Why it is almost impossible to ban Uber and Ola in India

Pranesh Prakash

2014-12-10

Quartz India

Abstract

Preventing bookings through mobile apps is difficult.

On Dec. 8, days after a woman accused her Uber driver of rape, an under fire Delhi government exercised the most convenient option—it banned Uber.

But ordering Uber, Ola, TaxiForSure and similar companies to discontinue their services in Delhi until they get taxi licenses does not seem to have worked. These services are still available in the national capital.

After all, these aggregators do not offer a taxi service, but in fact provide an information service with both riders and drivers as customers. Some of them work exclusively through mobile phone apps, while others also take taxi requests through call centre operations.

What's common between them—and differentiates them from Meru, Easy Cabs, and your neighborhood cab companies—is that they operate services that trade information and not services renting out their cars and employee drivers: they don't own any of the capital goods (such as the cabs, etc.), nor are the drivers their employees.

So what can the government do to shut down such a service, which operates virtually?

It can seek to interrupt the communications channels that are used by them.

For instance, given the wide leeway that telecom licenses provide the Department of Telecommunications, the department can require telephone operators to take down the phone lines used by Olacabs for its bookings.

Preventing bookings through mobile apps is more difficult, and requires other avenues.

First, the government can "sniff" the traffic emanating from these apps, figure out the servers that these apps are communicating with, and attempt to block the IP addresses used by these servers.

However, when I sniffed the traffic from Uber, I found it came from IP addresses 54.238.155.186, 104.36.192.152, and 97.64.122.27 —addresses that correlate not only with Uber's own servers, but also Amazon Web Services and a hosting service called Peak Web Hosting. The same goes for Olacabs, which used a content distribution network called Fastly, along with Amazon Web Services.

Given this, it is practically impossible to block these services alone without accidentally blocking other services. The fact that these large content distribution networks and cloud services cannot be blocked without over-blocking can also be used to circumvent censorship in repressive societies: a report (pdf) by David Robinson and Harlan Yu calls this tactic "collateral freedom."

Aside from blocking servers, the government nudge Google and Apple—the two main distributors of these taxi service apps—to prevent these apps from being downloaded, and also to retroactively delete these apps from people's phones.

It would, however, be very difficult (although within the realm of possibility) to accurately target users from Delhi—by getting IP address from ISPs operating in Delhi. Realistically, it is unlikely that Google or Apple would oblige the government on such a request.

At any rate, all these technological means, even if deployed with sophistication, can be defeated by the users—both riders and drivers—using "virtual private networks" or VPNs, or obfuscation techniques like the Tor/I2P networks, which prevent any restrictions at the ISP level from being effective.

Apart from Uber, these services offer the option of payment by cash, so it is next to impossible to actually shut them down either technologically or financially. However, Uber, which relies on a pre-paid wallet service (Paytm) or a foreign credit card, could be targeted this way.

The fact that it is technologically difficult to block access to these services does not mean that an intelligent and nuanced conversation on appropriate regulation of these services is unnecessary or futile. Having such as debate is needed—not just in India, but across the world.