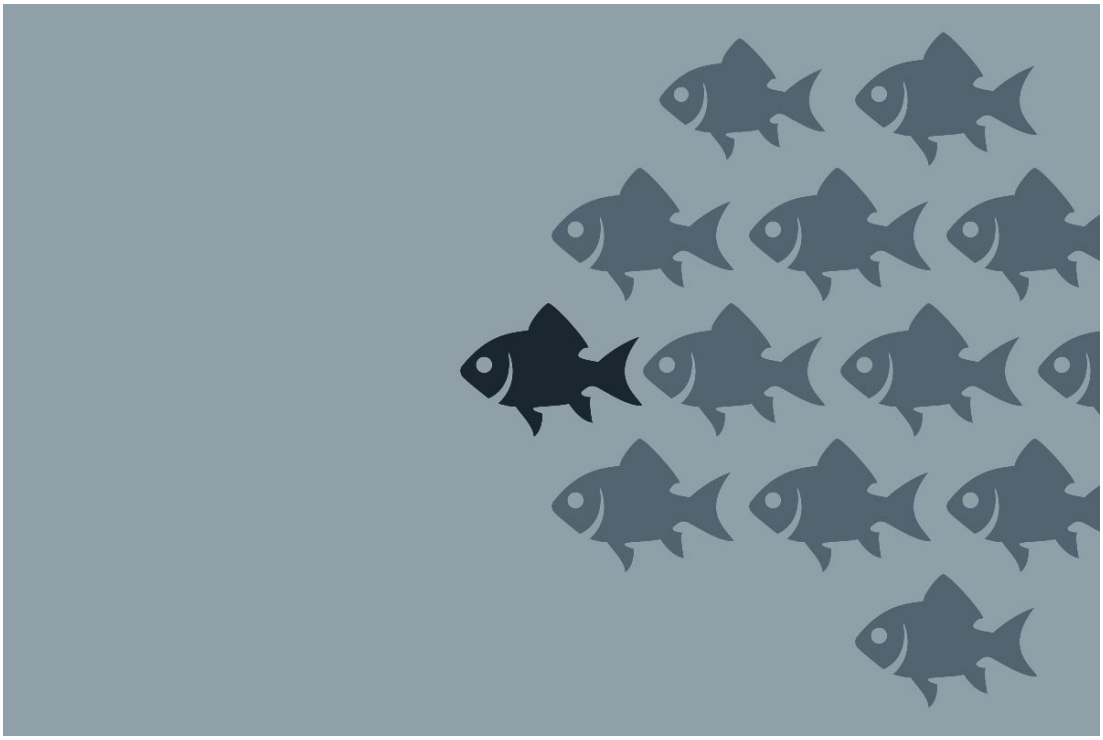
California Management Review

STRATEGY

Decoding the Envelopment Challenge

by Sai Prakash R. Iyer



How multi-sided platform businesses can understand and respond to envelopment attacks

INSIGHT | FRONTIER 25 Apr 2021

During recent decades, Multi-sided Platform (MSP) business models have become more prominent. Some of them such as Airbnb have overtaken market leaders in valuation within a decade of founding. The leaders have been following Linear Value Chain (LVC) business models where value flows in one direction – from suppliers to customers through the business. MSP

businesses add value by facilitating transactions (or interactions) between two or more groups of users,[1] such as guests and hosts for Airbnb. MSP businesses are characterized by non-linear value flows and the presence of positive network effects.

Network effects set MSPs apart from LVCs in their growth dynamics. More users on one side attract more users on the other side. Think of how Airbnb becomes more valuable to a host when there are more potential guests in the platform. MSPs grow at breathtaking speed by riding on the upward spiral of user adoption on one side, and bringing in users on the other side. Double digit month-on-month growth is the norm among successful MSPs while LVC businesses struggle to stay at high single-digit annual growth. Eight out of the ten most valuable corporations in 2020 have adopted MSP business models. Twenty years ago, only one out of top ten did so.[2]

Network effects is a double-edged sword though. If users find the platform not so great, the spiral can change direction and the MSP quickly loses most of its users. Entrepreneurs running MSP businesses have a good reason to lose sleep over fear of losing their userbase. New and interesting MSP business ideas being tried out by startups quickly get copied, and some of the prominent copycats are the largest MSPs – the big brothers.

A common piece of advice given to entrepreneurs building MSP startups is to *get big fast*. If they don't, a big brother who is dominant in an adjacent MSP market will enter their market and swallow them by integrating its core offerings and operations with those in the target market – an *envelopment attack*.[3] Well known examples include how Microsoft pushed RealNetworks out of the market for media server software or how it killed Netscape's browser. Envelopment attacks are a competitive threat to the targeted MSP as the big brother will deploy its superior resources and capabilities including its readily accessible userbase to quickly absorb the target's users and transactions. If the targeted MSP's userbase falls below a threshold, it will implode.

Fear of being enveloped is among the key drivers for the impetus of MSP managers to grow their userbase quickly and by whatever means possible. As a result, they tend to ignore metrics more relevant for long term success such as favourable unit economics and profitability. In the process, they undermine the survival of the venture they are trying to protect.

Typical recommendation to targeted MSPs to ward off an envelopment attack is to match the attacker's integrated or bundled offering, either on its own or through an alliance with partners including rivals of the attacker.[4] Reciprocal entry into attacker's market is an extreme measure for the targeted MSP as it is likely to be at a disadvantage on resources and capabilities including financial clout. Even well-heeled targets might find it daunting to mount a reciprocal attack.

Consider Netflix trying to enter online retail or theme parks against the entry of Amazon or Disney into video streaming. How can the targeted MSP respond to or preempt an envelopment attack? In order to make a determination, the targeted MSP must understand the nature and scope of potential envelopment attacks.

Defending from Envelopment

The big brother brings to battle a wide array of resources and capabilities such as intellectual property, physical assets, human capital, financial resources, channel presence and so on. Of particular importance for an MSP business model would be the attacker's userbase. The nature and scope of an envelopment attack can be understood through two factors. First is the extent of overlap of target market userbase with the attacker's core market userbase. Second is the degree of integration of product / service offerings and operations that the attacker is likely to achieve between its core market and the target market.

Common Userbase

Having common userbase helps the attacker in multiple ways. The attacker can hit the ground running, as it can easily solve the challenge of platform ignition – onboarding the critical mass of users faster and easier. Recall that number of users drives value of a platform to its users due to network effects. The attacker's platform would be more valuable to users compared to the targeted MSP due to larger userbase, triggering an exodus of the targeted MSP's users to the attacker's platform. The targeted MSP is now faced with the challenge of fizzle – loss of users below a threshold, which can lead to implosion.

Commonality in userbase is not just about *who* the users are. It's about how users are represented in the databases of the two MSPs. Even if the two MSPs have the same individuals as users, the attacker's userbase would have low commonality if data on users has limited overlap. Take for instance Google, which entered payments in 2006 – an envelopment attack on PayPal. The logic for the attack was that Google already had consumers using its search engine to look for products, and this userbase would become one of the sides of Google's payment platform – the side that pays for online purchases through PayPal.

In reality, PayPal's consumer-side dataset was very different from that of Google's search user dataset. While PayPal had highly specialised payment-relevant information about its consumer-side users such as bank account or credit card details and purchase history, Google knew them

from their online search history and had limited financial data, at least then. The reason that consumer-side users went to PayPal was to make payments, especially to pay merchants with whom they weren't willing to share their bank or card data. The reason users went to Google was to find information. The *job-to-be-done*[5] of PayPal's consumer-side was very different from that of Google's search users, as a result the data that these platforms had on its users was also different.

The second side for PayPal's platform was merchants selling online. Many of these merchants were already present in Google as advertisers. So while there was good commonality on the merchant-side with PayPal, Google had limited commonality of userbase on the consumer-side, making the overall commonality of userbase low. In hindsight we can see that Google's initial foray into online payments fizzled due to low adoption among consumer-side users.

Commonality in userbase needs to be assessed on the basis of the type of user data attacker has about target's userbase compared to what's needed to do business in the target market. Commonality in userbase has to be aggregated across various sides of the target MSP's business to get the overall commonality.

The higher the overall commonality of userbase, the easier it will be for the attacker to solve the ignition challenge and build its userbase in target market.

Integration of Offerings and Operations

The attacker can integrate its offerings and operations across the two markets which will result in substantial advantage in the target market through superior value proposition to users and higher profitability through better efficiencies. Even when potential for integration in offerings or operations is limited, the attacker could tactically bundle its offerings across the two markets to gain users.

Integration of Offerings

Full integration of core and target market offerings could pose a serious threat to the target MSP, as the value proposition from integrated offering is likely to be vastly superior to targeted MSP's standalone offering. During the late 1990s, RealNetworks was dominating the media streaming server business with a market share of more than 90%, while offering RealPlayer free to PC users. Microsoft enveloped RealNetworks's streaming server market by integrating streaming server functionality into its Windows NT server operating system. In addition, it provided Windows Media

Player free with its PC operating system. Real's clients had to go for Windows NT or one of its rivals for their enterprise needs. The added functionality of media streaming made Windows NT a compelling option for Real's potential clients, and most of them went with Windows NT.

Full integration of offerings is rare due to technical or organizational constraints. More often, attackers resort to partial integration of offerings across core and target markets. Given that most MSP businesses are digital and make heavy use of mobile apps and online portals, a common approach to partial integration is to create deep links between the user apps or portals for the two markets.

Zomato, a restaurant discovery and table booking platform, entered the local food delivery market in India with a separate app for the new service. It created deep links between its core app for restaurant discovery and the new one for food delivery, allowing users to move seamlessly from one service to the other. Primary users of either platform could effortlessly use the other. Gojek and Jio have over time added many new offerings to their core app (termed super apps) enabling users to access an ever increasing range of products and services from a single integrated interface.

Allowing users to leverage common user-facing capabilities is another approach to partial integration of offerings. Ola's ride-hailing customers can pay for food delivery orders placed with Food Panda (a subsidiary of Ola in India) through Ola Money, the parent's prepaid wallet. Partial integration provides users incremental improvements while full integration will likely result in substantially superior offerings.

The more integrated the offerings across the two markets are, the more compelling the value proposition will be to the target's users.

Integration of Operations

The attacker can integrate its value chain across the two markets to achieve better efficiencies and the ability to offer lower prices, which in turn would make the offering more compelling to target's users. The attacker can use its core MSP resources and capabilities in transaction management and fulfilment in the target market. Improved efficiencies would arise from economies of scope as well as learning.

Swiggy, one of the leading food delivery startups in India, built a dedicated delivery fleet along with robust scheduling and navigation capabilities, with which it delivered consistently high customer experience. However, daily and weekly fluctuations in number of orders meant fleet idle time for a

number of hours a day. Swiggy started offering local delivery of medicines and groceries as well as peer-to-peer local delivery to improve fleet utilization. Swiggy's move resulted in an envelopment attack on the likes of Dunzo who focused on peer-to-peer local delivery market.

The more relevant the core market resources and capabilities are for the target market, the higher the efficiency improvements that attacker will obtain from integration of operations.

Uber uses its scheduling and navigation capabilities honed through ride hailing business in its local delivery operations. Jio uses its payment platform JioPay across multiple MSP businesses that it operates such as JioMart, AJio, NetMeds, etc.

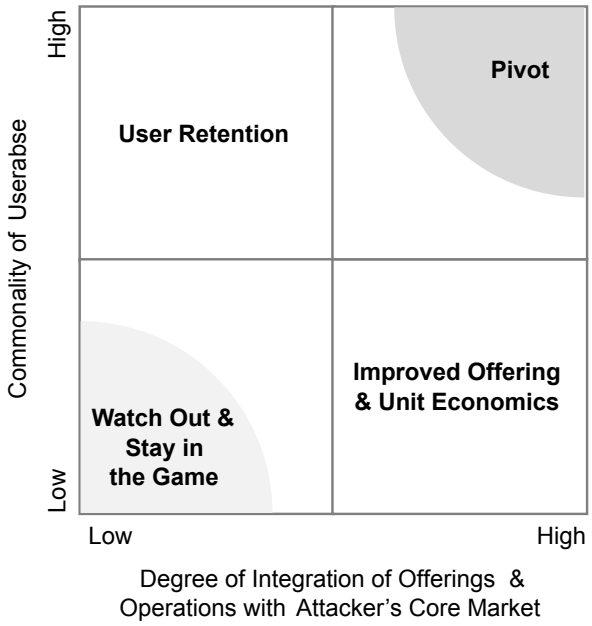
The more generic the resources and capabilities are, the more relevant and valuable they will be, across different MSP markets.

In scenarios with limited scope for integrated offerings or operations, the attacker can choose to bundle, primarily as a tactic to take away customers from targeted MSP. Tactical bundling indicates that the attacker may not derive significant long run advantage from presence in both MSP markets. If the attacker comes with deep pockets, as most dominant MSPs are likely to do, bundled pricing as a tactic can be a way to trigger a war of attrition, with the aim of driving the targeted MSP out of cash and out of business.

The less the potential for integration of offerings or operations, the more the tendency of the attacker to rely on tactical bundled pricing to win the target market.

Types of Attacks & Appropriate Responses

It is essential for a targeted MSP to assess commonality of userbase with the attacker and how the attacker might integrate its core offerings and operations with that in target market. Comparing the unit economics of attacker's core MSP business and the likely unit economics of attacker post-envelopment with the target's own unit economics will give valuable insights on how the attacker is likely to compete. With this, the target MSP can look at effective counter measures.



Tactical Bundled Pricing: Watch Out & Stay in the Game

Tactical bundling is often resorted to by the attacker when there is limited overlap of userbase and low potential for integration in offerings or operations across the core and target markets. The attacker's unit economics post-envelopment won't show a significant advantage. The intent of the attacker would be to trigger a war of attrition, draw in the target and bleed them to exit or fire-sale.

The targeted MSP's response should be to stay in business by focusing more on its own offerings and operations, along with adequate funding to stay in the game. The attacker will have to solve the ignition challenge of getting enough users on board. The offering is not likely to be significantly superior to that of the targeted MSP. Given this, a wait and watch approach is appropriate. PayPal kept its course when Google launched its online payment platform in 2006, and waited to see Google's attack fizzle out, at least in that round.

User & Transaction Grab: User Retention

The attacker may enjoy high commonality of userbase but with limited ability to integrate offerings or operations. Here, the attacker is likely to press its better ability to access users to drive up adoption of its offering, resulting in the targeted MSP losing users. The attacker's offering and unit economics would at best be marginally better than that of the targeted MSP given the low to medium scope for integration of offerings or operations.

In this scenario, the priority for the targeted MSP is to protect its userbase and transaction volumes. Users of MSPs often *multihome*, meaning they are concurrently active in more than one competing platform. Many of us carry multiple credit cards in our wallet and there is high chance that we would have at least one card each from providers such as Visa, Mastercard, Amex, JCB etc. For an MSP, the problem with multihoming is that each time a customer wants to transact, she can choose from among the MSPs that she is active in. This heightens the rivalry among MSPs to capture each transaction. MSPs try to discourage multihoming by rewarding their customers for repeated transactions with loyalty incentives. One way for the targeted MSP to limit the ability of the attacker to quickly build its userbase is to discourage multihoming. In addition, as a second priority, it helps the targeted MSP to improve its offerings to its customers.

Faced with envelopment attack by Zomato, Swiggy embarked on a cloud kitchen initiative called Swiggy Access to discourage multihoming by its restaurant-side users. Restaurants who signed up for Access were able to set up delivery-only kitchens with minimal investments to capture demand from geo-locations they weren't present. From the Access kitchen, the restaurant can only deliver through Swiggy.

Better Offering & Lower Cost: Improved Offering & Unit Economics

This scenario is the flip side of earlier one. Here, the attacker is able to achieve considerably high levels of integration in offerings or operations resulting in superior value proposition and unit economics and lower price. But it has to work its way up the spiral of user adoption as user commonality would be low. The targeted MSP's first priority is to double down and improve its offerings so that it can stay comparable with the offering and cost that attacker will bring to its market. Its second priority would be to improve retention of userbase and transaction volumes.

When UberEats launched in Mumbai, it provided a new feature – scheduled deliveries. A rider in Uber could order food and its delivery will be coordinated with the rider's arrival at destination. Swiggy had been following a first-in-first-out fulfilment logic, as scheduled deliveries would increase the complexity and cost of its operations. To counter the improved offering from UberEats, Swiggy quickly launched Swiggy Schedule which allowed customers to specify delivery times up to two days ahead.

Fully Integrated Envelopment: Pivot or Transform

With full integration and high commonality, the attacker brings vastly superior offering at significantly better unit economics, posing a serious threat to the targeted MSP. This is likely the only scenario where the targeted MSP could explore the option of reciprocal entry into attacker's core market, either on its own or by allying with partners such as a competitor of the attacker. Even then, differences in resources and capabilities would impose serious limits on the targeted MSP's ability to benefit from a reciprocal entry.

More feasible for the targeted MSP would be to pivot away from the market that the big brother is about to gobble up. Is that a victory? Not really. But then, you don't want to fight a battle that you can't survive. Living to fight another day makes more sense.

RealNetworks was practically kicked out of the streaming media server market when it was enveloped by Microsoft with its Windows NT. Rather than a reciprocal entry into the market for operating systems, Real pivoted to media streaming as a subscription service with RealRhapsody.

Assessing the extent of commonality in userbases, understanding the attacker's resources and capabilities and evaluating its relevance for target MSP market, being able to judge potential integration opportunities for the attacker by entering the target MSP's market, and assessing comparative unit economics are some of the critical analyses that will help the targeted MSP gain insights into the nature and scope of envelopment and how to respond. In any case, as long as the targeted MSP's customer value propositions for its users remain superior even after envelopment, its users would continue to prefer it over competition.

1. Andrei Hagiu. "Multi-sided platforms: From microfoundations to design and expansion strategies", HBS Working paper 07-094, 26p. ↩

2. **https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization#2020** ↩

3. Thomas Eisenmann, Geoffrey Parker & Marshall Van Alstyne. "Platform envelopment", Strategic Management Journal, 2011, Vol.32(12) p.1271-1285. ↩

4. *Ibid.* p.1282-83. ↩

5. Clayton M. Christensen, Taddy Hall, Karen Dillon, and David S. Duncan. "Know your customers' "Jobs to be Done"", *Harvard Business Review*, Sep 2016. ↩

Sai Prakash R. Iyer Follow

Prof. Sai Prakash R. Iyer is Adjunct Professor of Business Policy & Strategy at the Indian Institute of Management Udaipur, India where he offers MBA electives on advanced competitive strategy and multi-sided platform business models. He brings more than two decades of experience spanning academics, management consulting and industry.