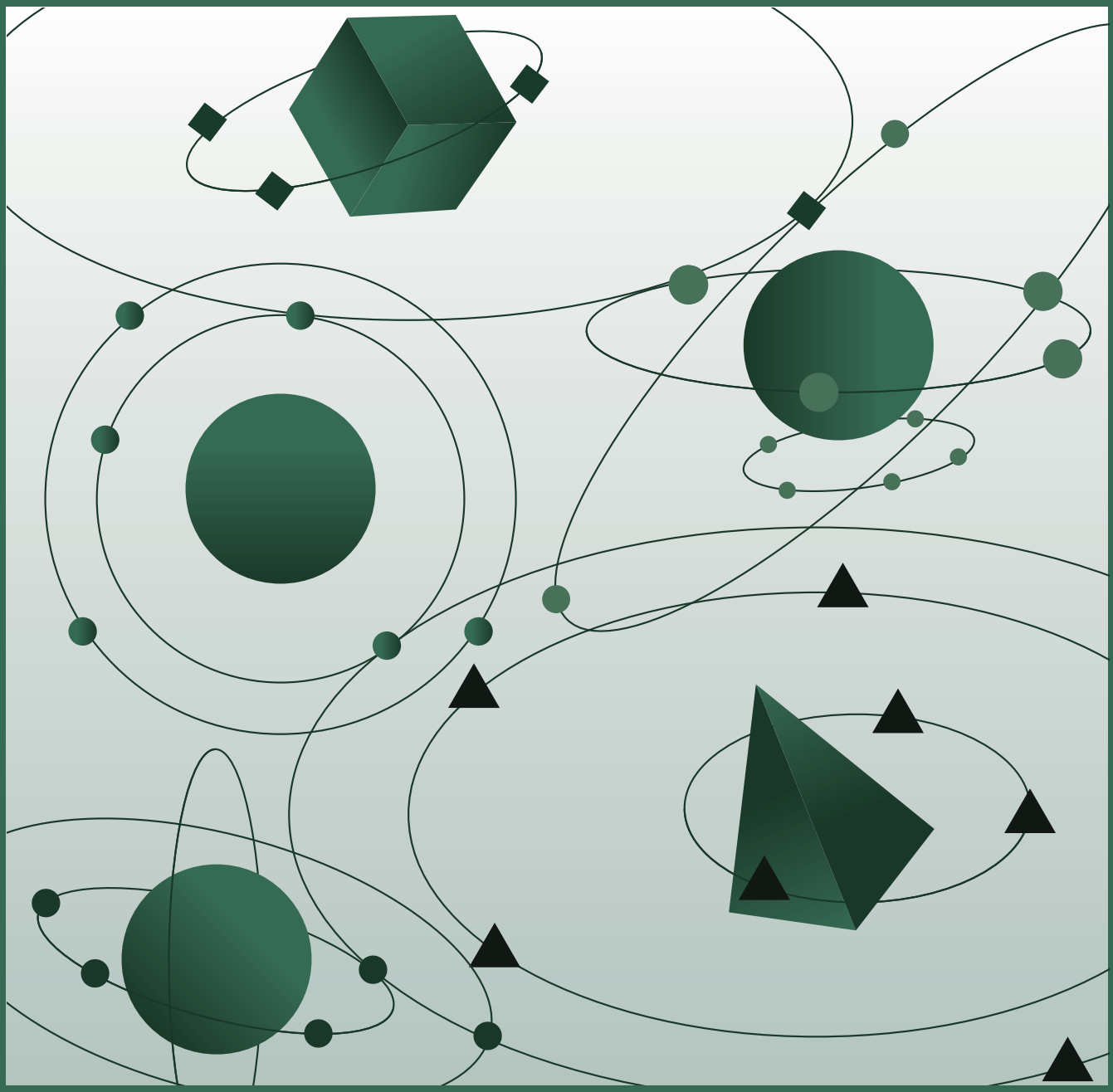
Growing with the People

Insights From Outline VPN Providers Operating in an Evolving Censorship Landscape



A collaboration between:

JIGSAW | OKTHANKS

Table of contents

Introduction p3

Research Background p4

(1) Social: The Lived Experience in Censored Environments p5
- Censored Environments
- Lived Experience of Using a VPN

(2) Technological: Outline Technology in Censored Environments p9
- Small Scale
- Large Scale
  - Same Need, Different Solutions
  - Challenges of Managing a VPN Service with Outline

(3) Operational: Needs of Large Scale Providers p14
- (a) Evolving Circumvention Tactics
- (b) Improved VPN Experience
  - Managing Expectations
  - Troubleshooting
  - Communicating Status
  - Split Tunneling
- (c) Content Controls

Conclusion p20

References p21

Research by:
José Gutiérrez, Carrie Winfrey, Emily Saltz, and David Ho

Report contributors:
A special thanks to contributors from the Jigsaw team including Maddy Hoffman, Vinicius Fortuna, Peter Wiegand and Simon Biddle-Snead.

Acknowledgements:
A special thanks to the research participants, including Okno, Izumo, WEPN, Paper VPN and our anonymous contributors.

Introduction

The circumvention technology space can be challenging to make sense of, as it entails multiple protocols, technologies, threat models, infrastructures, services, providers, and goals. It's also riddled with uncertainty as the space is intertwined with differing socio-economic realities and government ideologies and their evolving capabilities to limit access to the internet.

This report intends to bring clarity to this complicated environment by contextualizing insights gathered by Okthanks from two research studies with eight VPN providers that use Outline, an internet censorship circumvention tool developed by Jigsaw. Three aspects of internet censorship and circumvention will be covered:

1. Social: The Lived Experience in Censored Environments
2. Technological: Outline Technology in Censored Environments
3. Operational: The Needs of Large Scale Providers

While the objective of the research was to inform the future roadmap of Outline, this report focuses on the findings most relevant to the broader censorship circumvention community.

Research Background

Outline is open source software initially developed for small scale operators, allowing individuals and small organizations to run VPN services almost undetectable by censors. Over the years, however, people saw its potential to address other use cases and have adapted the code in intriguing ways, making the Outline team interested to learn more about how these groups were using the technology.

To find out more, Okthanks interviewed eight VPN providers with widely differing uses of Outline. Of the eight providers: two use Outline Manager to run their service,[1] two embedded Outline into their own VPN service,[2] and four had built custom management tools to run Outline's VPN service.[3] The Jigsaw team assessed this variety of uses and determined that they'd expand Outline's reach the most through those that have adapted their technology. The research team then went back for further interviews with the four providers that had adapted Outline in order to gain more insight into their operations, learn where they have spent and are spending time, and understand how they prioritized a variety of issues commonly faced by providers.

[1] They used two products: the Outline Manager application to create and share access to their VPN, and the Outline Client to connect to the Outline VPN.

[2] They used parts of the code to provide alternative protocols to their end-users. One of them uses the Outline Client app and the other uses other apps that allow their subscribers to connect to their service.

[3] They used the Server Code to bootstrap their service. One of them built their own app and the others are using the Outline Client app.

(1) Social: The Lived Experience in Censored Environments

Censored Environments

Authoritarian governments don't share their censorship strategies publicly. A picture of their strategies, however, can be developed by talking to the providers that circumvent them. These providers get continuous feedback from their systems and their users when the service stops working or the quality of service declines. The participants in the study focus their operations in specific regions, where they face distinct challenges directly related to the dynamics and challenges of each region.

For this phase of research, the research team spoke to providers serving users in Iran, Russia, China, and several countries in Africa. For all of the differences found, there's one major similarity: authoritarian governments will typically enforce controls during moments of heightened political tension.

Participants mentioned as examples the Russian invasion of Ukraine, the civil unrest and protests in Iran following the death of Mahsa Amini, as well as recurring events, like the anniversary of the Tiananmen Square protests and subsequent massacre in the PRC, as well as elections in a number of countries in Africa. While the triggers are consistent, governments' censorship strategies vary, as each country has different technical capabilities, legal frameworks, and telecom market structures.

Examples:

China: In 2009, the day before the 20th anniversary of the Tiananmen Square massacre, the government blocked services such as Hotmail, Flickr, and Twitter. In response, a number of other sites protested by placing themselves in maintenance mode, an event later referred to as "Chinese Internet Maintenance Day."[4] In 2013, search results for related terms, including "June 4 incident," were censored.[5] That same year, the microblogging platform Sina Weibo removed the candle icon from their platform.[6] In the research, a participant mentioned that there are major updates to the Great Firewall during these politically sensitive times, making VPN services useless for days or until a provider can hack their way through the new measures.

[4] Johnson, B. (2009, June 4). Chinese websites mark Tiananmen Square anniversary with veiled protest. The Guardian. https://www.theguardian.com/technology/2009/jun/04/chinese-websites-tiananmen-square-anniversary

[5] Business Insider. (2013, June 1). China is experimenting with a new form of internet censorship. Business Insider. https://www.businessinsider.com/chinas-new-form-of-internet-censorship-replaces-controversial-topics-with-fluff-2013-6

[6] Alia. (2013, June 3). Subtle censorship at its finest: Weibo took out candle icon ahead of Tiananmen anniversary. Offbeat China. https://web.archive.org/web/20140409030900/http://offbeatchina.com/subtle-censorship-at-its-finest-weibo-took-out-candle-icon-ahead-of-tiananmen-anniversary

Iran: In 2019 the Islamic Republic of Iran disconnected from the global internet entirely for a week while continuing to run a domestic intranet amid mass protests initiated by a sharp increase in oil prices.[7] In 2022, following the outbreak of protests after the killing of Mahsa Amini, Iran blocked Instagram, WhatsApp, Skype, and the Apple and Google Play app stores, and instituted a regular internet curfew, shutting down the internet for hours a day as they worked to regain control.[8] They also stepped up efforts to limit access to the open internet via VPNs and have become very efficient at blocking them.[9]

Russia: Following Russia's invasion of Ukraine in 2022, Russian telecoms blocked access to Facebook, Instagram, and X (formerly Twitter).[10] Internet censorship in the country has grown dramatically since, with Roskomnadzor, the federal agency responsible for monitoring and censoring domestic media, ordering the blocking of 885,000 websites in just the first six months of 2023.[11]

Tanzania: Amid Tanzania's 2020 elections, the government blocked Whatsapp, Telegram, social media websites (Twitter, Instagram, Tiktok, YouTube) and Tor.[12] Governments blocking access to social media and messaging apps is a common feature of elections in a number of African countries.

> "Circumvention is very country specific; and if you want to help, you need to understand the user requirements and specific context. Otherwise you can't really help people there." —Provider focused on China

Lived Experience of Using a VPN

Due to the diversity of governments' censorship strategies and technical capabilities, censorship as a lived experience can differ substantially from country to country. Even within the same country the experience of censorship may differ, as each network, e.g. an Internet Service Provider (ISP), represents a distinct environment where censors may have different social and technical capabilities to enforce control.

[7] Internet being restored in Iran after week-long shutdown. NetBlocks. (2019, March 26). https://netblocks.org/reports/internet-restored-in-iran-after-protest-shutdown-dAmqddA9

[8] Zad, A. (2022, September 29). When will Iran's internet censorship collapse? Slate Magazine. https://slate.com/technology/2022/09/iran-protests-mahsa-amini-internet-censorship.html

[9] Kılıç, D., & Chúláin, A. N. (2022, November 6). How Iranians are hopping between vpns to stay connected. euronews. https://www.euronews.com/next/2022/11/06/iran-protests-vpn-use-soars-as-citizens-seek-way-around-internet-censorship

[10] The Moscow Times. (2022, August 8). Russia has blocked 138K websites since Ukraine invasion, prosecutor says. https://www.themoscowtimes.com/2022/08/08/russia-has-blocked-138k-websites-since-ukraine-invasion-prosecutor-says-a7853²

[11] Meduza (2023, September 7). Russian authorities blocked more than 885,000 websites in first half of 2023. https://meduza.io/en/news/2023/09/07/russian-authorities-reportedly-blocked-more-than-885-000-websites-in-first-half-of-2023

[12] Xynou, M. (2020, October 28). Tanzania Blocks Social Media (and tor?) on Election Day. OONI. https://ooni.org/post/2020-tanzania-blocks-social-media-tor-election-day/

China

Only government-approved VPNs, which cannot be used to circumvent government censorship of the internet, are available in Chinese app stores. Individuals seeking to bypass government control via VPNs have to download and install them from alternative app stores or through files sent over messaging apps. Installing a non-approved VPN can be particularly risky, as people can be compelled to provide their phones for inspection.[13] In the lead up to politically sensitive events internet censorship becomes more strict. During these moments users often turn to online forums to search for working VPNs and to complain about those that do not function properly.

> "In the States, you can say you're a VPN provider. But you cannot do this in China. People resort to some sort of black market."
> —Provider focused on China

> "Last year, I found out that Shadowsocks became unstable in China. It was not unstable for all users. Only some of them reported it. I don't know if the issue comes from Shadowsocks itself or with the GFW deployed in China or even on different networks. At that moment, you can't really do anything." —Provider focused on China

> "A fast connection today may not be fast tomorrow." —Provider focused on China

> "If one website works on one internet provider, it may not work for another one. The result you get from Beijing can differ from Shanghai." —Provider focused on China

Iran

Getting and using a VPN in Iran can be challenging, especially during politically sensitive moments. The Iranian government is extremely efficient at blocking services by using multiple censorship strategies in concert. Going online or doing anything on social media requires patience and the tedious task of looking for a VPN that works has become part of some Iranians' daily routines.

Participants mentioned hearing about users that install several VPN apps, as well as users that try out any Outline access keys they find. They mentioned that it's a frustrating experience for end users to go through all the VPN apps and services to find one that works.

> "People in Iran are rotating different apps, I have seen people go through a lot of VPN apps to see which one works. Something that worked yesterday may not work tomorrow." —Provider focused on Iran

[13] Toh, B. (2019, November 29). Chinese police are now conducting random stop-and-search checks for banned foreign apps such as Instagram and twitter: Reports. Business Insider. https://www.businessinsider.com/chinese-police-search-banned-foreign-apps-phones-2022-11

Russia

The Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media) has been increasing pressure on VPNs by enforcing legislation and also by blocking protocols like Wireguard, L2TP, and OpenVPN.[14] Providers are worried about the future of Russian censorship and residents are increasingly looking for VPNs that consistently work.

Russians living inside the country need VPNs to connect to blocked content, including social media and independent news sources. Additionally, there are some Russians living outside of the country who use VPNs in order to access local Russian services that cannot otherwise be accessed from a foreign country.

> "We are running servers for people in Russia; [and] servers in Russia for people outside who want a 'local perspective' [...]"—Provider focused on Russia

African Countries

Although each country has its own peculiarities, there is a common problem in the region: limited infrastructure and blocklists. When people try to use circumvention tools it's normal to experience network drops and slow connections. Countries referenced by the providers who participated in the research include Tanzania, South Africa, Nigeria, Uganda, and Ethiopia. The participant mentioned they provide the service to many journalists, as they often need a VPN to do their jobs (e.g. to report on events censored by the government).

> "Most African governments have some sort of blocked code. They have a[n] ethics [law]. If they have an issue with ethics, they will block it." — Provider focused on Africa

> "We work across pan Africa; But there are countries with 3G connection. You are going to end up with a very slow connection when you add a VPN to this." —Provider focused on Africa

[14] Maxwell, A. (2023, October 31). Russia blocks 167 VPNs, steps up openvpn & Wireguard Disruption * torrentfreak. TorrentFreak. https://torrentfreak.com/russia-blocks-167-vpns-steps-up-openvpn-wireguard-disruption-231031/

(2) Technological: Outline Technology in Censored Environments

The research took place with providers serving users in China, Iran, Russia and a number of African countries; but it's known that providers are using Outline technology in many other locations, including Myanmar, Singapore, Thailand, and other countries where internet censorship is common. They use Outline because it works reliably in these regions, though Outline, like any VPN, can still be blocked by determined censors.

One aspect critical to Outline's success has been its focus on small-scale providers, which makes it harder for censors to detect.[15] Some providers, however, have adapted the code to create large scale operations. At least one organization has managed to scale Outline to serve over nine million monthly active users.

In this section we will go through the challenges organizations faced when scaling their operations and the strategies they have used to mitigate them.

Small scale

At the outset of the research we talked with activists and small scale providers, those who served fewer than 100 users and who used the Outline Manager app. These providers generally encountered few problems using Outline. But when the number of users increases to more than a few hundred access keys per server, challenges start to emerge.

In particular, one organization mentioned that the Outline Manager starts lagging when loading the app as it retrieves the server keys. It's also complicated to manage the service if there is more than one person in your organization managing keys as the Outline Manager application can only be installed on a single device.

> "Right now the panel is not searchable. If I try to find a key, I have to go through [the list] and look for it." —Provider focused on Africa

> "We can use Outline Manager to manage 100 keys per server. But once we have more keys we need an admin console. Because it improves work for our support team. We need to make it easier. [With] the Manager it's too complicated." —Provider focused on Russia

[15] How it works. Outline. https://www.getoutline.org/how-it-works/

> "The Outline Manager model was not scalable. So we had to come up with another system to build these automated processes." —Provider focused on Iran

Large Scale

Each of the providers interviewed that wanted to serve more than a few thousand users had built their own VPN service, adapting the Outline Server code to their specific context, needs, and users, and forgoing the Outline Manager tool entirely.[16] Though each design is different, they share several similarities in their adaptations:

Automation: Rather than manually generating keys, each of the providers created systems that automatically generated and distributed access keys when people signed up, paid a subscription, or started using the service.

Flexibility to Move Users Across Servers: To scale the service, each provider had to develop their own approach to balance traffic load across servers. In severely censored environments, this flexibility is also critical for censorship resilience as servers can be identified and blocked.

Support: Providers deal with many support issues, from people not understanding the service, to technical problems and troubleshooting. Their channels to receive and respond to support requests vary from email, to Telegram, to support desks. Some have additionally established automated support systems in the form of Telegram bots.

User Management: Service providers have differing approaches to managing users and usage, but in all cases, they have built their own consoles or scripts for user management.

VPN Service: Each organization has its own motives and goals in becoming a VPN service provider, leading to meaningful differences in the services they offer. Broadly, providers followed one of three models:

- **Free Access Keys:** These are services that are free to end users. They are either backed by grants or other initiatives.
- **Subscriptions:** These organizations provide VPN services for a monthly fee and operate as a business.
- **Mixed:** One provider followed a combined model, offering free access with limited bandwidth that can be extended for a small fee.

[16] Jigsaw-Code. (n.d.). Jigsaw-code/outline-server: Outline manager, developed by Jigsaw. The Outline Manager application creates and manages Outline servers, powered by Shadowsocks. Outline Manager uses the electron framework to offer support for Windows, macOS and Linux. GitHub. https://github.com/Jigsaw-Code/outline-server/tree/master/src/shadowbox

Same Need, Different Solutions

At the moment, the Outline Server code helps providers bootstrap the essential features of a VPN service, but each provider has to establish how it will be managed. While each of the providers interviewed took a different approach, they all ultimately sought to tackle the same needs, specifically:

1. Distributing access keys at scale;
2. Evading detection by censors;
3. Using resources optimally;
4. Communicating with users;
5. Managing their operation.

The goals and motivations of different providers played a determining role in the approach each took to solving these challenges. A closer look at some of these individual needs can be instructive.

Communicating with users: One provider focuses on high quality customer service. They employ three people to provide support 12 hours a day on any question users may have about the service or their account, and to help with troubleshooting. They use a ticket system to organize and keep track of their work, and have created an internal FAQ database to provide a consistent brand experience to users. In contrast, another provider emphasizes the power of open source communities and user collaboration to solve problems. They have created a telegram group chat where users of the same service post their issues and get feedback from the community. Another provider manages such a large number of users that people-powered support is an almost impossible task. As a result, they have created telegram bots to help users.

Evading detection by censors and using resources optimally: Depending on the organization, the adaptations vary in terms of sophistication as they are trying to solve different levels of complexity and scale. Providers giving free access keys have had to manage as many as half a million users, making manual load balancing infeasible. Other providers that aren't handling the same volume of traffic can manually change users to a different server in case a server gets blocked or to balance traffic across several servers to avoid overutilizing any one.

Challenges of Managing a VPN Service with Outline

The adaptations and paths each organization has taken to build their service stem from fundamental design constraints in the technology. In this section we will contextualize the most important challenges that arise from using Outline as a VPN technology.

Outline's design diverges from many other VPNs as it is an engine for services. Most VPNs don't work like this. Instead, most often users just download an app and turn the service on or create an account and pay a subscription that grants them access. Outline users must take an extra step. They have to acquire an "access key" first and add it to the app to access the service from a provider. The access key works like a password for users to access the VPN.

This design lets multiple providers offer their service using the Outline Client app rather than having to create their own app (as the access key is the way into the service).[17] This also allows users to have multiple VPN services within a single app. For example: a user could have keys from two different providers in case one fails. Alternatively, if a user frequently travels in and out of a heavily censored country, they may set up one server inside the country, allowing them to access local resources, and another outside the country, ensuring their continual access to uncensored information.

Despite their benefits, access keys also present several challenges:

Onboarding experience: *People can get lost in the multi-step process.*

A significant escalation in state censorship can cause chaos, not only for people on the ground, but also for the service providers attempting to keep them connected to the internet. As a diverse population, both in terms of age and technical know-how, seek to reconnect to their digital life en masse the onboarding process becomes critical. If people get frustrated or lost they may ultimately abandon the process altogether and remain disconnected.

> "There is a lot of friction and unknowns for people." —Provider focused on Iran

A provider focusing on Iran understood this challenge right from the start. They thought that directing users to download an app with a different name would be confusing. So they built their own app to reduce any confusion. They have further worked to create a seamless experience, eliminating the need for users to separately acquire an access key. They just download the app and it works.

[17] Get started. Outline. https://www.getoutline.org/get-started/

Providers in other regions are smaller in scale compared to this provider. The service providers focused on China and Russia interviewed during the research who we spoke to either sell subscriptions or ask for donations. They have designed the user journey of acquiring an access key (purchasing or asking for one) in ways that inform and adapt the user's mental model of the service and how it actually works. They also use the onboarding journey to explain the amount of data available to end users, the terms of service, and additional information about their service. These providers have not felt the need to create their own app, and are using the Outline app.

Avoiding detection: *When exposed, access keys can be used to easily detect servers*.

Providers have taken a range of approaches to manage server detection and blocking, including altering the design of the service to allow for easier assignment of users to servers should they need to be rotated. Service providers have additionally worked to improve performance and reduce latency of their services.

Source of Keys: *If keys are acquired online, it's not always clear who is providing the service*.

When an access key is obtained by an end user, it's not always clear who is providing the service. Access keys currently don't expose who the service provider is and keys are often shared publicly on the internet. Bad actors may potentially establish services and distribute keys in order to monitor the traffic of those attempting to circumvent censorship.

Potential misuse of keys by bad actors: *Keys can be acquired by unintended actors. Telecom providers could see the IP address and monitor traffic*.

Providers giving away access keys for free will sometimes find that their keys are distributed beyond their channels across social media or messaging platforms. This creates a risk of access keys falling into the hands of censors, potentially revealing sensitive information. For example, while we have no evidence of this occurring to date, an ISP could use an access key to monitor user traffic on a particular server.

Note: Outline's design prioritizes access in highly restricted environments over privacy and security. In contexts in which privacy and security are more important, technologies like Tor offer superior protection. For the best results, individuals can use the Tor Browser alongside an Outline server. This combination strengthens online anonymity while maintaining access to the Tor network.

(3) Operational: Needs of Large Scale Providers

Inspired by the ability of these adaptations to reach users, the research team delved deeper into the needs of these large providers. This section details several opportunities identified for the most pressing needs they shared: (a) evolving circumvention tactics, (b) improved VPN experience and (c) content controls.

(a) Evolving Circumvention Tactics

Providers interviewed who serve users in Iran, China and Russia shared that they are most worried about their services being blocked. Shadowsocks, the protocol leveraged by Outline, has been effective, but they are concerned about its resilience in the future as governments improve their censorship strategies. They feel a need to bolster their services and increase resilience. They are actively researching and considering additional circumvention methods to mitigate the risk of being blocked or seeing their service degraded, and seeking to enable the development of new strategies.

> "I'd want more ways to defend. Stealth protocols. We need to defend from Roskomnadzor. We're afraid of things getting blocked. Wireguard and OpenVPN are blocked in Russia." —Provider focused on Russia

"If we find a method that works in Iran, we can share it with the rest of the community and it can help the community work with some kind of addons for Outline and make it more effective for bypassing certain types of censorship." —Provider focused on Iran

"We have a problem in Iran: the DPI system sometimes blocks our IP addresses. We're thinking about improved masks for our traffic. Shadowsocks does okay. But I think we need more." —Provider focused on Russia

"Outline made the technology secure and working but the perception of the protocol is not great." —Provider focused on China

"Simplification is good. On the other hand, facing a censor as sophisticated as the Iranian government is difficult." —Provider focused on Iran

As censors' tactics evolve, circumvention techniques need to evolve in tandem. As voiced by providers, however, it's difficult to know how censorship, specifically the blocking of VPN services, is happening.

> "You don't know where the issue comes from. It could be the ISP, but also the many layers of the [firewall, or within the country itself]. It's basically a black box." —Provider focused on China

Providers dealing with censorship in China and Iran would benefit from knowing more about how their governments are blocking and the most effective ways to circumvent network censorship using Outline's technology.

Opportunity:

New protocols. Some providers are interested in keeping the infrastructure they've created and trying out new strategies in terms of obfuscation, encryption, protocols, proxies, ports, certificates, and other parameters. Outline could support this flexibility and learn from providers what works best in different censored environments while making the technology more resilient, relevant, and desirable for current and future providers.

Metrics to learn from the censor. Collecting anonymized data would create a better picture of reality, not only for providers but also for Outline itself and others working on internet freedom. Providers want to know, not assume, if censorship is a factor of time, port, or network, what cloud service providers are more likely to be blocked in which regions, the differences between different ISPs, if prefixes work, etc. Gathering these insights is not an easy task. There are, however, many Outline servers that could collect this information which could then be analyzed for patterns.

(b) Improved VPN Experience

The needs and opportunities for improving the VPN experience fall into four categories: managing expectations, troubleshooting, communicating status and split tunneling.

Managing Expectations

In areas of active censorship, such as Iran, VPNs do not work 100 percent of the time despite end user expectations that they will. As a consequence, when a VPN app stops working, people will often abandon it, sometimes giving up on the 'brand' altogether. Providers in these regions need to set more realistic expectations for their users to avoid losing their trust.

> "Expectation of working 100% or 70% is just an unjust expectation." —Provider focused on Iran

Opportunity:

Managing Expectations. The VPN experience users have when connections can't be made presents an opportunity to reduce friction and help users form realistic expectations.

For example, when users are unable to connect, providers could use that moment to communicate when blocking is more likely to take place, or the steps they are taking to make the service more reliable. Communicating when the service has come online again would also be valuable for end users. Communication like this could reduce the likelihood of users uninstalling or forgetting about the app.

Troubleshooting

Currently neither the Outline Client app nor the server provides the necessary information to help service providers quickly determine the type of problem a user is facing when the app has stopped working. In other words, providers need better service metrics to be more effective when troubleshooting users' problems.

> "When you can't connect, [we need] more insights into why you can't. Is it the internet? Is it because of the network? etc. We have a lot of client questions." —Provider focused on Iran

Providers using the Outline Client app don't have the ability to communicate directly with users in the app to troubleshoot problems. Troubleshooting instead relies on users checking Telegram or an email account – neither of which may be available.

> “In the app itself, there’s no way to troubleshoot.” —Provider focused on Iran

> “How can we inform the user in the app? This is a huge problem with being in an active censorship environment. That way of informing the user can be blocked itself.” —Provider focused on Iran

Additionally, some users contact the support channel of the Outline app thinking they are contacting their service provider. When they end up interacting with Jigsaw’s team instead, they are left confused and without a solution.

Opportunity:

Direct communication. Direct communication via the Outline Client app would provide a better experience for users and increase credibility for the provider, as support questions could be directed to the appropriate channel.

Better service metrics. When a user can’t connect, providers need more specific session information to help understand why a connection couldn’t be made.

Automate solutions. One provider mentioned that they would like to detect and issue automatic solutions before users need to contact them. To do this it would be necessary to define error codes that could trigger scripts and solve the issue automatically, for example moving them to a new server, re-issuing an access key, or changing the app configuration.

Communicating Status

Some providers set a bandwidth limit for users, but users can’t see how much data they have consumed in the Outline app. A provider created a workaround for this problem by writing a script that checks how much data all of their users have consumed 3 times a day. Users can message the provider’s Telegram bot to check their usage. Another provider shows this information when users log into their account on the provider’s website.

Opportunity:

Usage displays. Displaying the amount of data consumed in the app would help users manage their use of the service. It would also decrease support questions related to this information, which take time and resources from providers.

Split Tunneling

Many VPN users only want to use a VPN when they are accessing blocked or sensitive content. Otherwise, they don't need it and will use their normal connection. In some cases, accessing local sites from a server outside of the country is either impossible or a signal to censors that a VPN is being used. This can prompt a government censor to block the IP address that's accessing the service.

In Iran, domestic bandwidth is half the cost of international bandwidth for end users. When Iranians use a VPN all of their traffic is considered international, which can result in expensive bills. This feature could help reduce that cost.

Split tunneling is a modern VPN feature that can benefit users by only sending traffic that needs to be proxied through the VPN. With this feature, users or providers can predetermine which websites or apps to run through the VPN.

> "We want them to be able to constantly use the VPN... to split the service: to work with telegram and instagram; then to be able to access their Russian bank account [without a VPN]" —Provider focused on Russia

Opportunity:

Split tunneling. This functionality allows providers to offer a higher quality experience, and benefits users in a variety of ways. It (i) reduces user friction when using local services, (ii) helps manage bandwidth consumption for subscription users, (iii) allows for a faster connection to content when users don't need a proxy, and (iv) can reduce costs for users living in countries with higher fees for access to non-local services. This technique can also benefit providers. If less bandwidth is used per person, their cost per user decreases. It could also mean that their server IPs are less likely to get discovered and blocked.

(c) Content Controls

Most of the providers interviewed give free access to thousands of users. If many users misuse the service, for example, by using torrents, that has a direct impact on the cost to maintain the service and the provider's ability to support more people.

In addition to wanting to limit misuse for cost and quality purposes, multiple providers have received notices indicating that people are downloading illegal content. Currently, there's not much they can do in response, because the technology protects the user's identity. The only thing they can do is send a reminder of the terms of service to everyone assigned to the server where illegal activity was detected.

One tactic used by some providers is to host their servers in the Netherlands in order to avoid legal risks, as it's legal to download copyrighted content for personal use there. Another tactic is to use data limits. While data limits are primarily used to manage bandwidth usage, they also function as a soft tactic to discourage people from using the VPN to stream video or download torrents. Providers have found some workarounds to help reduce misuse, but they need stronger controls.

> It is hard to [detect] torrent traffic. But if [Outline] can do some limits on the server side that would be great." —Provider focused on Russia

> "If I see an abuse message, I send a notification [reminding them of] ' our rules.'" —Provider focused on Russia

> "Another thing I've seen, their servers are getting notices that people use torrents to download pirated content, etc. This is something that we are looking at. In Europe you get fines of $500-600. People [VPN services industry] were adding plugins to block torrent traffic. That might be something that managers might need. So they don't get their servers banned." —Provider focused on Iran

Opportunity:

Content controls for providers. The ability to enforce content controls would give providers a solid method to mitigate abuse and misuse of their service; affecting their costs, legal status and the resilience of their service.

Conclusion

The censorship circumvention space is highly complex due to both social realities on the ground and the ever-changing technical capabilities of governments to block the internet. As censors' tactics evolve, circumvention experts and VPN providers must evolve as well. Countering expanding internet controls will require a robust response from the entire censorship-circumvention community.

While Outline was initially developed for small scale providers – those providing access to the free and open internet for only a handful of individuals, and possibly only themselves – the community's efforts to adapt Outline's codebase to serve 10s and 100s of thousands of people reflect the urgent and growing need to protect internet access for all.

The recommendations in this report highlight the challenges large scale VPN providers have encountered in attempting to scale Outline as a service. However, they may be meaningful for other VPN providers working to counter government censorship. Specifically, the following needs will only grow in relevance in the future:

- Efficient management of end users and servers;
- New protocols to evade censors' improving technical capabilities;
- Improved channels for communication and troubleshooting;
- Privacy-preserving tooling to limit abuse.

In the fall of 2022, the Outline team released the Outline SDK, unbundling the core technologies that power Outline in order to allow others to more rapidly develop and evolve their anti-censorship approaches. The SDK is, however, only a first step. To better secure internet freedom in the future, it will be critical for the community to forge deeper connections, continue to share learnings, and develop and test a wide range of approaches that can meet the diverse challenges faced by communities around the world.

Join the Outline Community:

- Join other Outline providers on Reddit: https://www.reddit.com/r/outlinevpn/
- Join discussion on the Outline channel in the TCU Mattermost.[18]

[18] You must be a part of the Internet Freedom TCU Mattermost first.

References

Alia. (2013, June 3). Subtle censorship at its finest: Weibo took out candle icon ahead of Tiananmen anniversary. Offbeat China. https://web.archive.org/web/20140409030900/http://offbeatchina.com/subtle-censorship-at-its-finest-weibo-took-out-candle-icon-ahead-of-tiananmen-anniversary

Bigg, C. (2012, November 2). Russia's new internet blacklist. The Atlantic. https://www.theatlantic.com/international/archive/2012/11/russias-new-internet-blacklist/264434/

Business Insider. (2013, June 1). China is experimenting with a new form of internet censorship. Business Insider. https://www.businessinsider.com/chinas-new-form-of-internet-censorship-replaces-controversial-topics-with-fluff-2013-6

Freedom on the net report. (2023). Freedom House. https://freedomhouse.org/countries/freedom-net/scores?sort=asc&order=Total+Score+and+Status

Get started. Outline. (n.d.-a). https://www.getoutline.org/get-started/

How it works. Outline. (n.d.-b). https://www.getoutline.org/how-it-works/

Internet being restored in Iran after week-long shutdown. NetBlocks. (2019, March 26). https://netblocks.org/reports/internet-restored-in-iran-after-protest-shutdown-dAmqddA9

Jigsaw-Code. (n.d.). Jigsaw-code/outline-server: Outline manager, developed by Jigsaw. The outline manager application creates and manages outline servers, powered by Shadowsocks. It uses the electron framework to offer support for Windows, macos and linux. GitHub. https://github.com/Jigsaw-Code/outline-server/tree/master/src/shadowbox

Johnson, B. (2009, June 4). Chinese websites mark Tiananmen Square anniversary with veiled protest. The Guardian. https://www.theguardian.com/technology/2009/jun/04/chinese-websites-tiananmen-square-anniversary

Kılıç, D., & Chúláin, A. N. (2022, November 6). How Iranians are hopping between vpns to stay connected. euronews. https://www.euronews.com/next/2022/11/06/iran-protests-vpn-use-soars-as-citizens-seek-way-around-internet-censorship

Maxwell, A. (2023, October 31). Russia blocks 167 vpns, steps up openvpn & Wireguard Disruption * torrentfreak. TorrentFreak. https://torrentfreak.com/russia-blocks-167-vpns-steps-up-openvpn-wireguard-disruption-231031/

McConnell, E. (2023, March 29). Conclusions and opportunities from the 2022 VPN Community initiative: Digital Rights Defenders. Team CommUNITY. https://www.digitalrights.community/blog/conclusions-and-opportunities-2022-vpn-community-initiative

Meduza (2023, September 7). Russian authorities blocked more than 885,000 websites in first half of 2023. https://meduza.io/en/news/2023/09/07/russian-authorities-reportedly-blocked-more-than-885-000-websites-in-first-half-of-2023

Toh, B. (2019, November 29). Chinese police are now conducting random stop-and-search checks for banned foreign apps such as Instagram and twitter: Reports. Business Insider. https://www.businessinsider.com/chinese-police-search-banned-foreign-apps-phones-2022-11

Wikimedia Foundation. (2023, November 22). Small-World Network. Wikipedia. https://en.wikipedia.org/wiki/Small-world_network

Xynou, M. (2020, October 28). Tanzania Blocks Social Media (and tor?) on Election Day. OONI. https://ooni.org/post/2020-tanzania-blocks-social-media-tor-election-day/

Zad, A. (2022, September 29). When will Iran's internet censorship collapse? Slate Magazine. https://slate.com/technology/2022/09/iran-protests-mahsa-amini-internet-censorship.html