOS app was sharing user data with Facebook without declaration of the same to its users. It did so even for users without Facebook accounts. Even as Zoom promptly “apologised” and fixed the mistake, followed by a massive rise in the number of malicious domains impersonating Zoom to steal more data and money, although it can be said that the latter is not Zoom’s own fault.[[13]](#footnote-13)

A day after when Zoom updated its privacy policy[[14]](#footnote-14) significantly, reports stated that the service was being investigated by the office of New York Attorney General, Letitia James. Independent security researchers also found security problems with Zoom’s Windows[[15]](#footnote-15) and Mac apps — for Windows, the app was found to be leaking the login credentials of users to cybercriminals, whereas, on Mac, Zoom’s installer client did not need explicit user permission to be installed, creating an all-new threat of being accessible to hackers as a Remote Access Tool (RAT).

Security researchers have called Zoom “a privacy disaster” and “fundamentally corrupt” as allegations of the company mishandling user data snowball.[[16]](#footnote-16)

**PRIVACY ISSUES YOU NEED TO AWARE OF WHILE USING ZOOM**

ZOOM PRIVACY REGARDING YOUR DATA

According to the Zoom’s privacy policy, zoom collects a large amount of data, including your name, email address, physical address, mobile number, occupation, employer, what type of device you areusing(even if you don’t make an account with Zoom),and your IP address**.** It also collects information from your Facebook profile in case if you use Facebook to sign in and any “information you upload, provide or create while using the service.”[[17]](#footnote-17)

Some of this data (for example, email) you enter yourself when you are signing in, but reams of it are collected automatically by the Zoom app.

In its [privacy policy](https://zoom.us/privacy),[[18]](#footnote-18) under the question “Does Zoom sell Personal Data?” the policy says, “Depends what you mean by ‘sell.’” It means that they don’t sell personal data for money to third parties, but it does share personal data with third parties for those companies’ “business purposes.”For example, in its privacy policy, it is given that it may pass your personal information to Google.

Even if the user does not have a Facebook account, the Zoom iOS app shared a substantial amount of user data with Facebook.[[19]](#footnote-19) However, after two days when this news was published, Zoom removed the code that sent data to Facebook. In a statement to Vice, Zoom explained it was unaware that the Facebook software development kit (SDK) used to implement the “Login with Facebook” feature in its app was collecting unnecessary data. The statement also listed the types of device data the Facebook SDK had collected, including the mobile operating system (OS) type and version, device OS, the device time zone, device model and carrier, processor cores, screen size, and disk space.[[20]](#footnote-20)

A resident from California alleges that Zoom violated the California Consumer Privacy Act by not getting users’ consent before sharing their data with Facebook.[[21]](#footnote-21) Also, the New York Attorney General’s office recently sent a letter to the company, expressing concern that Zoom’s existing security practices fail to secure its users’ data. The Attorney General’s primary concern was that Zoom may not be doing enough to meet the state’s requirements to protect student data. Zoom has recently increased the number of participants allowed on their free calls to help teachers and schools reach students at home.[[22]](#footnote-22)

### ZOOM DOES NOT USE END-TO-END ENCRYPTION

End-to-End encryption, also known as E2EE, ensures that only users directly communicating with one another can read information shared with each other. The message is encrypted by the sender and decrypted by the guest; there is no middleman involved with the ability to decrypt the message.[[23]](#footnote-23)

While Zoom used own definition for end-to-end encryption (E2EE), Zoom’s security white paper[[24]](#footnote-24) states that a meeting host can enable End-to-End encryption, this option enables E2EE for chat messages only. Video is still handled by Transport Layer Security (TLS).[[25]](#footnote-25)

With TLS, the message is still encrypted by the sender; however, this connection is initiated with the vendor’s server. Think of the server as the middleman between you and the individual(s) you are in a call with. TLS terminates once communication is sent back to the server, and the company owning the server can view call information since it is not encrypted. The communication may be encrypted through TLS again once it is sent over to the recipient. [[26]](#footnote-26)

While this may not be a concern for most end-users, Zoom can look at private meetings and can provide recordings or details of meetings to governmental organizations or to companies interested in data collection. It should be noted that while Zoom can to distribute user information, its official privacy policy [[27]](#footnote-27) states that “We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment.”

A Zoom spokesman clarified that E2EE to Zoom means, “the connection encrypted from Zoom endpoint to Zoom endpoint.” Here “endpoint” refers to the Zoom server, not the Zoom app. This is not true E2EE.[[28]](#footnote-28)

ZOOMBOMBING

On 30 March, the FBI announced it was investigating increased cases of video hijacking, also known as “Zoom-bombing”, in which Online trolls have disrupted numerous online conference calls, by sharing pornographic material using a Zoom screen share feature.[[29]](#footnote-29)

Zoom meetings can be accessed by a short number-based URL, which can easily be generated and guessed by hackers,[[30]](#footnote-30) Zoom, by default, allows anyone to share their screen with the participants of a call without permission from the call’s host.If a call is public, anyone can join using the URL. This has allowed malicious actors to sneak into calls using publicly shared links and then take over by sharing their screen and showing the audience offensive material.[[31]](#footnote-31)

### THE CAMERA HACKING BUG

Johnathan Leitschuch, a Security consultant discovered that Zoom set up a local webserver on a user’s device (Mac device) that allowed Zoom to bypass security features in Safari 12. This local web server was used to bypass a pop-up window that Safari 12 would show before it turned on your device’s camera and was not mentioned in any of Zoom’s official documentation.[[32]](#footnote-32)

This remote web server was also not secured. Any website could interact with it and the result was that Zoom allowed malicious websites to take over your Mac’s camera without ever alerting you. [[33]](#footnote-33)

Electronic Privacy Information Center filed an FTC complaint against Zoom by, claiming that Zoom “intentionally designed its web conferencing service to bypass browser security settings and remotely enable a user’s web camera without the knowledge or consent of the user.”[[34]](#footnote-34)

While Zoom has since removed these remote web servers,[[35]](#footnote-35) its casual approach to getting user permission and its repeated carelessness for security and privacy concerns in the pursuit of convenience raises serious questions about security and trust.[[36]](#footnote-36)

SECURITY FLAWS

Several numbers of flaws affecting security and privacy have been reported in the past. Last year, it was revealed Zoom had quietly installed a hidden web server on user devices that could allow the user to be added to a call without their permission.[[37]](#footnote-37) And a flaw discovered this week would enable hackers to hack the microphone to take over a Zoom user’s Mac, including tapping into the webcam.[[38]](#footnote-38)

Zoom said that it had issued a release to fix the Mac issue, but Arvind Narayanan, an associate computer science professor at Princeton University said that the number of security issues with Zoom in the past years makes it as bad as malicious software.[[39]](#footnote-39)

IN-APP SURVEILLANCE MEASURES

There’s a feature, called “attention tracking” on Zoom that identifies whether participants have clicked away from the active Zoom window for 30 seconds or more.[[40]](#footnote-40)

Through this feature the employers will check if students are really watching a classroom presentation remotely or if employees are tuned in to a work meeting.

**HOW TO PROTECT YOUR DATA**

There are some steps users can take to keep their data safe.

* **Do not use Facebook to sign in:**It is a poor security practice and dramatically increases the amount of personal data Zoom has access to.
* **Keep your Zoom app updated:** If you recently downloaded Zoom, there’s no need to be concerned about this specific vulnerability. Zoom from the latest versions of its apps removed the remote web server.
* **Prevent intruders and Zoom bombing on your calls:** Before you set up a public Zoom call, go to Settings and turn Screen Sharing to “Host-only,” disable “Join Before Host,” disable “Allow Removed Participants to Re-join,” and disable “File Transfers.” You should also protect your conference call with a password.

**HOW TO AVOID “ZOOMBOMBING”**

GENERAL GUIDELINES

1. Use a unique Zoom ID for each meeting, avoid using your Personal Meeting ID.
2. Do not post meeting links on social media.
3. Do not share links to meetings you are invited to join without the host’s approval. The host can send more invites to relevant individuals or parties.
4. Do not use your Personal Meeting ID when hosting public meetings or webinars.

MANAGE PARTICIPANTS AS A HOST

1) Do not make meeting rooms open to the public. Require a password for attendees to join.

2) Utilize waiting rooms. This will enable the control and management of guests.

3) If appropriate for a meeting, change the screen-sharing option to “Host-Only.”

4) Lock the meeting after a desired amount of time has passed. This will prevent new participants from joining, even if they have the meeting ID and password. This can be done through Host Controls.

5) Require participants to join a meeting using the same email they were invited with.

6) If there is no need to share files during a meeting, you can turn this capability off.

7) If there is no need to annotate a screen share, you can turn off Annotation.

8) By disabling private chat to prevent participants from chatting with each other can be very useful in an educational environment.

9) You should also consider making your meetings Screen Share only. This will prevent participants from sharing inappropriate behavior. To further enhance security, it is recommended to set up Single Sign-On authentication.

**ZOOM VIOLATES RIGHT TO PRIVACY**

The Ministry of Home Affairs has announced that the 'Zoom App' is not safe to use in terms of Cyber Crime. Given the same, the Supreme Court Advocates has written a letter to the Chief Justice S A Bobde concerning violation of the Fundamental Right of Privacy by the citizens using the video conferencing app 'Zoom'. The petition referred to the K. S. Puttaswamy v. Union of India ruling and emphasised on the fact that the fundamental right to privacy is a sacrosanct right guaranteed under Article 21 of the Constitution of India as decided by the nine Judges constitution bench of the Supreme Court. Therefore, the petitioners pleaded for suo motu cognisance of this serious issue and urged for orders to protect the Fundamental Right of privacy of all citizens.

The Supreme Court on 22 May, based on privacy and cyber-security concerns, issued notice to the central government on public interest litigation (PIL) asking for a ban on the video-conferencing app Zoom.

**CONCLUSION**

While Zoom can be held accountable for all these flaws, and for simply having so many privacy issues at one go, it is important to note that even users need to be wary of the issues. Avinash Prasad, vice president and head of managed security services at Tata Communications, puts the onus on organisations to also take charge of cyber-security practices. In a statement, Prasad says, “Organisations must put together a cross-functional and collaborative team to have a holistic COVID-19 risk management strategy, covering both human safety as well as information and data security.”

Zoom may well be forced to tighten up the very parts of its app that make it so appealing for consumers and businesses alike in the coming months. Zoom’s appeal has been its simple approach to video conferencing, but that crucial ingredient now threatens to be its downfall unless it gets a firm grip on the growing concerns.

**REFERENCES**

1. Zoom, Security Guide Zoom Video Communications, Inc., available at: <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf> [accessed 8 August 2020].
2. Quest Center for Integrative Health, available at: <https://quest-center.org/sites/default/files/2020-04/Zoom%20Privacy%20Statement.pdf> [accessed 8 August 2020].
3. California Community College, Security Practices for Zoom Video Conferencing: A Guide for California Community Colleges, available at: <http://ets.fhda.edu/getting-help/staff/_documents/_zoom/ISC-Security-Practices-for-Zoom-fa.pdf> [accessed 8 August 2020].
4. The Verge, Zoom faces a privacy and security backlash as it surges in popularity, available at: <https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response> [accessed 8 August 2020].
5. ResearchGate, Zoom Tips for Privacy and Security, available at: file:///C:/Users/HP/Downloads/Zoom-Tips\_Coastline-College-CyberCenter%20(1).pdf [accessed 8 August 2020].
6. Zoom Security & Privacy FAQs, available at: <https://isc.idaho.gov/zoom/zoom_security_v4_04132020.pdf> [accessed 8 August 2020].
7. The Guardian, ‘Zoom is malware’: why experts worry about the video conferencing platform, available at: <https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing> [accessed 8 August 2020].
8. Forbes, Zoom’s A Lifeline During COVID-19: This Is Why It’s Also A Privacy Risk, available at: <https://www.forbes.com/sites/kateoflahertyuk/2020/03/25/zooms-a-lifeline-during-covid-19-this-is-why-its-also-a-privacy-risk/#3bb85d1928ba> [accessed 8 August 2020].
9. Campaign, 'Zoom's practices violate our human right to privacy', available at: <https://www.campaignlive.co.uk/article/zooms-practices-violate-human-right-privacy/1679551> [accessed 8 August 2020].
10. <https://epic.org/privacy/zoom/EPIC-FTC-Complaint-In-re-Zoom-7-19.pdf> [accessed 8 August 2020].
11. The National Law Review, Not so Zoomy: Use of Videoconferencing Technology "Zoom" is on the Rise, but Privacy and Data Security Inadequacies Users Should Tread Carefully, available at: <https://www.natlawreview.com/article/not-so-zoomy-use-videoconferencing-technology-zoom-rise-privacy-and-data-security> [accessed 8 August 2020].
12. Latest Laws, 'Zoom violates Right to Privacy', Lawyers write letter petition to CJI, asks for ban on app, available at: <https://www.latestlaws.com/latest-news/zoom-violates-right-to-privacy-lawyers-write-letter-petition-to-cji-asks-for-ban-on-app/#:~:text=The%20Ministry%20of%20Home%20Affairs,in%20terms%20of%20Cyber%20Crime.&text=In%20view%20of%20the%20same,video%20conferencing%20app%20'Zoom'.> [accessed 8 August 2020].
13. The Quint, Ban on Zoom App? SC Issues Notice on PIL Claiming Security Risk, available at: <https://www.thequint.com/news/india/supreme-court-issues-notice-pil-for-ban-of-zoom-privacy-security-zoombombing> [accessed 8 August 2020].
14. The Intercept, ZOOM MEETINGS AREN’T END-TO-END ENCRYPTED, DESPITE MISLEADING MARKETING, available at: <https://theintercept.com/2020/03/31/zoom-meeting-encryption/> [accessed 8 August 2020].
15. ProtonMail, Using Zoom? Here are the privacy issues you need to be aware of, available at: <https://protonmail.com/blog/zoom-privacy-issues/> [accessed 8 August 2020].
16. The Times of India, SC seeks Centre's reply on plea for ban on Zoom app until appropriate legislation is put in place, available at: <https://timesofindia.indiatimes.com/india/sc-seeks-centres-reply-on-plea-for-ban-on-zoom-app-until-appropriate-legislation-is-put-in-place/articleshow/75890010.cms> [accessed 8 August 2020].

**ABOUT THE AUTHOR**

Ayush Chaurasia is a First-year student currently pursuing B.A.LLB (Hons.) from Dharmashastra National Law University, Jabalpur. He has a keen interest in learning about socio-legal issues. He is also an intern at Probono India. He was a part of Indian Mediation Week which is recognised by the Ministry of Law and Justice, Government of India with a keen interest in writing articles on emerging and ongoing legal issues. He has publications in various reputed websites on various topics. He is also the editor of 2 websites. He is very thankful to Probono India for giving him an opportunity to intern.

1. Alexander Chailytko: “Zoom-Zoom: We Are Watching You”, CHECK POINT RESEARCH, available at: https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/, last seen on 28/08/2020. [↑](#footnote-ref-1)
2. Jonathan Leitschuh: “Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!” available at: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5, last seen on 28/08/2020. [↑](#footnote-ref-2)
3. Sensor Tower, available at: https://sensortower.com/ios/us/zoom/app/zoom-cloud-meetings/546505307/overview, Accessed on 28/08/2020. [↑](#footnote-ref-3)
4. The Guardian, ‘Zoom is malware’: why experts worry about the video conferencing platform, <https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing>, Accessed on 28/08/2020. [↑](#footnote-ref-4)
5. Jessica Goodfellow: “Security and privacy experts discuss video-conferencing app's flaws and how concerned we should be”, CAMPAIGN, available at: https://www.campaignlive.co.uk/article/zooms-practices-violate-human-right-privacy/1679551, last seen on 28/08/2020. [↑](#footnote-ref-5)
6. *Ibid.* [↑](#footnote-ref-6)
7. “Zoom Founder Apologises for App's Elaborate Privacy Issues, Reveals Plans for Future”, NEWS18, available at: https://www.news18.com/news/tech/zoom-founder-apologises-for-apps-elaborate-privacy-issues-reveals-plans-for-future-2562867.html, last seen on 28/08/2020. [↑](#footnote-ref-7)
8. “Zoom Video Conferencing and its Unending Privacy and Security Issues: The Full Timeline”, NEWS18, available at: https://www.news18.com/news/tech/zoom-video-conferencing-and-its-unending-privacy-and-security-issues-the-full-timeline-2563563.html, last seen on 28/08/2020. [↑](#footnote-ref-8)
9. LINDSAY OLIVER: “What You Should Know About Online Tools During the COVID-19 Crisis”, Electronic Frontier Foundation, available at: https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis, last seen on 28/08/2020. [↑](#footnote-ref-9)
10. Supra note 6. [↑](#footnote-ref-10)
11. Supra note 6. [↑](#footnote-ref-11)
12. “FBI Says Hackers are Disrupting Video Conferences on Zoom with Porn”, available at: https://www.news18.com/news/buzz/fbi-says-hackers-are-disrupting-video-conferences-on-zoom-with-porn-2561203.html, last seen on 28/08/2020. [↑](#footnote-ref-12)
13. Supra note 6. [↑](#footnote-ref-13)
14. “Zoom Privacy Statement”, available at: https://zoom.us/privacy?zcid=1231, last seen on 28/08/2020. [↑](#footnote-ref-14)
15. Lawrence Abrams: “Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links”, BleepingComputer, available at: https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/, last seen on 28/08/2020. [↑](#footnote-ref-15)
16. The Guardian, ‘Zoom is malware’: why experts worry about the video conferencing platform, available at: <https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing>, last seen on 28/08/2020. [↑](#footnote-ref-16)
17. Richie Koch: “ProtonMail, Using Zoom? Here are the privacy issues you need to be aware of”, available at: <https://protonmail.com/blog/zoom-privacy-issues/>, last seen on 28/08/2020. [↑](#footnote-ref-17)
18. “Zoom Privacy Statement”, Zoom, available at <https://zoom.us/privacy>, last seen on 28/08/2020. [↑](#footnote-ref-18)
19. Joseph Cox: “Zoom iOS App Sends Data to Facebook Even if You Don’t Have a Facebook Account”, VICE, available at <https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account>, last seen on 28/08/2020. [↑](#footnote-ref-19)
20. Joseph Cox: “Zoom Removes Code That Sends Data to Facebook”, VICE, available at <https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook>, last seen on 28/08/2020. [↑](#footnote-ref-20)
21. Joseph Cox: “Zoom Faces Class Action Lawsuit for Sharing Data with Facebook”, VICE, available at <https://www.vice.com/en_us/article/pke4vb/zoom-faces-class-action-lawsuit-for-sharing-data-with-facebook>, last seen on 28/08/2020. [↑](#footnote-ref-21)
22. Danny Hakim and Natasha Singer: “New York Attorney General Looks Into Zoom’s Privacy Practices”, The New York Times, available at <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html>, last seen on 28/08/2020. [↑](#footnote-ref-22)
23. California Community College, Security Practices for Zoom Video Conferencing: A Guide for California Community Colleges, available at: <http://ets.fhda.edu/getting-help/staff/_documents/_zoom/ISC-Security-Practices-for-Zoom-fa.pdf> , last seen on 28/08/2020. [↑](#footnote-ref-23)
24. Zoom, Security Guide Zoom Video Communications, Inc., available at: <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>, last seen on 28/08/2020. [↑](#footnote-ref-24)
25. Supra note 6. [↑](#footnote-ref-25)
26. Supra note 6. [↑](#footnote-ref-26)
27. “Zoom Privacy Statement”, Zoom, available at <https://zoom.us/privacy>, last seen on 28/08/2020. [↑](#footnote-ref-27)
28. Richie Koch: “ProtonMail, Using Zoom? Here are the privacy issues you need to be aware of”, available at: <https://protonmail.com/blog/zoom-privacy-issues/>, last seen on 28/08/2020. [↑](#footnote-ref-28)
29. “FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic”, BOSTON, available at: <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>, last seen on 28/08/2020. [↑](#footnote-ref-29)
30. Alexander Chailytko: “Zoom-Zoom: We Are Watching You”, CHECK POINT RESEARCH, available at: https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/, last seen on 28/08/2020. [↑](#footnote-ref-30)
31. Richie Koch: “ProtonMail, Using Zoom? Here are the privacy issues you need to be aware of”, available at: <https://protonmail.com/blog/zoom-privacy-issues/>, last seen on 28/08/2020. [↑](#footnote-ref-31)
32. Jonathan Leitschuh: “Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!” available at: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5, last seen on 28/08/2020. [↑](#footnote-ref-32)
33. Supra note 14. [↑](#footnote-ref-33)
34. “EPIC Files Complaint with FTC about Zoom”, Electronic Privacy Information Center, available at: https://epic.org/2019/07/epic-files-complaint-with-ftc-.html, last seen on 28/08/2020. [↑](#footnote-ref-34)
35. Richard Farley: “Response to Video-On Concern”, Zoom, available at: https://blog.zoom.us/response-to-video-on-concern/, last seen on 28/08/2020. [↑](#footnote-ref-35)
36. Supra note 14. [↑](#footnote-ref-36)
37. Jonathan Leitschuh: “Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!” available at: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5, last seen on 28/08/2020. [↑](#footnote-ref-37)
38. Zack Whittaker: “Ex-NSA hacker drops new zero-day doom for Zoom”, available at: https://techcrunch.com/2020/04/01/zoom-doom/, last seen on 28/08/2020.

 [↑](#footnote-ref-38)
39. The Guardian, ‘Zoom is malware’: why experts worry about the video conferencing platform, available at: <https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing>, last seen on 28/08/2020. [↑](#footnote-ref-39)
40. Jenna Amatulli: “Zoom Can Track Who's Not Paying Attention In Your Video Call. Here's How”, available at: https://www.huffingtonpost.co.uk/entry/zoom-tracks-not-paying-attention-video-call\_l\_5e7b96b5c5b6b7d80959ea96, last seen on 28/08/2020. [↑](#footnote-ref-40)