THE INFRASTRUCTURE OF INCLUSION AND EXCLUSION: ACCESSING THE "PRIVATE INTERNET" FROM MAINLAND CHINA

Fan Mai
University of Virginia

Introduction

There is a growing research literature on the technical aspects of internet censorship and circumvention, but the user's experience with circumvention tools has received less attention. Empirical data about the use of circumvention tools, especially in countries that engage in substantial web filtering, is hard to find. Measuring the use of circumvention tools is inherently difficult given that the function of these tools is to protect the identity of the users. There are a few exceptions. Since 2007, researchers from the Berkman Center for Internet & Society at Harvard University have conducted in-depth evaluations of prominent filtering circumvention tools. Relying on data collected from website visits, search terms and self-reported information from the service providers, researchers at the Berkman Center estimated that less than 3% of internet users, in countries (including China) that engage in substantial filtering, use any circumvention tools. They also indicated that the actual number of the users is likely to be considerably less than this estimate (Roberts, Zuckerman, and Palfrey 2011).

Comparing the estimate from the Berkman Center with my own findings, this question emerges: why is the adoption rate of proxy services is much higher among Western expatriates than among the general population of internet users in China? When studying the specific role of structure in affecting people's consumption preferences, researchers have to consider the factors of availability of the media product in the market, and of users' awareness enabled by the media environment (Webster 2009). This chapter first investigates the market that provides the VPN services, followed by a discussion of how expatriates learn about their circumvention options, especially the adoption of VPN service, in the Chinese context.

Overview of the circumvention tools

Circumvention technologies emerged in 1996 with Bennett Hazelton's Peacefire, which was designed to evade filtering within high schools and universities in the United States.
Filtering practice has become more generalized, and adopted by various players for different reasons. Governments may use filtering techniques to control web content not published within their national borders. Schools and businesses may filter their local connection to the internet. Many websites filter their own content according to the geographic location of the users. For example, the on-demand internet streaming media site Netflix blocks access by users in countries outside America and Europe. With increasing institutional control over the Internet, the interest in finding technical solutions to internet censorship is widespread around the world.

There are various techniques to cope with media censorship. Becker (2011: 172-187) outlines and classifies active transgressive mechanisms into two major categories: the first is technical strategies, including the use of proxy servers, virtual private networks, tunneling, circumventor pages, pictures instead of text, and peer to peer networks; the second group is linguistic and communicative strategies, including translating characters into Pinyin, exclusive use of numbers, exchange characters based on pronunciation, and the use of internet languages. Becker suggests that using the technical strategies requires a higher level of technological competence, while the linguistic and communicative strategies are the most popular among internet users. Here, I want to develop Becker’s theory to suggest two other important dimensions that differentiate these two mechanisms: 1) Technical strategies are primarily used for access-censored platforms and web contents associated with the platforms, while linguistic strategies are mainly used for content-creation and content-sharing which do not directly address the access issue with the media platforms where these contents are published. 2) Although technical strategies might require higher technical competence, an important part of media literacy, linguistic and communicative strategies require a higher level of cultural competence, especially language skills. It is worth noting that the result reported by the circumvention project at the Berkman Center only considered the use of technical strategies, while the practice of linguistic and communicative strategies was studied thoroughly in research on Chinese internet users (see references like Yang 2009).

Use of proxy services is one kind of technical strategy to bypass network filtering. By means of this method, the user is connected to the blocked website through third party sites that are not blocked themselves. A potential issue in all proxy services is that these third party sites can be blocked just like content and other sites. Despite this core similarity, proxy services may differ significantly in many implementation details. Using the typologies developed in the 2010 Circumvention Tool Usage Report published by the Berkman Center, proxy services can be further divided into categories based on their proxy implementations and their model of financial support: blocking-resistant tools, simple web proxies, VPN services, HTTP/ SOCKS proxies. While some of my respondents mentioned their knowledge and experience with simply web proxies, particularly the one called Freegate, the majority of them use the VPN services. Therefore, in the following, I focus particularly on the analysis of the VPN services.
As one type of proxy services, VPNs use virtual private network software to encrypt and tunnel Internet traffic through a proxy machine that allows remote access and remote control (Steward 2013). Unlike the simple web proxy, VPN services tunnel all Internet traffic. Therefore, in addition to web browsing, they can be used for email, chat, and any other Internet-based service. It can also be used on mobile devices. The principle of VPN service is to extend a private network across a public network such as the Internet. This service enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

VPN service is widely adopted by mobile employees to access their company’s intranet securely while being geographically distant from the office. It allows employees to work from anywhere by creating one cohesive virtual network. This is worth noting because VPNs are often adopted by business users to access corporate intranets and many governments are reluctant to block the VPN traffic (Palfrey 2011). Using VPN service can also protect the identity of ordinary Internet users. VPN encrypts the web data, including the IP address, making it unreadable to the third parties, including the Internet Service Providers. General discussion of VPN use is centered on “network security,” emphasizing privacy concerns over content accessibility. For example, Astrill, a popular global VPN service provider, advertised its service on major portal website this way, “a VPN creates a secure internet connection where your internet provider sees only encrypted data, and the final destination sees only Astrill location and IP information.”

Other VPN providers also advertise their service as privacy-focused, claiming that they do not track or monitor user activities when a VPN service is used. While VPN service provides great mobile connectivity and confidentiality, the major limitation is the speed of the intermediary network link (Steward 2013). Meanwhile, VPN service can be blocked either by blocking the protocols used to set up a VPN connection, or blocking the IP address in use.

### Selling “Internet Freedom”

In the Chinese context, accessing blocked web contents is the major reason for using a VPN service. According to the latest tracking results provided by GreatFire.org, a non-profit organization that closely monitors internet censorship in mainland China, there were 157 websites in the top 1000 most visited site list that have been blocked in mainland China. These blocked websites include Youtube, Facebook, Twitter, Blogger, WSJ and many other major social media and news sites. This censored media environment creates a real challenge for people in China, especially for Western expatriates who used to frequent these sites on a daily basis. Many respondents have complained about how the Chinese media environment makes them feel particularly disconnected. One respondent says:

1. https://www.astrill.com/
3. The top 1000 most visited site list is provided by Alexa
“If you don’t seek out news in America, it will still come to you. But if you don’t seek out news in China, news won’t come to you. So I was just in the bubble for most of the time when I was here. Now it is much better with VPN.”

Another respondent voiced the same concern, “I exposed to less news in China. I feel very disconnected from everything until I got the proxy, you need, foreigners need VPN to feel like they are using the Internet.” When I asked my respondents what kind of media devices they couldn’t live without in China, several of them responded without much thinking, “the VPN.” In the Chinese context, the use of VPN service becomes the major gateway for reconnecting with the “real” Internet. In other words, from the expatriates’ perspective, the Internet may not exist in China without using VPN service. The quality of VPN service is even considered as one key factor, among expatriates, to measure their overall quality of life in Chinese cities.

(Created by Jim Fields, 2015)

Since VPN service plays such a crucial role in expatriates’ lives in China, it is important to understand how the service is provided and by whom. It is extremely difficult, if ever possible, to get a complete list of available VPN service providers. Researchers at the Berkman Center have spent over a hundred hours searching the Internet for advertised VPN services and then surveyed each of the services for their daily and monthly usage numbers. According to their report, published in 2011, they have found 134 VPN service providers. I used a different approach here to locate VPN service providers. Since my interest is not to survey all available VPN services but to compare those service providers actually used by expatriates in China, I relied on self-reported data from my respondents and information provided by popular expatriate websites to generate a list of VPN providers that are popular among Western expatriates in China. I have included

4 This meme was shared widely among expats through social media, such as at: http://offbeatchina.tumblr.com/post/110545100596/how-to-calculate-your-happiness-in-beijing
11 VPN service providers in the table below. All of these VPN services are found to have a substantial user base in China. The first five providers in the list are mentioned several times by respondents, while the rest were recommendation from online forums and other websites that target expatriates living in China.

These websites are compared based on the following criteria: 1) Established history: when did the service become available? Service history has been used as a measurement for the credibility of a specific service provider. Those who have a longer history in the market are considered more credible than recently established players. This data may also shed some light on the emergence of the commercial market for VPN service. 2) Target Market: who are the target customers of the VPN service? Do these VPN service providers target general internet users or a specific group, such as the expatriate group? 3) Price: How much do these service providers charge for their service? 4) Number of servers and locations of servers: servers are critical to the reliability of the VPN service, as they act as intermediaries to connect the users and web resources. The location of the servers directly affects the speed of the internet access and the availability of the web content. For example, television-streaming websites like Hulu can only be accessed through servers located in the United States. The number of available servers is also important, because it gives options to the users to choose which server is the most suitable and that depends on the locations of the users and other concerns; 5) Accessibility: who can access the VPN service? There are two aspects to consider in how accessible the service is for the user. First is the language. What language options are provided in the interface of the VPN service? Second is the technical accessibility. Can the users, especially those based in China, access the service website without using any proxies? One possible scenario is that the VPN service website itself is blocked by the government, so that Chinese users cannot access the site and purchase the service. I used two platforms to test technical accessibility. One was provided by GreatFire.org, a non-profit organization that has closely monitored internet censorship in mainland China since 2011. This online organization shares real-time and historical information about thousands of websites it routinely monitors, as well as testing their own URLs. The other one is called Blockedinchina⁵, which provides accessibility test results in different regions of China. When the results given by the two test platforms were inconsistent, someone who was physically present in the censored region conducted the in-country testing. Except for accessibility test, all the other data are compiled based on the major portal site of the VPN service provider. All information is publicly available.

<table>
<thead>
<tr>
<th>VPN</th>
<th>History</th>
<th>Target Market</th>
<th>Price (mo)</th>
<th># of Server Location</th>
<th>Language Accessibility</th>
<th>Web Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Astrill</td>
<td>2009</td>
<td>Global with China-focused</td>
<td>$5.83</td>
<td>208 servers in 55 countries;</td>
<td>Available in 9 languages; Chinese not</td>
<td>80% blocked</td>
</tr>
</tbody>
</table>

⁵ http://www.blockedinchina.net/
<table>
<thead>
<tr>
<th>Service</th>
<th>Year</th>
<th>Location</th>
<th>Price</th>
<th>Features</th>
<th>Blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>StrongVPN</td>
<td>1995</td>
<td>Global</td>
<td>$7</td>
<td>4 servers in 20 countries, including 12 US cities.</td>
<td>100%</td>
</tr>
<tr>
<td>PureVPN</td>
<td>2007</td>
<td>Global</td>
<td>$9.95</td>
<td>300 servers in 89 countries: 161 servers in the US</td>
<td>Conflicted</td>
</tr>
<tr>
<td>VyprVPN</td>
<td>2009</td>
<td>Global</td>
<td>$6.67</td>
<td>700 servers in 45 locations</td>
<td>33%</td>
</tr>
<tr>
<td>VyprVPN</td>
<td>2009</td>
<td>Global</td>
<td>$8.32</td>
<td>97 server locations in 78 countries.</td>
<td>67%</td>
</tr>
<tr>
<td>WiTopia</td>
<td>2005</td>
<td>Global</td>
<td>$5.99</td>
<td>Servers in 72 cities, 44 countries</td>
<td>Unblocked</td>
</tr>
<tr>
<td>PIA (Private Internet Access)</td>
<td>Unknown</td>
<td>Global</td>
<td>$6.59</td>
<td>2,091 servers in 13 countries</td>
<td>100%</td>
</tr>
<tr>
<td>SecuriTales</td>
<td>Unknown</td>
<td>Global and China-focused</td>
<td>$6</td>
<td>Unknown</td>
<td>Unblocked</td>
</tr>
<tr>
<td>VPNinja</td>
<td>2009</td>
<td>Global and China-focused</td>
<td>$6</td>
<td>Unknown</td>
<td>Unblocked</td>
</tr>
<tr>
<td>Vpn.ac</td>
<td>2012</td>
<td>Global</td>
<td>$4.9</td>
<td>Servers in 15 countries</td>
<td>Unblocked</td>
</tr>
<tr>
<td>12vpn</td>
<td>2007</td>
<td>Global</td>
<td>Start at $2.4</td>
<td>Servers in 17 countries</td>
<td>100% blocked</td>
</tr>
</tbody>
</table>
Most of these VPN service providers were established after 2007. The rise of commercial VPN service for personal use has to do with an increasing concern with online anonymity and increasing control from both government and companies. Although the Chinese government began to regulate online content and services since 1997, the massive blockage targeting foreign websites started later. Facebook was blocked in China following the Urumqi riots in 2009. Other popular social media platforms such as Youtube and Twitter were blocked in the same year. Many respondents indicated that their adoption of VPN service is directly related to the desire to access Facebook in China.

All of these VPN service providers advertise their business to the widest pool of possible users. The protection of users’ privacy is emphasized in the more general use of VPN service. For example, Astril, the most popular VPN provider, formulated the main reasons to adopt VPN service on its website as follows: “Stop anyone to trace your Internet activity- browse the web, don’t let others to browse you; Feel safe wherever you use Internet at public places- airports, cafes, libraries, schools, hotels…”

Many VPN websites intentionally display the IP address with the geo-location of the visitors and contrast it with the anonymized result using the VPN. These service providers promote their business by depicting two types of internet: the private internet and the public internet. According to their depiction, the private internet is anonymous and unfiltered while the public internet is filtered and insecure. The VPN is depicted as a powerful tool to protect users’ privacy from the gatekeeper, such as the Internet Service Provider (ISP). For example, on the website of StrongVPN, it says “ISP is able to see all locations you view from your computer; Ports and all other available protocols are under ISP control” in the context of “public filtered internet.” In contrast, “your IP changes to the VPN server developed IP, not your ISP IP; all traffic outbound from your computer encrypted; ISP no longer has logs” in the private internet powered by VPN. According to Astrill, “Thousands of customers from over 190 countries across the globe choose Astrill as their virtual shield on the Internet every day.”

China has the largest online population among all countries. At the same time, it has the most extensive Internet censorship. Given this background, it is not surprising that some of these popular VPN service providers particularly catered to the China market. Astrill posts users’ reviews on its front page. A majority of the posted reviews are from users located in China. Several providers have servers located in Hong Kong and Singapore in order to provide faster connection for users in China, since the speed is directly related to the distance between the users and the server. One service provider, 12vpn, is headquartered in Hong Kong. However, this does not necessarily mean these VPN services are targeting Chinese users, as I will further illustrate in the evaluation of their
service accessibility. In fact, some service providers indicated that their target customers are expatriates from US, Canada and European countries. According to StrongVPN, expats living abroad “use VPN to view their favorite content provider websites, such as Hulu, Netflix, BBC and more” is by far the most popular use of VPN today.” In the video demonstrating the possible uses of its service, Strong VPN depicted four types of users: an American business man, Jim, who travels to UK and who wants to unblock Netflix; British traveler Casey who wants to access BBC during her vacation time in the Caribbean; Western traveler Craig spending a holiday in China who wants to post a “Great Wall” picture on Facebook; Sam, who wants to check his email from a public location without compromising his personal information. Except for the last example, all the other three typical users are depicted explicitly as international travelers from Western countries.

All of these VPN services are subscription-based and charge a monthly fee ranging from $2.49 to $9.95. The rate is even cheaper for a one year subscription. It is worth noting that most of these VPN sites only accept international credit cards and Paypal, which is not Chinese-friendly. The payment system reveals that the target users of VPN service are not ordinary Chinese but expatriates from Western countries.

Many VPN service providers advertise the number and the location of the servers they provide. Most of these servers are located outside Mainland China and tend to concentrate in Western countries. These servers act as alternative conduits to blocked sites. The more server locations a VPN service covers, the more options for the users to “relocate” their internet connection virtually. As 12vpn articulated on its website, the VPN service enables the users to “be anywhere.” By using a VPN service, internet users can either “connect to a local server for the best performance or a far way server to get a foreign experience.” In the Chinese context, a VPN connection from a location inside China to a site outside China would effectively give the same access as if the user were outside China. By using a VPN linked to an outside server, expatriates not only bypass the “Great Firewall,” but also relocate themselves outside China and virtually reside in another country. VPN users are able to keep their local IP, as if they never left their native country, from anywhere in the world. By doing so, expatriates are able to transport their American or “native” media experience into their lives in China.

Besides the emphasis on privacy and location flexibility, many VPN service providers also promote the idea of “internet freedom.” For example, Vyprvpn puts the slogan “Internet privacy and freedom for everyone, everywhere” in its front page. In a recent blog post, Vyprvpn promotes itself as “Netflix customer’s best friends”:

---

6 Except for 12vpn and Vpn.ac who accept more Chinese-friendly options like Alipay and Unionpay
“ISPs in every country use deep packet inspection (DPI) to identify internet traffic so they can throttle or block streaming services such as Netflix. Golden Frog is network-neutral and doesn’t discriminate against devices protocols or applications. That means we don’t inspect our user’s traffic. VyprVPN acts as a “Virtual ISP” by encrypting traffic and defeating DPI to keep ISP’s from identifying internet traffic as streaming content from Netflix.”

The issue of “network neutrality” is relevant here. Network neutrality is currently a hotly contested issue with serious implications for the future of digital media. The fundamental principle of network neutrality is that Internet Service Providers (ISP) and governments should treat all data on the Internet equally for all, regardless of different users, content, site, platform application, or mode of communication. There should be no different cost to access any sites for any users. Lack of net neutrality imposes a tiered service system, in which internet service providers can charge different fees for internet access. If there are different fees charged for accessing certain sites, it would foreclose equal opportunities for people to access information. Internet service providers would have the discretion to decide what sites can be accessed. Therefore, the power in the relationship between consumers and providers shifts in their favor. Internet service providers can charge more for sites that people use most and charge more money to allow certain users faster access to their sites.

The VPN acts as “virtual ISP” to prevent Internet Service Providers from discriminating against users overseas who access certain websites, such as Netflix. Similarly, PureVPN promotes the use of its service as a way to gain internet freedom: “If you want internet freedom, internet security and full internet privacy, there is none better out there than PureVPN.” Getting a VPN service is promoted as the best way, if not the only way, to access secure and unrestricted internet. “Enjoy Internet Freedom with Pure VPN,” is presented as the major feature of using the service:

“A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a user to send and receive data across shared or public network as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.”

By using VPN, the Internet as a public network becomes privatized. Those who pay for the VPN subscription can benefit from the private network, while the other internet users who are not protected are excluded from enjoying Internet freedom. This infrastructure

---

8 The Federal Communications Commission (FCC) voted in February 2015 to reclassify broadband under Title II of the Telecommunications Act, and thus to secure Network Neutrality and the principle of nondiscrimination at its center.
10 http://www.purevpn.com/features.php
is, in principle, quite similar to the tiered service system without network neutrality. In other words, VPN service becomes a private solution to the public issue of network neutrality. But who has the access to this private service?

“ExpressVPN is for Everyone.” This is a slogan displayed on the front page of ExpressVPN website. “We made ExpressVPN because we believe that everybody, no matter their level of technical experience, should be able to use the Internet freely and securely.”11 Despite this statement, ExpressVPN is not accessible for ordinary Chinese living in China, who constitute the largest online population for the following reasons.

First, language barriers: Like many other VPN service providers, ExpressVPN does not support Chinese as a language option to access its interface. Actually, among the eleven popular VPN providers listed in the table, only three support Chinese language options. Five of them do not support any other language except English. The lack of language diversity contradicts the “global” image these VPN service providers depict for themselves. This also supports my earlier argument that VPN providers are mainly targeting English-speaking expatriates from Western countries rather than ordinary Chinese people as their customers.

Second, technical barrier: in the Chinese context, the major use of VPN service is to access blocked websites. However, a potential user still needs to be able to access the VPN service website from his/her current location in order to register and purchase the service. Based on the recent accessibility test provided by the two platforms, only four out of the eleven VPN service websites are consistently accessible in Mainland China. And none of these four websites are among the names suggested by my respondents. In other words, the VPN services that were most popular among expatriates in China became blocked at various times, depending on the location and the date of access. Since late 2012, Chinese government has upgraded the “Great Firewall” to disrupt VPN services in China.12 According to the state media, Global Times, Chinese officials claim it is illegal for foreign companies to operate a VPN business in China. Access to a number of popular VPN providers’ websites, including Astrill, StrongVPN and PureVPN, has been blocked in China since 2012. Because my interviews with Western expatriates were conducted between 2012 and 2013, it is highly possible that many of my respondents had already purchased the VPN service before their websites were blocked in Mainland China. Another related question regarding the accessibility issue is: how did Western expatriates in China learn about the VPN service in the first place?

Accessing the inaccessible

11 https://www.expressvpn.com/
12 See Global Times “Foreign-run VPNs illegal in China” available at:
http://www.globaltimes.cn/content/750158.shtml published 2012-12-14; The Guardian 12/14/2012
“China tightens Great Firewall internet control with new technology”
http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control
VPN service is usually advertised for its potentially unrestricted scope, indiscriminate distribution, and relatively low price. However, the promotion of VPN service faces structural constraints, especially in the Chinese context. The Chinese government has tightened the regulation of VPN service providers in recent years. Given its “illegitimate” and spread-out nature, VPN service is constrained in a “grey market” with a lack of market-driven publicity based on advertising and visibility on mainstream media platforms. In legitimate, mainstream media markets, advertising and other market-driven publicity have significant impact on directing consumption patterns. In contrast, the market of VPN service has limited public channels to advertise its business. The issue of awareness becomes crucial for comprehending the difference in the use of VPN service between expatriates and local Chinese. How do people come to know about VPN service and decide to give it a try?

There are two kinds of distribution channels: the formal system of distribution and the informal system of distribution. The formal system includes using search engines and affiliation with institutions that have access to VPN service. The informal system includes personal contacts and use of social media, like online forums. Expatriates who are affiliated with the international educational institutions of foreign companies in China usually have access to VPN service provided by those institutions. But sometimes, the access to VPN service is limited to the workplace and cannot be used at home or in other public places. In this case, people still need to find a VPN service for their personal use. The second way of distributing VPN service is through online searching. People who know they need a VPN service to access certain websites in China conduct these kinds of online searches purposefully. The purposeful online search, provided by popular search engines like Google, may help people in navigating through huge inventories of media products and services.

A Google search by using the term “VPN in China” displays advertising for the following VPN service providers: StrongVPN, EZNow (a Hongkong-based VPN service provider targeting Internet users and business in China), Vyprvpn, ExpressVPN, and three aggregated service recommendation sites (vpnfinder.com; bestvpservice.com; top10bestvps.com). The following is a list of search results for “VPN in China” displayed on the first page of Google:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Web Address</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What’s the Best VPN for China</td>
<td><a href="http://startuplivingchina.com/best-VPN-for-china/">http://startuplivingchina.com/best-VPN-for-china/</a></td>
<td>Online blog that gives expats tips for living in China; VPN sources are listed first as must read guides, followed by the guide to best mobile phone plan for foreigners; Guide to optimize Internet speeds;</td>
</tr>
<tr>
<td>2. Best VPN in China</td>
<td><a href="http://www.bestvpninchina.com/">http://www.bestvpninchina.com/</a></td>
<td>Online blog written by an expat living in China specialized in providing recommendations for VPN service providers</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3. China-StrongVPN.com</td>
<td><a href="http://www.strongvpn.com/packages_china.shtml">http://www.strongvpn.com/packages_china.shtml</a></td>
<td>VPN service provider page specifically carter to users in China</td>
</tr>
<tr>
<td>7. Astrill VPN</td>
<td><a href="https://www.astrill.com/reviews.php">https://www.astrill.com/reviews.php</a></td>
<td>Linked to the review page based on users in China</td>
</tr>
</tbody>
</table>

(Source: Google.com, January 31, 2015)

There are different types of references presented in the first page of the list. Some of the links (links 3 and 7) are to the sites of VPN service providers. However, there are more links (links 1, 2 and 5) to blogs giving recommendations and providing tips for using the VPN service in China. These review sites further direct users to a list of recommended VPN service sites. When the domain name of the VPN service is blocked, these recommendation sites can provide the link to a mirror site with an unblocked domain name or other alternative providers. There are two links from the conventional sources: the online encyclopedia Wikipedia and the question-and-answer website Quora. These sources are based on user-generated contents. They did not directly link to any VPN service providers, but provided important background information regarding the use of VPN in China; specifically, blockage and legal issues.

Given the “illegitimate” nature of overseas VPN service in China, online searching might be the primary way for these service providers to gain public visibility. However, empirical studies suggest that the role of search engines in orienting cultural consumption is rather limited. People tend to use the Internet to find more details about certain cultural products they are already interested in (Kayahara & Wellman 2007). The Internet basically reinforces existing consumption habits shaped by “traditional factors,” such as friends’ recommendations and mainstream media (Tepper & Hargittai 2009). In short, this empirical research suggests people do not tend to discover new cultural items through purposeful searches online.
For VPN service providers, exposure on mainstream media is rather limited. In the China context, the access to Google is not guaranteed without the use of the VPN. Therefore, the power of online searching to connect available VPN service providers with potential users in China is limited. In this situation, the informal distribution networks become more important than the formal ones. A person’s decision depends on the visibility of the choices made by other people (Salganik, Dodds, & Watts 2006).

There are two types of informal networks for getting VPN service: the first type is through the word-of-mouth; the second type is through social media, such as online forums. Most of my respondents learned about VPN service through their personal contacts. Giving suggestions about VPN service has become a common topic among expatriates in China. “VPN becomes the code word for expatriates here.” (White American male, in his late 20s, lived in China for a year) The following conversation is quite typical among the Western expatriates I had interviewed:

Q: How did you find out your previous VPN?  
A: My husband, who heard from someone else, who heard from someone else 
Q: So it is always come through the word-of-mouth?  
A: Yes. Because you don’t know which one will be successful.

These conversations illustrate how expatriates rely on their personal networks to find out “trustworthy” VPN service providers in China. The discussion about which VPN to adopt also takes place online, especially on those regional-based online forums for expatriates. Below is an expert from the online posts published on a popular expat forum (Aug 14, 2014):

Haali (280 posts): My Astrill subscription just ran out. Before I renew, are there any other VPNs people would recommend?  
Jeanie (8 posts): We use 12 vpn. It’s been good and reliable so far. There’s a 2 week free trial. We found it better than Astrill. http://12vpn.net/  
Spartans (93 posts): You can buy a vpn on taobao. It works great and I pay only 16rmb a month.  
Doraemon: I recommend webfreer, all you need to do is just downloading and installing it, much like a browser, it is good.  
Magnifico (1536 posts): @jeanie, why is it better than Astrill? Faster?  
Jeanie (8 posts): We think it’s faster and has a better signal. It’s also cheaper at $6/month. There can be periods of spottiness, but overall we still think it’s better.
The wonderer (59 posts): I would not recommend Astril. I signed up so I could check them out. VPN speeds seemed fine but when I found it caused problems with my web browser when I was not connected and they could not fix it I asked to cancel within the 7 day free trial and they are doing everything to say no.

Dazzer (1065 posts): @wonderer I have no such problems, I used to but them changed my settings to different vpn mode, or not automatically use a proxy. Or the setting for only use vpn on selected sites. Can't remember which. This is using chrome browser. Contact astril customer service with a different question and you might get the response. You need also remember your first call center opo might have been a newbie, maybe you get someone better next time.

Anonymous Coward (185 posts): With ExpressVPN, I have this list of 2 dozen servers I can connect to, but the only server that really works properly most of the time is Hong Kong. Sometimes Singapore or LA will work, but usually anything other than HK is too slow to be usable. I'm talking dial-up speed here.

Ouyang (244 posts): For ExpressVPN I find it'll be slow if you try to connect to the “recommended” list except for Hong Kong. Usually Malaysia, Japan, Indonesia, and Singapore are good enough for Youtube. Also I find if I “fake” connect to three or four other random countries first by cancelling before it finishes connecting, the feed is usually much faster. Their Android client is also much better than their desktop clients.

From the above excerpt, we can see that the effective use of VPN service is quite tricky and the service from the providers is not always reliable to address the problems. It requires experience and knowledge on the user side. One of the major issues raised in the discussion, also suggested by my respondents in the interviews, is the speed of the internet connection by using a VPN service. Since the VPN service directs the internet traffic to a proxy server, this proxy server could become a bottleneck for internet connection if it was not chosen properly. However, there is no standard or universal way to decide which server is the best choice because this can vary according to the location of the user, the number of people choosing the same server at the same time, and the availability of the connection itself (since the traffic to the server can be blocked). Because of these wide variations and the lack of standardized practices, it creates the need for a local-based mechanism that I call the “VPN talk,” which offers information that orients people’s practices. Unlike systematically aggregated consumer information provided by media institutions, the “VPN talk” is a bottom-up, community-oriented resource which servers as an intermediary in this media environment.

The significance of the “VPN talk” is not only that it circulates useful information and tips, but more importantly, it builds trust and community among users in a “grey market” that lacks of transparency and consistency. Like the one illustrated in the excerpt, the “VPN talk” usually takes place online anonymously. However, users can interact with each other easily and users who engaged in the conversation displayed their entire history of publicly posting on the same website. The above discussions involved long-term users like Magnifico who had 1536 posts and newly registered ones like Jeannie,
who had 8 posts on record. These forms of “VPN talk” effectively oriented consumption at the grassroots level.

The “VPN talk,” through personal connections or/and online discussion, plays an important role in reconnecting users in China with the World Wide Web. Therefore, it is important to analyze who is included in the “talk” and who is excluded. People who are well connected to those have experience with VPN service are obviously more likely to engage in the “talk” than those who are more socially isolated. However, people who do not have many personal contacts to rely on could actively search for the information online or accidentally come across the information by frequenting certain websites. The key difference between the Chinese-language users and the English-language users is that the online media environment is much more censored for the Chinese-language users, for whom the “VPN talk” can rarely take place publicly.

In summary, I found the distribution of VPN service, especially in the Chinese context, is more effective through the informal networks than through formal channels. Compared to the formal channels, the informal information distribution is more personal and community-oriented. But there are limitations particularly related to this micro-level distribution. From such micro-mechanisms arise a ubiquitous phenomenon described as “power-law distribution.” When faced with many options to choose from, people end up giving a disproportionate amount of attention to a small subset of the whole (Webster 2011, pp 54-55). Since most expatriates rely on their personal networks to gain information about proxy services, the usage of VPNs tends to concentrate on a handful of brand names. The dilemma of this concentration is that when a certain brand of VPN gets popular, it will catch the attention of the Chinese authorities and eventually be shut down. The more people use the same VPN service provider, the more likely this VPN service will be blocked or disrupted. This is exactly what happened to some of the most popular VPN providers, such as Astrill, Express VPN and Strong VPN, recently.  

Implications for Internet Freedom in China

Concerning the research question about why the adoption of VPN service is more prevalent among expatriates than the local Chinese population, I find there are three main factors to consider: Motivation: Why do people adopt circumvention tools? This question was asked in a recent study of a selective subgroup of Chinese internet users who are circumventing internet censorship. Based on a survey of 1,175 Chinese Internet users, Robinson, Yu and An (2013) found that the vast majority of users adopt circumvention tools in order to gain access to blocked websites, rather than acting out of privacy concerns. The three leading reasons for Chinese users to circumvent the “Great Fire Wall” were for web search (access Google or other search engines blocked

---

_\text{r}=0
in China), social media (to use Twitter, Facebook, or other social network sites), and foreign news (like the New York Times). In the interviews, I found these are also leading reasons Western expatriates gave for using the VPN service. If the motivations to bypass censorship are quite similar among internet users in China, why are Western expatriates more likely to adopt circumvention tools than ordinary Chinese?

Various surveys have found that tolerance of Internet censorship runs relatively high in China (Guo and Feng 2011; Li 2009). 89% of Chinese Internet users agree or strongly agree that they “have full access to all of the information that is available on the Internet” (Internet Society 2012, 20). Many Chinese people are either unaware of the “Great Fire Wall,” or unconcerned by it (Damm 2007; Liu 2010). Besides, the emphasis on state censorship in explaining media consumption patterns may obscure the role played by audience preferences (Taneja and Wu 2015). By analyzing the structure of country-to-country hyperlinks between websites, Barnett, Chung and Park (2011) found that sites in the same languages or that focus on the same country tend to have more hyperlinks with one another than with sites in different languages or focusing on other countries. Similarly, people who share the same language and close geographic proximity, or have direct air connectivity between their locations are more likely to form Twitter ties than people who don’t share this geo-language proximity (Takhteyev, Gruzd, and Wellman 2012).

By analyzing audience traffic among the 1000 most visited websites, Taneja and Xiao Wu (2015) found that internet users frequent websites they find culturally proximate, based on language and geography, and access blockage matters only when such sites are blocked. Cultural proximity helps to explain why Western expatriates are much more motivated than ordinary Chinese users to adopt circumvention tools in order to access blocked websites, like Facebook. Access blockage is coercive only when it prevents users from browsing culturally proximate content. The Chinese internet users who use circumvention tools are mostly males in their mid-twenties, highly educated with a college degree, either working professionals in the information technology sector, or students from elite schools (Robinson, Yu and An 2013). These are more cosmopolitan internet users who seek out information and cultural experience beyond their native country but they are not representative of general Chinese internet users.

1) Alternatives: Do people have alternative ways to get what they want without using circumvention tools? This question is also related to motivation, as people who find they have fewer alternatives would be more motivated to bypass censorship. Most media users today have a large number of media options at their disposal. Yet they do not consume all these options and tend to focus on a small number of subsets. In the Chinese context, by blocking major foreign websites, state censorship limits people’s knowledge about their media choices. In other words, many Chinese internet users may not be fully aware of what media platforms/contents, especially the ones outside their cultural proximity, are available to them. In this way, the “Great Fire Wall” may have manipulated Chinese internet users’ media preferences without them noticing it (Webster 2011). Besides, the “Great Fire Wall” acts as a trade barrier that protects and
facilitates the fast growth of Chinese online service providers. The increasing censorship goes hand in hand with the development of Chinese versions of Facebook, Twitter, and YouTube (Liu 2010). These Chinese “copycats” act as viable alternatives for Chinese internet users to search for information and socialize without circumventing the “Great Fire Wall.” By habituating Chinese users’ preferences towards local products, it is quite likely that people on average would keep consuming local websites, even if the censorship were lifted (Taneja and Xiao Wu 2015). The situation is quite different with Western expatriates, who were generally aware of the massive media censorship that significantly limited their options of using the media platforms they felt to be culturally proximate.

2) Accessibility of VPN Service: As I illustrated earlier, the major overseas VPN service providers target expatriates and other international users. These VPN services are less accessible to Chinese internet users, due to the language barrier and the technical barrier. Among Chinese users of circumvention tools, only 30% of them had used paid VPNS (Robinson, Yu and An 2013). Most Chinese users rely on proxy servers like GoAgent and other web proxies to access blocked websites. Unlike expatriates who learned about circumvention tools through word-of-mouth from their more tech savvy friends or co-workers, a wide majority of Chinese users found their first circumvention tool through web searches, blogs or news. These Chinese users adopted a range of different types of circumvention tools, allowing them to use one tool to diagnose the problems they are facing with a different tool (Robinson, Yu and An 2013). Taobao is the most popular online shopping site, similar to eBay and Amazon, for Chinese users. Millions of products are listed for sale on this online platform. However, a search for “VPN” is blocked on Taobao. When the term “VPN” is entered as a search word, the result is nothing but a system indication that “according to related policy and law, the results of VPN cannot be displayed.” In contrast, a search for “proxy” on Taobao is unblocked and generates seven pages of product suggestions. Some of these products are not related to circumvention tools, but there are at least five relevant products listed on top of the first page. If the search is conducted using the Chinese term for circumvention tools, “翻墙软件” (meaning “software for leaping the wall”), the search term itself is not blocked but the results are mostly irrelevant to circumvention tools.

VPN service provides a private, market-driven solution to “Internet Freedom.” But is it the only or the best solution in the Chinese context? There are limitations to using proxy services to bypass censorship. First, though the VPN service providers are largely based overseas, the Chinese authorities still have the capability to block and interrupt the service. In late 2012, several VPN service providers reported that the “Great Fire Wall of China” became able to “learn, discover and block” the encrypted communication methods used by a number of different VPN systems. Astrill, a popular VPN provider for users inside China and beyond, emailed their users to notify them that at least four of the common protocols used by VPNS have been blocked by the Great Firewall of
China\textsuperscript{14}. The Chinese government has long had some of the world’s most sophisticated internet censoring technologies. But until recently, the authorities had tolerated the proliferations of VPN and other proxy services because of the concern for prohibiting the commercial activities that rely on less-fettered access to the internet. The situation represents a “digital dilemma” that a choice has to be made between permitting new communication technologies, accepting their potential to be used to subvert the authoritarian regime, or blocking access to those tools and suffering slower economic growth.

The Chinese authorities steer a middle course, disrupting VPN traffic in the interest of censorship at critical time periods, and at other times allowing VPN traffic in the interest of economic development. The availability of proxy services and the existence of less censored “internet space” (e.g. research institutes, multinational companies, high-end hotels targeting foreigners) are deliberate compromises made by the government to ensure that economic interests are not jeopardized by internet censorship. This compromise is based on the presumption that the unfettered internet would only be available to a limited number of people and their use is under control. In fact, a number of research institutions and corporations reported publicly that visiting overseas websites was disrupted for a full week in 2011. Several technology bloggers\textsuperscript{15} suspect that this massive disruption had to do with the recent upgraded system that allows the Chinese government to monitor data flows of local IPs. With this new system, when a local IP is discovered to access a large number of overseas IP addresses, the connection would be suspended through China Telecom and China Unicom, the two major state-owned telecommunication service providers in China. Since corporations and other institutions are more likely to exceed the limit than individuals, this disruption has been found to mainly affect corporate connections and universities, while the connections at home perform normally. Several institutions have posted notices to ask their employees to curb their use of VPNs and access to overseas websites in general\textsuperscript{16}. The prominent Chinese University has been found to charge an hourly fee for on-campus access to foreign websites\textsuperscript{17}. 

Recently, the Chinese government had imposed further restrictions on using Gmail and cracked down the VPN service provided by some popular providers including Astrill, StrongVPN and Gloden Frog. The short-term disruption is interpreted as part of the


Chinese authorities’ long-term quest for “cyber-sovereignty.” The Chinese government is implementing policies that may improve its ability to separate commercial activities from circumvention-related uses of VPN service. Western expatriates and a small number of Chinese internet users are relying on tools that the Chinese government does not want the “Great Fire Wall” to block completely for the sake of economic interest. This is not Internet freedom, but a “collateral freedom” built upon what Chinese regime finds economically or politically indispensable (Robinson, Yu and An, 2013).

Besides, the VPN service is also highly commercialized. Users have to pay an extra “toll fee” to access overseas websites. By doing so, internet and other media access has been developed into a two-tier system, where the global elites have much more freedom and flexibility to access the more unfettered internet, given that the majority of the Chinese population live with the much more constrained and censored media environment. This kind of approach goes against the fundamental principle of “open internet,” as defined by the Federal Communications Commission, which mandates the use of free, publicly available standards that anyone can access and build to.

On the one hand, by reducing Chinese internet users’ reliance on foreign websites, the Chinese government facilitates the construction of a “Chinese web,” which is a geolinguistic cluster in terms of its composition and degree of isolation. On the other hand, by using commercial VPN services, expatriates can easily transport and reconstruct the media environment they were familiar with at home. While the use of the global internet creates a sense of being globally connected, this may be a disincentive to getting involved with the local environment and thus contribute to the “expat bubble.” As a media practice to deal with existing infrastructural boundaries, the use of a VPN requires a minimum of effort from the expatriates to adapt to the local environment, and reinforces the “digital divide” between the expatriates’ communities and the local Chinese communities.

---

19 Available at www.fcc.gov/openinternet
References


