

**IN THE SUPREME COURT OF INDIA
ORIGINAL CIVIL JURISDICTION
WRIT PETITION (C) NO. OF 2020
(Under Article 32 of the Constitution of India)**

IN THE MATTER OF:

Mrs. Harsh Chugh
W/o Late Sh. M.M. Chugh
R/o C 10/53 First Floor,
Sector -15, Rohini,
Delhi-110089

...Petitioner

Versus

1. Union of India
Ministry of Electronics &
Information Technology
Through its Principal
Secretary,
Electronics Niketan, 6, CGO
Complex,
Lodhi Road,
New Delhi – 110003
India
E-mail :
webmaster@meity.gov.in

...Respondent no.1

2. Cyber & Information
Security(C&IS) Division
Through its Joint Secretary
Ministry of Home Affairs
North Block
New Delhi - 110001
India
Email:-jscis-mha@nic.in

...Respondent no.2

3.ZoomVideo
Communications, Inc
Through its CEO

Mr. Eric S Yuan
 Having its office at San Jose
 Headquarters
 55 Almaden Boulevard, 6th
 Floor, San Jose,
 CA 95113
 USA
 Contact No +1.888.799.9666
 Email: info@zoom.us

...Respondent no.3

**Respondent nos. 1 and 2 contesting,
 Respondent no.3 is proforma**

**A PETITION UNDER ARTICLE 32 OF THE
 CONSTITUTION OF INDIA FOR PROTECTION AND
 ENFORCEMENT OF RIGHT TO PRIVACY OF
 GENERAL PUBLIC RECOGNIZED AS
 FUNDAMENTAL RIGHT UNDER ARTICLE 21 OF
 THE CONSTITUTION.**

AND

**A PETITION FOR WRIT OF MANDAMUS OR ANY
 OTHER WRIT, ORDER OR DIRECTION IN THE
 SIMILAR NATURE DIRECTING THE RESPONDENT
 NOS.1 AND 2 TO CARRYOUT AN EXHAUSTIVE
 TECHNICAL STUDY INTO THE SECURITY AND/OR
 PRIVACY RISKS OF USE OF 'ZOOM' FOR OFFICIAL
 AND PERSONAL PURPOSE BY THE PUBLIC.**

AND

**A PETITION FOR WRIT OF MANDAMUS OR ANY
 OTHER WRIT, ORDER OR DIRECTION IN THE
 SIMILAR NATURE THEREBY DIRECTING THE
 RESPONDENT NOS.1 AND 2 TO BAN THE USE OF
 'ZOOM' FOR OFFICIAL AND PERSONAL PURPOSES**

**BY THE PUBLIC UNTIL AN APPROPRIATE
LEGISLATION IS PUT IN PALCE.**

To,

**THE HON'BLE CHIEF JUSTICE OF INDIA AND HIS
COMPANION JUSTICES OF THE HON'BLE
SUPREME COURT OF INDIA.**

**the humble petition of
the petitioner above named**

MOST RESPECTFULLY SHOWETH:

1. That the petitioner- a bonafide citizen of India and a part time private tutor by avocation-prefers the present petition under Article 32 of the Constitution of India feeling concerned about the privacy and security risk posed by a communication software/application titled 'Zoom' owned, marketed and controlled by the respondent no.3. Hence, the present petition is relatable to Article 21 of the Constitution wherein Right to Privacy is recognized as a Fundamental Right.
2. That in the present petition the petitioner has neither any personal gain or private motive nor the present petition is being filed for any oblique reason.
3. That the present petition is necessitated in view of various facts and incidents reported by the media sources against breaching of cyber security through

Zoom App, one of the most overused applications for enabling video communications i.e. for video and audio conferencing, meetings, chats and webinars. The Zoom App is available free of cost in App Stores on all smart phones, tablets, laptops and computer and hence is easy to download and use or misuse. It is pertinent to point out that the CEO of the respondent no.3 has already apologised publically and has accepted the app to be faulty in terms of providing a secure environment digitally which is against the norms of cyber security.

4. That in view of the ongoing lockdown the petitioner could not give any representation to any of the respondents, however, as the reliefs which are sought in the present petition are urgent in view of the penetration of offending software increasing with each day and as the concern raised in the present petition have Pan India ramifications, hence, the petitioner is directly filing the present petition before this Hon'ble Court. It is also pertinent to point out that the risk to the privacy of users of the offending software is also recognized by the respondent nos. 1 and 2. Hence, they are already familiar with the subject matter.

However, still the respondent nos. 1 and 2 have not taken any steps to protect the general public and have not banned the offending software.

5. That the petitioner has not filed any other petition for the same or similar relief before this Hon'ble Court or before any other Court.
6. That the petitioner has never filed any other petition either under Article 32 or Article 226 of the Constitution for any relief whatsoever.
7. The Petitioner is a house maker and takes tuition classes and has now started doing the same through zoom. The petitioner is a peace loving citizen and is concerned about such cases of hacking and cyber breach being reported innumerable.
8. The Respondent No. 1 is Union of India through Ministry of Electronics & Information Technology which is responsible to maintain the Internet Governance in the country and the responsible authority to enhance efficiency of digital services while making sure of providing a secure cyber space. The Respondent No. 2 is Cyber & Information Security (C&IS) Division of Ministry Of Home affairs which is responsible to ensure Cyber Security and prevent

Cyber Crime. The Respondent no. 3 is Zoom Video Communications, Inc., organized in Delaware, USA and headquartered in San Jose, California, USA. It is a public incorporation listed at NASDAQ. The respondent no.3 provides software, including a mobile app, for video telephony, online chat, and business telephone systems. Use of the platform is free for video conferences of up to 100 participants, with a 40-minute time limit. For longer or larger conferences with more features, paid subscriptions are available, costing \$15-20 per month. The Zoom Video Communications which is the software company providing a remote conferencing service that combines video conferencing, online meetings, chat, and mobile collaborations but is providing poor privacy and security practices to its users, the same has also been accepted by the CEO of the said company. The same was founded on 21/04/2011 and the Founder and CEO of the company is Mr. Eric Yuan.

9. That the Zoom App practices data hoarding and cyber hoarding which includes mass storage of personal data of its users and stores cloud recordings, instant

messages, files, whiteboards, etc. Further, there have been concerns about what now is being called ‘*zoombombing*’ where an unauthorized person or stranger joins a Zoom meeting/chat session and causes disorder by saying offensive things and even photo bombing the meeting by sharing pornographic and/or hate images.

10. That during the times when the world is under the shadow of Covid-19 pandemic which has forced millions of people to stay home since March 2020, Zoom suddenly became the video meeting service of choice of the people worldwide and daily meeting participants on the platform surged from 10 million in December, 2019 to 200 million in March 2020 as revealed by the CEO of the app, Eric S Yuan.
11. That the Zoom founder and CEO Eric S Yuan has also accepted the fact that his company wasn't prepared for the influx of novice users.
12. That though India’s top cyber-security chief, reporting to the Prime Minister’s Office (PMO), Lt. General Rajesh Pant has issued a ‘cyber-advisory’ for the lockdown and it comes in the backdrop of cyber criminals taking advantage of the emerging work from

home (WFH) environment during the lockdown, the sudden boom in the use of Zoom App has severely affected the cyberspace by leaking the personal data of its users and the poor privacy and security of the app has further enabled the hackers to get access to the meeting, classes and conferences being conducted online through this app.

13. That Zoom is reported to have a bug that can be abused intentionally to leak information of users to third parties. The app has falsely claiming calls are end-to-end encrypted when they are not.
14. That monitoring would be less of a concern if Zoom were encrypted end-to-end, as the company is falsely claiming in its marketing materials. But it admitted to the 'Intercept', an online news publication owned by First Look Media, that Zoom did not use End-to-End Encryption (E2EE) for video calls. Zoom uses some encryption (known as transport encryption), which is not as secure as end-to-end.
15. That zoom falsely advertised end-to-end encryption, while many companies are prioritizing people over profits to fight COVID-19, Zoom is prioritizing profits over people. Zoom was capitalizing off of the global

pandemic by selling user information to Facebook without user consent. Zoom compounds this felony by falsely advertising that its software is equipped with end-to-end encryption. Zoom pedals its products knowing that hackers are accessing to user webcams, exposing its users to extreme invasions of privacy.

16. That there were questions raised about where Zoom is sending the data it collects from the computer of its users and Zoom was found to be sending data to Facebook, even if the users weren't logged in to a Facebook account. Zoom also apologized publically for mistakenly routing traffic through China, where the internet is heavily monitored by the government.
17. That joining a call on the Zoom App is particularly easy with the click of a meeting URL, the page automatically launches the desktop app instantly taking the person inside the meeting/video conference.
18. That further in times of lockdown all the schools, agencies, corporates and in fact the court of law including this Hon'ble Apex Court of India and various other High Courts have resorted to function through video conferencing. While this Hon'ble Court

has adopted Vidyo Mobile/ Computer App for its functioning as the same is vetted by the National Informatics Center (NIC), some other High Courts are using Zoom App.

19. That recently Hon'ble Bombay High Court decided to live stream court hearing on a trial basis. For this, the bench of Hon'ble Mr. **Justice G.S. Patel** made the hearing of listed matters on 9th April 2020, publicly accessible. Further, the Hon'ble High Court of Kerala has also started live-streaming of court hearings through the Zoom App. The hearing in the court of Hon'ble Mr. Justice Patel could be accessed by anyone and everyone via the Zoom app/plugin, thorough the videolink viz., <https://zoom.us/j/427322355>, without any password.
20. That on 12.04.2020, The Cyber Coordination Committee issued a public advisory as to how this app is unsafe and laid out certain steps to take care of while using the said app. However, there have been no mention of how this app is not end to end encrypted and is still receiving data of the user in a full-fledged manner.

21. That it is important to realise how zoom consistently violates its duty to implement and maintain reasonable security practices, and misleads consumers about the security benefits of the Product. Zoom has targeted consumers, businesses, and schools.

22. That the global COVID-19 pandemic has drastically reshaped the way in which consumers, businesses, and schools communicate. Rather than lending a hand to people in need, Zoom violates the privacy of its millions of users by misusing and exploiting their personal information, and falsely, deceptively, and misleadingly advertising fictitious security benefits of the program.

23. That it is of utmost pertinence that at a time when almost everyone in the country is locked down at their houses and have easy access to internet and apps such as Zoom, it is not safe to conduct these conferences through an app which has already been banned in several countries over security issues and that the founder of the said app has himself accepted

the app to have certain bugs leading to leakage of data and making it easy for hackers to access it.

24. That to illustrate the risk of compromising privacy and web security the petitioner is relying upon the following reported incidents world over:

26.03.2020:

- An investigation by Motherboard (Tech by Vice), a London based online magazine revealed that Zoom's iOS app was sending user analytics data to Facebook, even for Zoom users who did not have a Facebook account, via the app's interaction with Facebook's Graph API. The true typed copy of the said article by Motherboard is being annexed herewith and is Marked as **Annexure-P1[Pg.44 to 49]**

28.03.2020-

- Responding to concerns raised by the Motherboard investigation, Zoom removed the Facebook data collection feature from its iOS app and apologized in a statement.

30.03.2020-31.03.2020:

- An investigation by The Intercept found that Zoom call data was being sent back to the

company without the end-to-end encryption promised in its marketing materials and further a Zoom's spokesperson agreed to it stating that it was currently not possible to encrypt the data end-to-end on Zoom due to bugs. The true typed copy of the said article published by the intercept is being annexed herewith and is marked as **Annexure-P2 [Pg.50 to 62]**.

- After the discovery of a Windows-related Zoom bug that opened people up to password theft, two more bugs were discovered by a former NSA hacker, one of which could allow malicious actors to assume control of a Zoom user's microphone or webcam. Another of the vulnerabilities allowed Zoom to gain root access on Mac OS desktops, a risky level of access at best. The said information was published by 'appleinsider' and the true type copy of it is being annexed herewith as **Annexure-P3[Pg.63 to 66]**.
- A class-action lawsuit was filed against the company, alleging that Zoom violated California's new data protection law by not obtaining proper consent from users about the transfer of their

Zoom data to Facebook. The true typed copy of said information published in an article by 'Bloomberg' is annexed herewith and is marked as **Annexure-P4[Pg.67 to 69]**.

- The office of New York Attorney General Letitia James sent Zoom a letter outlining privacy vulnerability concerns, and asking what steps, if any, the company had put in place to keep its users safe, given the increased traffic on its network. The said information was published by the New York Times, true typed copy of which is being annexed herewith and is marked as **Annexure-5[Pg.70 to 74]**.
- Reporting cases of classroom Zoombombings, including an incident where hackers broke into a class meeting and displayed a swastika on students' screens, led the FBI to issue a public warning about Zoom's security vulnerabilities. The organization advised educators to protect video calls with passwords and to lock down meeting security with currently available privacy features in the software. The warning issued by the FBI on their website and true typed copy of it

is being annexed herewith and is marked as

Annexure-P6[Pg.75 to 77]

01.04.2020

- Elon Musk's SpaceX rocket company prohibited employees from using Zoom, citing "significant privacy and security concerns," as reported by Reuters.
- Reporting from Motherboard again revealed another damaging security flaw in Zoom, finding the application was leaking users' email addresses and photos to strangers via a feature loosely designed to operate as a company directory. The true typed copy of the said article by Motherboard is being annexed herewith and is marked as **Annexure-P7[Pg.78 to 82]**.
- The founder and CEO of the Zoom app issued a public apology in a blog post, and vowed to improve security. That included enabling waiting rooms and password protection for all calls. Further, it was assured that the company would freeze features updates to address security issues in the next 90 days. The true typed copy of the blog published by zoom on its

website is being annexed herewith and is marked as **Annexure P8[Pg.83 to 91]**.

02.04.2020

- It was revealed an automated tool was able to find around 100 Zoom meeting IDs in an hour, gathering information for nearly 2,400 Zoom meetings in a single day of scans, as reported by an American journalist who is said to be a cyber-security expert, Brian Krebs. The true typed copy of the article published by Brian krebs is annexed herewith and is marked as **Annexure-P9[Pg.92 to 100]**.
- The New York Times reported that a data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users.

03.03.2020

- Motherboard, meanwhile, discovered that users of 8chan forum (image board/message board forum available for online s but is majorly linked to child pornography, neo-nazism, racism, hate crimes, etc.) had planned to hijack the Zoom calls of a Jewish school in Philadelphia in an

anti-Semitic Zoombombing campaign. The true typed copy of said information published by Motherboard is annexed herewith and is marked as **Annexure-P10[Pg.101 to 104]**.

- An investigation by The Washington Post found thousands of recordings of Zoom video calls were left unprotected and viewable on the open web. A large number of the unprotected calls included discussion of personally identifiable information, such as private therapy sessions, tele-health training calls, small-business meetings that discussed private company financial statements, and elementary school classes with student information exposed, the newspaper found. That true type copy of the article published by the Washington Post is being annexed herewith and is marked as **Annexure-P11[Pg.105 to 113]**.
- Reporting from both CNET and The New York Times revealed social media platforms, including Twitter and Instagram, were being used by anonymous attackers as spaces to organize "Zoomraids" -- the term for coordinated

mass Zoombombings where intruders harass and abuse private meeting attendees. Abuse reported during Zoomraids has included the use of racist, anti-Semitic and pornographic imagery, as well as verbal harassment. The true typed copy of the news article published by CNET is being annexed herewith and are marked as **Annexure-P12[Pg.114 to 117]**.

- Zoom conceded that its custom encryption is substandard after a Citizen Lab report found the company had been rolling its own encryption scheme, using a less secure key instead of the more secure encryption it previously claimed to be using.
- Tycko and Zavareei LLP filed a class action lawsuit against Zoom, the second suit against the company, for sharing users' personal information with Facebook.
- Democratic Representative Jerry McNerney of California and 18 of his Democratic colleagues from the House Committee on Energy and Commerce sent a letter to the CEO of the Zoom App raising concerns and questions regarding

the company's privacy practices. The letter requested a response from Zoom by April 10. The copy of the said letter available on internet is being annexed herewith and is marked as **Annexure-P13[Pg.118 to 122]**.

04.04.2020-

- The CEO of Zoom in an interview with the Wall Street Journal gave another public apology stating that he failed as a CEO and also addressed how Zoom pushed for expansion in an effort to accommodate workforce changes during the early stages of the COVID-19 outbreak in China.

05.04.2020-

- In a statement, Zoom admitted that some video calls were mistakenly routed through two Chinese whitelisted servers when they should not have been.

06.04.2020-

- Schools in New York began banning teachers from using Zoom to teach remotely in the midst of the coronavirus outbreak, citing security and privacy issues surrounding the

videoconferencing app. New York's Department of Education urged schools to switch to Microsoft Teams as soon as possible. The true typed copy of the article published by CNET giving the said information is being annexed herewith and is marked as **Annexure-P14**[Pg.123 to 125].

- An Israeli B2B cyber intelligence company Sixgill revealed that it discovered an actor in a popular dark web forum had posted a link to a collection of 352 compromised Zoom accounts. Sixgill told Yahoo Finance that these links included email addresses, passwords, meeting IDs, host keys and names, and the type of Zoom account. Most were personal, but not all.
- In an open letter, the Electronic Privacy Information Centre, an independent non-profit research centre in Washington, D.C, urged the Federal Trade Commission to investigate Zoom and issue privacy guidelines for videoconferencing platforms.
- Sen. Richard Blumenthal, a Connecticut Democrat more recently known for

spearheading legislation that critics say could cripple modern encryption standards, called on the FTC to investigate Zoom over what he described as "a pattern of security failures and privacy infringements."

- A third class action lawsuit was filed against Zoom in California, citing the three most significant security issues raised by researchers: Facebook data-sharing, the company's admittedly incomplete end-to-end encryption, and the vulnerability which allows malicious actors to access users' webcams.

07.04.2020-

- Taiwan's government agencies were told not to use Zoom due to security concerns, with Taiwan's Department of Cybersecurity authorizing the use of alternatives such as products from Google and Microsoft. The true typed copy of said news information was published by ZDnet in an article and the same is being annexed herewith and is marked as **Annexure-P15[Pg.126 to 128].**

08.04.2020

- Zoom shareholder Michael Drieu filed a suit against Zoom and accused the company of having inadequate data privacy and security measures and falsely asserting that the service was end-to-end encrypted.
- In an email to employees, which cited security vulnerabilities, Google banned the use of Zoom on company-owned employee devices and warned against working of the app and a spokesperson of Google clarified that the Zoom app did not meet the required security standards. The said news information was published by Buzzfeed news in an article and the true typed copy of the same is being annexed herewith and is marked as **Annexure-P16[Pg.129 to 132]**.
- Hackers around the world have begun turning to bug bounty hunting, searching for potential vulnerabilities in Zoom's technology to be sold to the highest bidder. A Motherboard report detailed a rise in the bounty payout for weaknesses known as zero-day exploits, with

one source estimating that hackers are selling the exploits for \$5,000 to \$30,000.

- Zoombombing took a surreal turn when a Samsung engineer Zoombombed a colleague with an AI-generated version of Elon Musk.

09.04.2020-

- The US Senate told members to avoid using Zoom for remote work during the coronavirus lockdown due to security issues surrounding the videoconferencing app. The true typed copy of the news article giving out the said information published by CNET is annexed herewith and is marked as **Annexure-P17[Pg.133 to 135]**.
- Singapore's Ministry of Education said it's suspended the use of Zoom by teachers after receiving reports of obscene Zoombombing incidents targeting students learning remotely. Channel News Asia reported that the ministry is currently investigating the incidents. The true typed copy of the said information was published by CNA and is annexed herewith as **Annexure-P18 [Pg.136 to 139]**.

- The German Ministry of Foreign Affairs told employees in a circular to stop using Zoom due to security concerns. "Because of the associated risks for our IT system as a whole, we have, like other departments and industrial companies, also decided for the (Federal Foreign Office) not to allow the use of Zoom on the devices used for business purposes," the ministry said in a statement.

25. That another incident was reported when a popular daily public Zoom call was hosted by The Verge reporter Casey Newton and investor Hunter Walk. Suddenly, dozens of attendees were bombarded with disturbing imagery. A troll entered the call and screenshared horrifying sexual videos. Attempts to block the attack were thwarted as the perpetrator simply re-entered the call under a new name and screenshared more such clips. The hosts ended the call rather than subject viewers to the assault until they could stop it.

26. That the Indian Computer Emergency Response Team (CERT-In), India's nodal cyber security

agency, has also warned Zoom users of cyber risks and that the Zoom app is prone to cyber-attacks.

27. That on April 1st 2020, the Hon'ble Defence Minister of Union of India Shri Rajnath Singh posted certain pictures on twitter of his video conferencing with chief of Defence Staff General Bipin Rawat which raised privacy concerns regarding the government meetings and it was suggested by the NIC director Neeta Verma that 'vidyo' is much more safer than the Zoom app.
28. That there are alternative and much secure apps available for enabling the users to conduct meetings and conferences online. Some countries have suggested Microsoft Teams meeting, GoToMeeting whereas Indian Government is choosing Vidyo for their official work, both the apps being equally safe and following end-to-end encryption.
29. That after the advisory issued by Ministry of Home affairs through its cyber coordination committed on 12.04.2020 regarding the steps that need to be followed by the users if they are using Zoom App, some consumers although have switched to other apps but it is not out of place to suggest that India being so populated and especially now when every person is

locked down and every organization is using the video conferencing as remote form of communication, not all of them can be expected to be out of the risk as many wouldn't even be following the given steps in the said advisory. Guidelines dated 12.04.2020 issued by the Ministry of Home Affairs is being annexed herewith and is marked as **Annexure-P19[Pg.140 to 155]**.

30. That Further, the consumers are also using Zoom to socialize and keep in touch with friends and family during such crucial times. Almost every second person working from home considers Zoom to be synonymous with their everyday schedule. Schools and colleges are still using the said app and it will take sometime till all of them switch to any other app. The major population at risk is the youth which s=is anyway prone and vulnerable to such cyber bullying, cyber threats due to the overuse of cyber ecosystem. Hence, it will only be better if the said app is banned completely without any delay as it may give rise to several cases of cyber crimes and threats.

31. That there have been instances where students attending the classes are disturbing the online classes by gaining access to the camera and whiteboards to

display obnoxious pictures and comments. Such misuse was later blamed and pinned on the flaw in the zoom which gives access to the hackers online.

32. That on 16.04.2020 the Cyber Coordination Centre (CyCord), under the Union Ministry of Home Affairs (MHA), has issued an advisory on secure use of ZOOM Meeting Platform by private individuals who still want to use the said computer programme. This advisory states that the platform is not for use by Government officers/officials for official purposes.

The document makes reference to earlier advisories of the Indian Computer Emergency Response Team(Cert-In) and states that Zoom is not a safe platform.

The broad objective of this advisory is to prevent any unauthorized entry into a Zoom Conference Room and prevent the unauthorized participant to carry out malicious attacks on the terminals of other users in the conference. However, those guidelines are not sufficient and do not protect the citizens from data theft completely. Here it is pertinent to point out that the Zoom Meeting Platform is widely being used by the schools etc. to impart education during the

lockdown to students. The younger children who are students of lower classes, e.g., class I to XII are using the computer systems / smart phones of their parents, which in most cases have various sensitive information viz., online banking related information etc. and in case of data theft it is obvious that the loss caused would be catastrophic. Copy of Advisory dated 16/04/2020 issued by Ministry of home affairs on secure use of zoom platform are annexed herewith and is marked as **Annexure-P20[Pg.156]**.

33. That due to various privacy and security concerns till date following organizations and governments have banned the use of Zoom App:

- Australian Defence Force
- Berkeley, California (public school use)
- Canada (Federal government use that requires secure communications)
- Clark County, Nevada (public school use)
- German Ministry of Foreign Affairs
- Google
- NASA
- New York City (public school use)
- Singapore Ministry of Education
- Smart Communications
- SpaceX
- Taiwan (government use)
- United Kingdom Ministry of Defence
- United States Senate

34. That further Hon'ble Bombay High Court, which was earlier using zoom for video conferencing has stopped

using zoom and a fresh notice dated 17/04/2020 has been issued and a shift has been made from zoom to vidyo. Notice dated 17/04/2020 issued by Bombay High Court issuing fresh guidelines in respect to video conferencing are annexed herewith and is marked as **Annexure-P21[Pg.157]**.

35. This petition is far more comprehensive in terms of the coverage of the already reported instances as there are several instances coming up and being reported on a daily basis. Hence it is prayed that this petition may also be admitted and heard.

Grounds:

The petitioners have preferred the present Writ Petition, interalia on the following grounds:

- I. Because it is as important to have a safe and secure environment virtually as it is to have one in physical world.
- II. Because cyberspace risk is increasing everyday due to global connectivity and other online services which makes it easier to hack and access sensitive data of the users, be it private and confidential it is not that difficult to hack if a secure network is not used.

- III. Because usage of the said app has increased unexpectedly in the times of lockdown and it was neither prepared nor able to handle the sudden inflow of users in such heavy numbers.
- IV. Because there is a sudden rise in the incident of hacking and Zoombombing via Zoom App and the same has also been accepted by the founder of the said app.
- V. Because the zoom app gives rise to violation of Section 43 and Section 43A of Information Technology Act,2000, which states as follows-

“43. Penalty and compensation for damage to computer, computer system, etc.—If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,— (a) accesses or secures access to such computer, computer system or computer network [or computer resource]; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or

data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer

network; (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage; he shall be liable to pay damages by way of compensation to the person so affected.”

“43A. Compensation for failure to protect data.—Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.”

VI. Because the Zoom App also violates various rules of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

“24. Prohibition of interception or monitoring or decryption of information without authorisation.—

(1) Any person who intentionally or knowingly, without authorisation under Rule (3) or Rule (4), intercepts or attempts to intercept, or authorises or assists any other person to intercept or attempts to intercept any information in the course of its occurrence or transmission at any place within India, shall be proceeded against and punished accordingly under the relevant provisions of the laws for the time being in force.

(2) Any interception, monitoring or decryption of information in computer resource by the employee of an intermediary or person in-charge of computer resource or a person

duly authorised by the intermediary, may be undertaken in course of his duty relating to the services provided by that intermediary, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with the following matters, namely--

(i) installation of computer resource or any equipment to be used with computer resource; or

(ii) operation or maintenance of computer resource; or

(iii) installation of any communication link or software either at the end of the intermediary or subscriber, or installation of user account on the computer resource of intermediary and testing of the same for its functionality;

(iv) accessing stored information from computer resource relating to the installation, connection or maintenance of

equipment, computer resource or a communication link or code; or

(v) accessing stored information from computer resource for the purpose of--

(a) implementing information security practices in the computer resource;

(b) determining any security breaches, computer contaminant or computer virus;

(c) undertaking forensic of the concerned computer resource as a part of investigation or internal audit; or

(vi) accessing or analysing information from a computer resource for the purpose of tracing a computer resource of any person who has contravened, or is suspected of having contravened or being likely to contravene, any provision of the Act that is likely to have an adverse impact on the services provided by the intermediary.

(3) The intermediary or the person in-charge of computer resource and its employees

shall maintain strict secrecy and confidentiality of information while performing the actions specified under sub-rule (2).”

- VII. Because the Zoom app is totally in violation to the Right to Privacy i.e. Article 21 of the Indian Constitution. Indian constitution defines the privacy as personal liberty in Article 21. “Protection Of Life and Personal Liberty” No person shall be deprived of his life or personal liberty except according to procedure established by law. However, it is not wrong to suggest that Data collection, storage and access without letting the user know is nothing but infringing their fundamental right of privacy. The base line of privacy in cyberspace still remains blurred but it is nothing but a fact that data protection in cyberspace is the most essential form of privacy one seeks while accessing the internet and if an app cannot even assure its consumers of such data protection and rather sends out the data, it is the safest to ban such app. Because the right to privacy would include privacy online and

offline and the zoom app violates this right of its users and further the people hacking the meetings would only misuse such data giving rise to cyber threats.

VIII. Because according to the Data Security Council of India, it was recently reported that in the recent past, there has been a significant increase in cyber threats, and if the situation is not addressed, this could impact the GDP of the country, massively. The average cost for a data breach in India has risen up to 7.9% since 2017, with the average cost per breached record of INR 4,552.

IX. Because it is pertinent to mention that though the Indian Government have multiple times tried to take steps for data privacy online by introducing National Cyber Security Policy and bringing Personal Data Protection Bill, 2019, nothing till date has successfully been implemented regarding the cyberspace. If now this app is not banned in time it is only going to take disadvantage of the said fact and further cause threat to the Indian cyber ecosystem.

- X. Because despite various media channels, digital e-media and print media reporting about security issues in the said App and the hackers taking advantage of it on day to day basis but no concrete and firm step has yet been taken to ban the app.
- XI. Because there have been numerous reported incidents all over the world regarding the cyber threats and cybercrimes being done through Zoom App.
- XII. Because continued usage of this app may put our national security at stake and may also give a boom to number of cyber-threats and cybercrimes in India.
- XIII. Because in 2018, India was ranked third in the list of countries where the highest number of cyber threats were detected, and second in terms of targeted attacks in 2017, according to security software firm Symantec and since the countries much ahead of ours in terms of cybersecurity have banned the said app it will only be sensible to do the same.

- XIV. Because there are alternative, securer and much more reliable apps present for the same purposes and services being provided by Zoom App.
- XV. Because the continued use of this App is only making the users vulnerable and prone to cyber threats as the same is being done in online classes by showing pornographic images and giving hate speeches instigating the users which might leave any child of such tender age scarred for a very long time.
36. Because the Petitioner has not filed any other Petition/Petitions with similar or same reliefs before any Court, including this Hon'ble Court or any other Court.
37. Because this Hon'ble Court has adequate territorial jurisdiction to issue directions, orders and writs given the case of action in whole and in part arises within the territories in which it exercises jurisdiction.
38. Because the Petitioner has no other equally efficacious alternative remedy and therefore, the

Petitioners are approaching this Hon'ble Court by filing the present petition. The facts warrant interference of this Hon'ble Court under Article 32 of the Constitution of India.

Prayers

IN THE PREMISE THIS HON'BLE COURT MAY KINDLY BE PLEASED TO:

a) issue a Writ of Mandamus or any other appropriate Writ order or direction in the similar nature thereby directing the Respondent nos. 1 and 2 to carryout an exhaustive technical study into the security and/or privacy risks of use of 'zoom' for official and personal purpose by the public;

b) issue a Writ of Mandamus or any other appropriate Writ, order or direction in the similar nature thereby directing the Respondent nos.1 and 2 to ban the use of 'zoom' for official and personal purposes by the public until an appropriate legislation is put in place;

c) To pass any other order which this Hon'ble Court
deems fit and appropriate in the matter.

AND FOR THIS ACT OF KINDNESS, THE
PETITIONERS AS IN DUTY BOUND SHALL EVER BE
GRATEFUL.

DRAWN BY:
NIMISH CHIB
DIVYE CHUGH
ADVOCATES



FILED BY:

[Wajeeh Shafiq]

ADVOCATE FOR THE PETITIONER

DRAWN ON: 19.04.2020

FILED ON: 20.04.2020