Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG POLICY BRIEF

Covid-19 Spurs Quest for Indian Video Conferencing Platforms

Author

Abhimanyu Ghosh

Volume V, Issue 23

JUNE 15, 2020

Delhi Policy Group

Core 5A, 1st Floor, India Habitat Centre, Lodhi Road, New Delhi- 110003

www.delhipolicygroup.org

Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG Policy Brief Vol. V, Issue 23
June 15, 2020

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

Author

Brig. Abhimanyu Ghosh (Retd.), Senior Fellow for Cyber Security and Digital Technologies, Delhi Policy Group

The views expressed in this publication are those of the author and should not be attributed to the Delhi Policy Group as an Institution.

Cover Photographs:

Prime Ministers Narendra Modi and Scott Morrison attending the India India-Australia Virtual Summit on June 04, 2020. Source: PMIndia

Prime Minister Narendra Modi participating in the Virtual Summit of the Non Aligned Movement (NAM) Contact Group called to discuss response to the COVID-19 pandemic on May 04, 2020. Source: PMIndia

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003.
www.delhipolicygroup.org

Covid-19 Spurs Quest for Indian Video Conferencing Platforms

by

Abhimanyu Ghosh

Contents

Covid-19 Spurs Quest for Indian Video Conferencing Platforms

by
Abhimanyu Ghosh

Introduction

The Covid-19 pandemic sweeping across the globe has brought normal life to a standstill. Even with the partial lifting of prolonged lockdowns in India, a number of restrictions remain in place. Meanwhile, norms of social distancing at workplaces have become necessary. Across the globe, governments, businesses and institutions have adjusted to a new normal of "working from home".

In the prevailing scenario, digital video and data connectivity has provided essential workplace solutions, with almost all institutions resorting to digital platforms for their routine functioning. Seeing the continuing spread of the pandemic, this situation is unlikely to change anytime soon. Video conferencing platforms are providing a sense of 'alone together', boosting social and professional solidarity.

Prime Ministers Narendra Modi and Scott Morrison attending the India India-Australia Virtual Summit on June 04, 2020. Source: PMIndia

There are several global video conference platforms vying with each other to capture this business space; virtually all of them, including Microsoft Teams, GoTo Meeting, WebEx, Google Meet etc. have experienced an exponential surge in their exploitation. Among all these platforms, Zoom has emerged as the most popular, mainly because of its user-friendly features. In 2020 alone,

Zoom has added 2.2 million new users each month, outstripping its entire 2019 new user base of 1.19 million. Zoom has surpassed its revenue guidance as well as analysts' forecasts, reporting year-on-year growth of 169 percent in its April, 2020 quarterly revenue to $328.2 million from $122 million a year-ago.

Security Issues with Video Conferencing Platforms

This explosive surge of Zoom's popularity has also brought to light the security flaws of these platforms. In March 2020, a new verb was created - 'Zoom bombing' - referring to the practice of uninvited users crashing into conversations and making threatening or obscene calls. In April, 2020 the Indian Computer Emergency Response Team (CERT-IN) issued advisories that multiple vulnerabilities have been reported in video conferencing applications which could allow an attacker to obtain sensitive information on the targeted system. This followed media reports that 500,000 Zoom accounts had been sold on the dark web anonymously. Around the same time, an advisory was also issued by the Union Home Ministry asking government officials not to use this application and advising all users to take certain precautions.

Prime Minister Narendra Modi participating in the Virtual Summit of the Non Aligned Movement (NAM) Contact Group called to discuss response to the COVID-19 pandemic on May 04, 2020. Source: PMIndia

Based on these developments, a writ petition was filed before the Supreme Court of India on May 20, 2020 seeking a ban on the use of the Zoom video conferencing application by Indian citizens, claiming that it breaches privacy. The petition stated that Zoom does not have end-to-end encryption and is violating the Information Technology Act, 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and

Decryption of Information) Rules, 2009. It called for legislation to be put in place in order to effectuate a standard regulation to safeguard the rights of citizens.[1] The Supreme Court has issued a notice to the Government on May 22, 2020 on the writ petition. The next hearing is tentatively scheduled for July 7, 2020.[2]

The security flaws which have been pointed out are not necessarily limited to Zoom; most video conferencing platforms have the following common flaws:

- Not using meeting codes with passwords to prevent intrusion, which leads to breaches like 'zoom bombing' or the hijack of meetings.

- Attackers joining meetings uninvited; sending malicious links in chat to extract information; and shared content being stolen using third parties.

- Lack of end-to-end encryption to preserve privacy of meetings. Normally AES-256 encryption is implemented to keep sensitive information shared during video calls secure. For corporate customers, the issue of encryption is especially important, be it to safeguard valuable company information or to meet privacy obligations to customers.

Indian Initiatives

The security and privacy flaws which have been highlighted in these platforms during the Covid-19 pandemic have given rise to consideration of national video conferencing solutions.

On April 14, 2020 the Ministry of Electronics and Information Technology (MeitY) launched an "Innovation Challenge" for indigenous alternatives to address security and privacy issues of global video conferencing platforms. This "Innovation Challenge" is being held in three stages - ideation, prototype building and finally solution building. Under the "Digital India Programme", MeitY has called upon India-based developers to create an application with the primary function of video-conferencing. There has been an enthusiastic response from companies, start-ups and academia. As part of the first stage of the selection process, on May 25, 2020 the government has shortlisted ten companies, among them HCL Technologies, Zoho Corp and People Link.[3] These companies will receive INR 5 Lakhs ($6618) each from the government to develop a prototype of a product similar to global counterparts.

[1] https://telecom.economictimes.indiatimes.com/news/plea-in-sc-seeks-to-ban-zoom-video-conferencing-app-claiming-it-breaches-privacy/75852700
[2] https://www.medianama.com/2020/05/223-supreme-court-zoom-india-ban/
[3] ET BUREAU | UPDATED: MAY 25, 2020,

Meanwhile, the government is also separately developing its own secure video-conferencing platform. The responsibility to develop a platform for use by government officials, the judiciary and the public has been entrusted to the Centre for Development of Telematics (C-DoT).[4] C-DoT's video conferencing platform will expand on all features of overseas rivals like Zoom and Microsoft Teams and is said to be almost ready for deployment.

Thus far, the National Informatics Centre (NIC) has been providing video conferencing services to the government since 1995. These services are available from about 1800 existing studios spread across the country including in state capitals, union territories and districts. NIC provided services are being used for monitoring of various Government Projects, Schemes, Covid-19 pandemic management and even international virtual conferences.

Indian Start-Ups

Besides these government platforms, several start-ups are independently developing viable Indian alternatives for corporates to choose from, depending on their reliability. These also need to be encouraged and incentivised.

One of these is 'Say Namaste', developed by Mumbai based start-up Inscript. On June 08, 2020 it was reported that the 'Say Namaste' video conference platform, fully developed in India, is now available on both the Google Play Store as well as Apple Store. Earlier, it was available only on the browser Google Chrome.[5] This app comes with features such as screen sharing, text mode and file sharing, similar to Zoom and other video platforms. The app is just 23 MB in size and currently has more than 100,000 downloads on the Google Play Store. It supports up to 50 participants. On both the Google Play Store and the Apple Store, the app is listed with 4.5 stars.[6]

Another such platform is 'Bharat.Live', which claims to integrate privacy and security. It is a browser-based application, with secure log-in and password. The site does not ask for email ID; no chat or records are stored on servers as of now. The trusted cryptographic standards like AES 256-bit encryption and TLS (Transport Security Layer) SSL encryption are in place to increase network security. This platform is Health Insurance Portability and Accountability Act (HIPAA) compliant and conforms to General Data Protection Regulation (GDPR) safeguards, enhancing its acceptability in the global market. It claims secure user authentication, proper information storage and reports generation

[4] https://economictimes.indiatimes.com/tech/internet/hcl-peoplelink-zoho-among-10-cos-in-zoom-rival-race/articleshow/75955326.cms
[5] www.saynamaste.in accessed on 21 April 2020.
[6] https://indianexpress.com/article/technology/tech-news-technology/say-namaste-india-video-conferencing-app-on-google-play-store-6448332/

with access control, audit controls, integrity controls and transmission security.[7]

The third such Indian platform is 'AIRMEET', which is an online meeting and event hosting platform where instead of simply broadcasting the event, participants can connect with other event attendees for one-to-one and one-to-many online interactions. 'AIRMEET' is scalable and offers options such as virtual tables, networking lounges, backstage, stage, claps and audience reactions to participants, to recreate a live atmosphere online. This Bengaluru-based virtual meet-up start-up, founded in 2019, has recently announced that it has raised $3 million in funding.[8]

Implications for India's National Security

There are several companies involved in the development of a video conferencing platform, including the ten selected by the Government. These efforts do not preclude international IT companies offering secure applications to be deployed in the Indian business space.

While corporates and citizens may be satisfied with upgraded technical privacy and security controls provided by these companies, policy makers may need to worry about the challenges posed to India's national security. Most video conferencing companies store conference audio-video-text data, originated in India, beyond the jurisdiction of India. Such platforms are accountable to local laws in which the data is stored and the companies are registered. For instance, Zoom recently suspended the account of a group of US-based Chinese activists, after they held a video meeting on the platform to commemorate the Tiananmen Square crackdown on May 31, 2020. Zoom said that the account had been closed to comply with "local laws".[9] This can happen to any Indian group or institution at critical times, if the host country so desires.

There are thus two requirements of national security that stand out prominently. First, the need for a viable and popular 'Made in India' Video Conferencing Platform with secured Data that is accountable to Indian legal and regulatory requirements. Second, the need for effective coordination among Cyber Security stakeholders at the national level to provide the required synergy for development and deployment of a secure Video Conferencing Platform.

[7] https://www.outlookindia.com/newsscroll/bharatlive-this-uttarakhand-startup-has-made-a-zoom-alternative-in-just-20-days/1823157
[8] https://entrackr.com/2020/04/airmeet-provides-an-alternative-to-zoom-for-hosting-large-events/
[9] https://www.bbc.com/news/world-asia-53003688

Data Security

As reported by the media, Chinese servers are being used to store conference data and to distribute encryption and decryption keys for video links on Zoom. Also, even after the recent updates on Zoom, only paying users can opt for 256-bits encryption and to keep data outside the purview of Chinese laws, by geofencing Chinese servers. In the backdrop of India's deteriorating relations with both China and Pakistan together with the continuing standoff in Ladakh, the possibility of cyber espionage through access to such data cannot be ruled out. Similarly, other global platforms have their own designated data centres in several countries, subject to the laws of those host countries.

These platforms are intermediaries that need to be guided by Indian laws, rules and regulations which would require the service providers to ensure privacy, confidentiality and privilege of sensitive, commercial or financial information. For law enforcement, Security Agencies should be able to ask for lawful interception from intermediaries via the Telegraph Act (Section 5(2) or Rule 419(a)), the IT Act (Section 69 or Rule 3(7) Intermediary Guidelines Rules, 2011)), or the CrPC (Section 91). But implementation becomes difficult when these companies are not registered in India and data is stored abroad. Data needs to be protected, as per laws of our country, without compromising on the security and privacy of its customers.

India is in the process of finalising a Draft Personal Data Protection Bill (PDPB-2020). The Bill is the first legislation that focuses on the privacy of citizens and could potentially result in a significant overhaul of digital businesses and companies. Platforms being developed should adhere to the PDPB-2020 for business and personal entities and conform to the requirements of national security. One live copy of the data that originates in India on these platforms should be kept in the jurisdictional territory, so that the laws of the land can prevail. Also, for these companies, purpose limitation of data while taking consent from users is necessary. These aspects need to be incorporated at the design and development stage itself, before these platforms are publicly deployed.

Coordination: Synergy of Efforts

Development of these platforms is being technically steered by the Ministry of Electronics and Information Technologies (MeitY) as part of the 'Innovation Challenge' and also independently by several startups taking advantage of the surge in demand for Indian alternatives. It is imperative that this innovation is harmonised with global technology standards and national security norms. A consortium approach is suggested to bring complementary skill sets of the start-ups together to build a robust product. The recent example of the hurried

launch of Indian Apps that were taken down by the Google Play Store has embarrassed many.

Coordinated responses to the security and privacy challenges of video conference applications, through a whole of government approach, is required. The security evaluation should be conducted by a team of designated Agencies, under the aegis of the National Cyber Security Coordinator (NCSC). It is recommended that the Coordinator should synergise these efforts, in collaboration with MeitY, to develop and deploy Indian video conferencing platforms, but without unnecessary bureaucratic overreach.

Conclusion: The Way Forward

Security and privacy breaches with the Zoom Video Conferencing Platform have been a wakeup call for Indian Cyber Security establishment. The announcement of the "Innovation Challenge" for Indian companies to develop a "Made in India" product is a welcome development. The fact that a number of Indian startups have taken up the challenge is encouraging. These platforms should be secure, robust and accountable. The ecosystem should promote informed choice for customers - government, corporate, educational or private - for the best suited product. Developing a secure and reliable product will be the key to validate the 'Aatmanirbhar' slogan by providing Indian alternatives to global products.

***

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org