stratechery.com /2020/zooms-genuine-oversight-zooms-strengths-and-weaknesses-virality-versus-network-effects/

Zoom's "Genuine Oversight", Zoom's Strengths and Weaknesses, Virality Versus Network Effects

11-13 minutes

Good morning,

A bit of an earnings break to talk about a company we are all becoming very familiar with.

On to the update:

Zoom's "Genuine Oversight"

From The Verge:

> Zoom has admitted it doesn't have 300 million daily active users. The admission came after The Verge noticed the company had quietly edited a blog post making the claim earlier this month. Zoom originally stated it had "more than 300 million daily users" and that "more than 300 million people around the world are using Zoom during this challenging time." Zoom later deleted these references from the original blog post, and now claims "300 million daily Zoom meeting participants."
>
> The difference between a daily active user (DAU) and "meeting participant" is significant. Daily meeting participants can be counted multiple times: if you have five Zoom meetings in a day then you're counted five times. A DAU is counted once per day, and is commonly used by companies to measure service usage. Only counting meeting participants is an easy, somewhat misleading, way to make your platform usage seem larger than it is.
>
> The misleading blog was edited on April 24th, a day after the numbers made headlines worldwide. After The Verge reached out for comment from Zoom, the company added a note to the blog post admitting the error yesterday, and provided the following statement:
>
> > "We are humbled and proud to help over 300 million daily meeting participants stay connected during this pandemic. In a blog post on April 22, we unintentionally referred to these participants as "users" and "people." When we realized this error, we adjusted the wording to "participants." This was a genuine oversight on our part."

"A genuine oversight", just like Zoom "mistakenly added our two Chinese data centers to a lengthy whitelist of backup bridges" (link), or "incorrectly suggest[ed] that Zoom meetings were capable of using end-to-end encryption" (link), or "implemented the 'Login with Facebook' feature using the Facebook SDK for iOS (Software Development Kit) in order to provide our users with another convenient way to access our platform" without being "aware…that the Facebook SDK was collecting device information unnecessary for us to provide our services" (link), or secretly installed a local web server on Macs without "an easy way to help a user delete both the Zoom client and also the Zoom local web server app on Mac that launches our client [which] was an honest oversight", and "misjudged the situation and did not respond quickly enough" (link). Every single quote and link is from the Zoom blog.

Of course, to Zoom's credit, in nearly every instance the issues raised were fixed, often with exceptional speed. I last wrote about the company on April 1, arguing that Zoom needed a full security reset from the top down; CEO Eric Yuan committed to doing just that the same day, and has followed up, as promised, with weekly updates about Zoom's progress, and regular updates of Zoom clients addressing issues. That speed, though, makes me worried about whether or not Zoom can ever truly stop making these "mistakes".

Zoom's Strengths and Weaknesses

One of my favorite axioms about life — and it applies to both companies and individuals — is that strengths and weaknesses are often two sides of the same coin. Apple excels at integrated devices, and struggles with online services; Amazon builds incredibly scalable services and delivered the worst phone I've ever used; Google devises brilliant technical solutions at Internet scale and couldn't build a social network if its corporate life depended on it; Facebook connects everyone for good, and connects everyone for bad, much as Twitter surfaces valuable information, and is the mechanism for both disinformation and mob justice. Strengths and weaknesses, yin and yang, two sides of the same coin.

So it is with Zoom: on one hand the company moves incredibly quickly, fixing problems within days; on the other hand, is there anyone that has confidence that Zoom is actually doing a careful evaluation of how said problems were allowed to happen in the first place, and making changes in its processes to anticipate issues before they occur? How many problems in the future will result from hot fixes made today, which were probably to fix problems caused by moving rapidly in the past?

That is why the "genuine oversight" that resulted in 300 million participants being classified as 300 million users is a bit dispiriting, even beyond the material implications for the company's stock price: it suggests the same lack of care and oversight that led to the company's other missteps is endemic to Zoom's culture. It's not just engineering, it's not just operations, it's not just marketing: it is all of the above. It really was impressive how quickly Yuan responded to Zoom's PR crisis, but that speed has both upsides and downsides, and as long as those downsides include a lack of rigor and attention to detail these stories are going to continue — and corporate IT buyers, who actually need to pay Zoom in order to justify the company's valuation, are going to notice.

The worst part about this latest episode, though, is the lack of transparency in terms of correcting the mistake. Major kudos to *The Verge* for noticing the change, and major thanks to the Internet Archive for recording the change (donate!), because otherwise Zoom was apparently content to let its investors make decisions on wrong information without any proactive attempt to correct the record. And, unfortunately, as recorded above, this too seems to be a pattern: Zoom ignored and downplayed the security implications of that local server, suggested its security issues were due to being an enterprise app (when in fact most arose because of Zoom adopting consumer-app-like approaches), and misstated its encryption policies. How can anything the company say be trusted?

This would be a problem for all companies, but it is especially a problem for Zoom given its China exposure. Yuan wrote in a post on Zoom's blog yesterday:

> Recently, questions have also been raised about Zoom and China. At first, this seemed to stem from a temporary misconfiguration in our global data center routing that we fixed. But outside of that isolated incident, in the past few weeks, we have seen disheartening rumors and misinformation cropping up. I would like to set the record straight here.
>
> - I became an American citizen in July 2007.
> - I have lived happily in America since 1997.
> - Zoom is an American company, founded and headquartered in California, incorporated in Delaware, and publicly traded on NASDAQ (ZM).
> - Zoom is also a global company, with 21 offices around the world, including in the UK, Australia, Japan, France, and elsewhere. More than half of our employees are based in the United States.
> - Similar to many multinational technology companies, Zoom has operations and employees in China. And like many multinational technology companies, our offices in China are operated by subsidiaries of the U.S. parent company. Our engineers are employed through these subsidiaries. We don't hide this. On the contrary, we disclose this type of information in our public filings, as appropriate. Our operations in China are materially similar to our U.S. peers who also operate and have employees there.
> - Among our 17 global co-located data centers, we have 1 (one) co-located data center in China. This data center is in facilities run by a leading Australian company and is geofenced. Its design ensures meeting data of users outside of mainland China stays outside of mainland China. It exists primarily to satisfy our Fortune 500 customers that have operations or customers in China and want to use our platform to connect with them.

Points 1-4 and 6 are all perfectly valid; the issue is point 5, which unfortunately exhibits the duplicitousness I just fretted about. Saying that Zoom's China operations "are materially similar" to other U.S. tech companies is probably true on an absolute basis; as of its most recent 10-K Zoom had "more than 700 employees" in research and development centers in China. Assuming that other U.S. tech companies have a similar number of employees in China then this statement is correct. Those other companies, though, have many more employees *outside* of China, particularly in engineering; that is a very different situation that having “a high concentration of research and development personnel in China” and a “product development team [that] is largely based in China”, as Zoom’s 10-K notes.

The issue is what happens if the Chinese government were to ever come knocking, asking Zoom or some number of its employees to insert a vulnerability or a back door? It is very hard to argue that Zoom’s stringent review practices and strict oversight would prevent that from happening, given that those things don’t exist. And, unfortunately, if Zoom would prefer to silently edit material information in a blog post, it is very hard to believe that Zoom would volunteer information about government interference.

China is a huge strength for Zoom — I suspect the company’s operations there are related to its ability to move fast, all with lower costs than its peers — but it also is a significant weakness. Zoom admits in its 10-K that even the perception of China being a security issue is a risk factor, and the company’s mistakes and lack of transparency are contributing to making that risk a reality.

Virality Versus Network Effects

This all might not matter if Zoom were able to use the massive surge in usage to create network effects that lock users into the service. That’s the thing though: Zoom is so popular and so viral in part because it has no network effects. Only a host needs an account; everyone else just clicks a link.

Sure, it is likely they will have a good experience with Zoom — it really is so much better than competitors, not just in terms of features but especially peformance, both on the computer and over the network — and will be likely to become hosts in their own right. That’s exactly what we have been seeing happening, and it is to Zoom’s benefit: it is getting massive trial while the product is materially better.

But, given Zoom’s security issues, it is also to its detriment. To switch to another solution, whether because you yourself are concerned about Zoom’s security, or more likely because your CIO is, takes nothing more than changing a link on a calendar invite. Yes, the experience is worse, because Teams or Webex or GoToMeeting or Google Meet aren’t as good, but without a real barrier to switching Zoom could lose ~~users~~ participants — especially paying ones — as quickly as it adds them; strengths are weaknesses.

This Daily Update will be available as a podcast later today. To receive it in your podcast player, visit Stratechery.

The Daily Update is intended for a single recipient, but occasional forwarding is totally fine! If you would like to order multiple subscriptions for your team with a group discount (minimum 5), please contact me directly.

Thanks for being a supporter, and have a great day!