DE JURE NEXUS LAW JOURNAL

Author:

Saksham Rai

IMS Law College, Noida

5th Year, BA LL.B.

PLEA AGAINST ZOOM IN SUPREME COURT-ANALYSIS

Abstract

In the times of distress because of the pandemic, zoom seems to be acting as a helping hand during this era of fear. From calling to your friends to look up to them or by simply calling to parents when you are living alone in the alien city, zoom seems to be working fine until there were some serious loophole found in the app. In the recent light of events, privacy was a main concern people found during the use of this app followed by the plea in the Supreme Court by Mrs. Harsh Chugh to ban zoom app by claiming that this app poses a threat to privacy of the individuals who are using it and also it breaches cyber security. Many countries and organizations have already abandoned the use of this app like Google, Space X, NASA, United Kingdom and Taiwan etc. The petition has also impleaded other stake holders responsible – the Centre through the Ministry Of Electronics and IT and Cyber and Information Security Division of MHA (Ministry Of Home Affairs). The CEO of ZoomVideo communications has already apologized publicly and accepted the app to be faulty in terms of providing a secure app digitally which is against the norms of Cyber Security.

Arguments made in the plea

- The petitioner, Mrs. Chugh is a tutor by profession and she finds zoom app to be violating the article 21 of the Indian Constitution (no person shall be deprived of his life or personal liberty except according to the procedure established by law).

- Zoom app is the most overused app for video conferencing, chats and webinars and it is available free in the app stores so hence it is easy to misuse.

- 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 prevention of cyber crime and 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 petitioner has serious concern towards the use of this app. Zoom app uses data hoarding and cyber hoarding which includes mass storage of personal data in its cloud recording and zoom was found to be sending data to Facebook, even if the users weren't logged in to a facebook account causing breach of privacy of the people.

- Zoom is making profits from this pandemic and prioritizing profit over people and has falsely advertised end to end encryption. In end to end encryption, your messages, photos, videos, documents are all secured from falling into the wrong hands. Zoom is reported to have a bug that can be abused intentionally to leak information of users to third parties.

- Zoom has been found to route its internet traffic to china, where the internet is closely monitored by their government hence there is a chance of leaking confidential information to the neighbor country.

- The joining in the zoom app is easy by just clicking a simple URL thus, leading to incidents of **Zoom Bombing** where a stranger can join zoom meetings and share objectionable content. It is important to realize how Zoom consistently violates its duty to implement and maintain reasonable security practices and misleads consumers about the security benefits of the product.

- Zoom market has grown from 10 million in December 2019 to 200 million in march 2020 and the founder **Eric S Yuan** has accepted the fact that his company was not prepared for the inrush of the users.

- Even the Cyber Coordination Committee has issued a public advisory that the app is not safe and is not end to end encrypted yet it is still receiving data of the user in a full-fledged manner.

- During this pandemic zoom app has targeted schools, colleges, tuition centers. There have been reports of various incidents that occurred during teaching session in school/colleges where some strangers were found to be using some pornographic sounds, images infringing the privacy of the students and causing a feeling of uneasiness among students.

- The younger children who are students of lowers 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.

- Many major countries have banned the use of Zoom app like Australia, Taiwan, Canada, United Kingdom, Singapore and organizations like NASA, Space X etc have already banned the use of this app.

- It said that there is a need for a legislation to be put in place in order to effectuate a standard regulation to safeguard the rights of citizens as has been brought to light by

various leaders across the world. The plea has sought a direction to the Centre to carry out an exhaustive technical study into the security and privacy risks of using Zoom application.

- The plea submitted to further ban the use of this app for personal and official use by issuing a Writ of Mandamus directing to Union Of India through Ministry of Electronics & Information technology and one of the respondents, cyber & Information Security, Division of Ministry Of Home.

Right to privacy

It seems to be saddening that although India got its freedom back in the 1947, it took more than 70 years to grant its citizens, the freedom of being alone. The Right to Privacy unlike in U.S, was not deemed to be an absolute right and hence, there followed a number of cases in the Indian Courts until year 2018, when the Hon'ble Supreme Court, in the **Puttaswamy Judgment** held privacy as an inviolable and non-negotiable right.

The Supreme Court has asserted that Article 21 is the heart of the fundamental rights. Article 21 has proved to be multi-dimensional. The extension in the dimension of the article 21 has been made possible by giving an extended meaning to the word "life and liberty" in Article 21.

Article 21- "No person shall be deprived of his life or personal liberty except according to a procedure established by law". First of all we need to put emphasis on the meaning of Right to Privacy. According to Black's law dictionary - right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters which the public is not concerned.

What zoom is doing is letting the users to live with the fear that they are being monitored and are prone to the hackers and their data is not safe. That at any time user knows that Zoom Bombing can happen with them or with their children, that there is a chance of suffering from banking fraud from this app yet this app is still running.

Article 21 secures two rights

- Right to life and

- Right to personal liberty.

Justice K.S. Puttaswami (Retd.) and Anr. vs Union Of India And Ors.

In august 2017, a nine-judge bench of the Supreme Court in Justice K.S. Puttaswami (Retd.) vs Union Of India held that the people of India have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under article 21. It held that privacy is a natural right that inheres in all the natural persons, and that the right may be restricted only by state action that passes each of the three tests:

- State actions must have a legislative mandate.
- It must pursue legitimate state purpose.
- It must be proportionate i.e., such state actions both in the nature and extent, must be necessary in a democratic society and the action ought to be the least intrusive of the available alternatives to accomplish the ends.

Critical analysis

Zoom has failed to protect the user's privacy. Infringement of someone's privacy will only lead to the termination of the app. At first zoom was able to capitalize from this pandemic leading it to make 200 million users from 10 million in just 4 months. At first people were intrigued by this app but after people began realizing that just because it offers mass people to join in the video conferencing it is not worth to peril one's privacy.

India's cyber security agency C.E.R.T. (Computer Agency Response Team) has cautioned against the vulnerability of the app from cyber attacks including leakage of sensitive office information. Zoom has the technical ability to spy on private video meetings and would be compelled to hand over recordings of meeting to government or law enforcement in response to legal requests.

Here are some Data Protection Laws that can be asserted in breach of privacy:

Information Technology Act, 2000

It deals with the issues relating to the payment of compensation (Civil) and punishment(Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Penalties for breach of privacy and confidentiality

Section 72 of the Information Technology Act- It provides any person who, in pursuance of any of the powers conferred under the **IT Act Rules** or Regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or any other material without the consent of the person concerned, discloses such material to any other person shall be punishable with imprisonment of a term which may extend to two years, or with fine which may extend to Rs 1,00,000 or with both.

Information Technology Amendment Act, 2008- The Information Technology Amendment Act, 2008 is a substantial addition to India's Information Technology Act, 2000. The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In). The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The following sections have been inserted by the IT Amendments Act, 2008-

Section 43A – Compensation for failure to protect data

Section 66C: Punishment for identity theft.

Section 66D: Punishment for cheating by personation by using computer resource.

Section 66E: Punishment for violation of privacy.

Section 66F: Punishment for cyber terrorism.

Section 67: Punishment for publishing or transmitting obscene material in electronic form.

Section 67C: Preservation and retention of information by intermediaries.

Section 69A: Power to issue direction for blocking of public access of any information through any computer source.

Conclusion

There's also been a lot of scrutiny about Zoom's privacy policy, which until recently seemed to give Zoom the right to do whatever it saw fit with any user's personal data, and its encryption policies, which have been more than a tad misleading that created a backlash against Zoom. People say that it is safe to use Zoom by disabling certain functions though the company has come up with so many solutions, there is a lurking doubt in the minds of people and they are looking for other options. People continue to use Zoom because it is easy and free. Zoom has found massive success in the dark time of the world and it will try to maintain that position, although doing so will require prioritizing user's privacy and security over ease of use. Nothing is precious then one's privacy, this plea has made to the headlines because it connected people to their friends, family, business but if doing so will cause hindrance in the privacy of the people then it can face major consequences in near future.