A closer look at the Privacy Policies of Video-Conferencing Apps/Software
written by Rajeev Rambhatla | May 14, 2020

Where does our Privacy Stand with Video Conferencing Apps?

"The times, they are changing" are words that were famously written and sung by Bob Dylan a little less than six decades ago, but these words are truly coming to life now in the wake of the current circumstances. The SARS CoV2/ Covid-19 or Novel Corona Virus ("the virus") as its better known is the new variation of the Corona Virus which has taken over the world and is showing no signs of backing down anytime soon.

The virus which originated from China sometime around November 2019 has quickly spread to other parts of the world causing a devastating impact in some of the world's most technologically advanced countries such as Italy, Spain, the USA, France, and the UK amongst others. India and several other Asian countries have been affected as well but various efforts are being taken to try and curb the virus while valiant efforts are being made to develop either a cure or a vaccine.

Unprecedented times such as these usher in unprecedented changes, in a bid to tackle the virus and ensure continuity various businesses, and people across the world have started practising social distancing and consequently encouraged their employees to work from home wherever possible. This is possible because of the availability of video conferencing tools and other remote means of communication, which have seen our homes transform into office spaces. They also help us human beings stay connected with friends and family, regardless of where they are on the planet.

The increase in the adoption of video conferencing tools over the course of the last few weeks has been impressive. Microsoft's video and audio chat service, Skype, has witnessed a 70% increase of daily users compared to one month ago, with 40 million people using it on a daily basis[1]. The other tools like Cisco's Webex Meetings and Zoom have also reported record usage of their services over the last two months[2]. Video conferencing tools enable us to virtually access the outside world from the safety and comfort of our homes.

While we appreciate how video conferencing tool providers facilitate this, it is equally important for us to ensure the safety of our digital footprint and the data that is being shared with these various video conferencing platforms. This article aims to analyze the privacy policies of two major platforms, Zoom and Vidyo while also trying to analyze their interplay with proposed laws in India such as the Personal Data Protection Bill, 2019 ("PDP Bill") and existing international covenants such as the General Data Protection Regulation ("GDPR").

Zoom

Zoom is an immensely popular video conferencing app available for personal computers as well as other smart devices such as smartphones and tablets. Zoom's privacy policy and terms and conditions that are provided on its website are rather comprehensive and clear about the data that is taken from

its users and how that data is used. Most of the information is collected at the time of signing up/registration. This is the basic information such as the account owner's name, business address, email address, username, etc. In turn, this information is used for creating a customer account, responding to support requests, and otherwise communicating with customers. Zoom's privacy policy specifically mentions that it does collect customer content like information uploaded, provided, or created while using Zoom. This includes text messages exchanged on the platform, cloud recordings, whiteboards, files, and other information shared while using Zoom's service. This information is said to be used for providing Zoom services, storage of chat logs, storage of recordings if explicitly required by the host or customer, and for storage of voice mail for Zoom phone, which is another one of Zoom's unique offerings. Zoom has a separate modality for its marketing sites. If you visit them and provide information, then that information can be used for the purposes of advertisement and marketing.

However, despite this, Zoom has repeatedly insisted that it does not sell user data. Interestingly, Zoom's privacy policy makes a special mention of compliance with legal obligations such as detecting, investigating, and stopping fraudulent, harmful, unauthorized, or illegal activity.It also states that the data collected by it may be disclosed while responding to a valid legal process.

Zoom claims to use end-to-end encryption, however, it has drawn severe flak from the general public as these claims have been found to be untrue. End-to-end encryption would render all communication content only visible to the actual participants and not to the service providers, something which is indeed appreciated from a privacy perspective. However, Zoom's claims have been shown to be misleading and false as it does not actually use end-to-end encryption as commonly understood, but only transport layer encryption that leaves the communication content visible to Zoom[3].

Similarly, Zoom appears to also have poorly implemented its "Company Directory" feature, leaking both email addresses and photos[4]. However, one key feature that Zoom provides is that it allows recording of the video calls conducted on its platform either locally on the user's device or Zoom's cloud. It is advisable to save these locally, as an individual user's device is less likely to be compromised.

Zoom has recently been in the news for the wrong reasons as well. The Government of India has issued circulars to various government departments asking them to avoid using Zoom and it has further been categorized as unsafe and dangerous. Zoom has gone the extra mile and published its security measures on its website and it also enlists the measures it is taking to protect user privacy in a separate post on its website. This is indeed a welcome step, as any user who is using Zoom is now provided with a simple interface to understand the infrastructure in place to keep their conversations private and ensure their privacy.

Vidyo

Vidyo is a relatively newer app/software which is in the same space as Zoom, Skype, and other video conferencing service providers. In fact, Vidyo is the app that is also used by the Hon'ble Supreme Court of India for taking up urgent matters through video conferencing. Vidyo's privacy policy *prima facie* doesn't appear to be as crystal clear or transparent as Zoom's as the terminology used by Vidyo is a little vague and not entirely accurate which

is not a good thing when it comes to framing privacy policies.

It says it collects “many kinds of information” in order to ensure that it offers and improves the quality of its services which it provides. Further, instead of being crystal clear about collecting information about a user who visits its website and uses its services, the phrase that Vidyo uses is “may collect” which is a slightly worrying sign for its users as the usage of the word “may” creates unnecessary ambiguity and confusion in the mind of the user.

Privacy policies should be precise and simply state the information the companies are collecting, why they are collecting it, and with whom they are sharing it. In fact, the data that Vidyo collects as per its own definition is inclusive and not exhaustive thereby wavering away from the concept of data limitation. Ideally, such information should be collected with the user’s consent.

Vidyo’s usage of the word “may” while stating that it might automatically collect and store certain information about the user's usage of and interaction with Vidyo’s services is not a welcome sign. More importantly, it states that it will store a user’s Call Data Records, which will contain details pertaining to a particular user’s calls and other specified device and internet-related data concerning that particular user. Interestingly, like Zoom, Vidyo also provides a feature that allows a participant to record the content of video conferences and text messages exchanged on the platform. In the event a user decides to use this feature, a notice will appear on the user’s screen which reads Vidyo “may” collect and store the content of such video conferences and instant messaging communications. Vidyo can make use of the information such as an individual user’s Call Data Records to provide tech support and can also take remote access to any user’s device to help resolve issues which in the long run sounds like it will create more issues than it will resolve.

Thankfully, this is limited only to the providing of technical support, and there is no indication that they will take remote access in any other situation. According to its privacy policy, the information Vidyo collects may be used for the following:

- Providing its products and services;
- In connection with ongoing customer relationships such as providing customers with information about software updates, etc.;
- Evaluating and improving products and services;
- Operating and evaluating websites as well as customizing and improving its marketing activities; and
- To comply with legal or governmental requirements or demands.

Despite the convenience factor and the safety factor, Vidyo seems to be the preferred communication platform of the Government as opposed to Zoom.

Conclusion - Privacy Stand with Video Conferencing Apps

India’s proposed PDP bill and the GDPR both emphasize video conferencing platforms to have clear-cut and defined privacy policies that make governance easier for the authorities as well as ensure that users of such apps are at peace with regard to their privacy. Zoom as it appears despite being called unsafe by the Indian Government seems to have an airtight privacy policy that has not only been evolving and going through updates constantly but Zoom also takes the extra efforts of providing tips and other security measures on its website which puts the minds of its users at ease when it comes to their

privacy while using these apps/software.
Vidyo on the other hand despite being the first choice of the government seems to suffer from ambiguity and uncertainty in terms of its privacy policy and there is no clear mention anywhere in Vidyo's privacy policies or its terms and conditions that user data will not be sold or used otherwise for commercial gain by the service provider.
This lack of clarity is likely to make a user prefer Zoom over Vidyo and this is probably the reason behind Zoom's popularity despite the setbacks and also the reason for Vidyo's lack of popularity which goes to show that for users using these video conferencing solutions, the top-most priority is safety and privacy of their information and their overall digital presence.

- [1] Ian Sherr, "Microsoft's Skype sees massive increase in usage as coronavirus spreads" (cnet, 30 March 2020), accessed 31.03.2020.
- [2] Jordan Novet, "Cisco says Webex video-calling service is seeing record usage too, even as competitor Zoom draws all the attention" (CNBC, 17 March 2020), accessed 31.03.2020.
- [3] Micah Lee, Yael Grauer "Zoom meetings aren't end-to-end encrypted, despite misleading marketing" (The Intercept, 31 March 2020), accessed 5.5.2020, available at https://theintercept.com/2020/03/31/zoom-meeting-encryption/
- [4] Joseph Cox "Zoom is leaking peoples' email addresses and photos to strangers" (Motherboard, Tech by Vice, 1 April 2020), accessed 5.5.2020, available at https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addressesphotos

Contributed By - Rajeev Rambhatla
Designation - Head - Hyderabad
King Stubb & Kasiva,
Advocates & Attorneys
Click Here to Get in Touch
New Delhi | Mumbai | Bangalore | Chennai | Hyderabad | Kochi
Tel: +91 11 41032969 | Email: info@ksandk.com