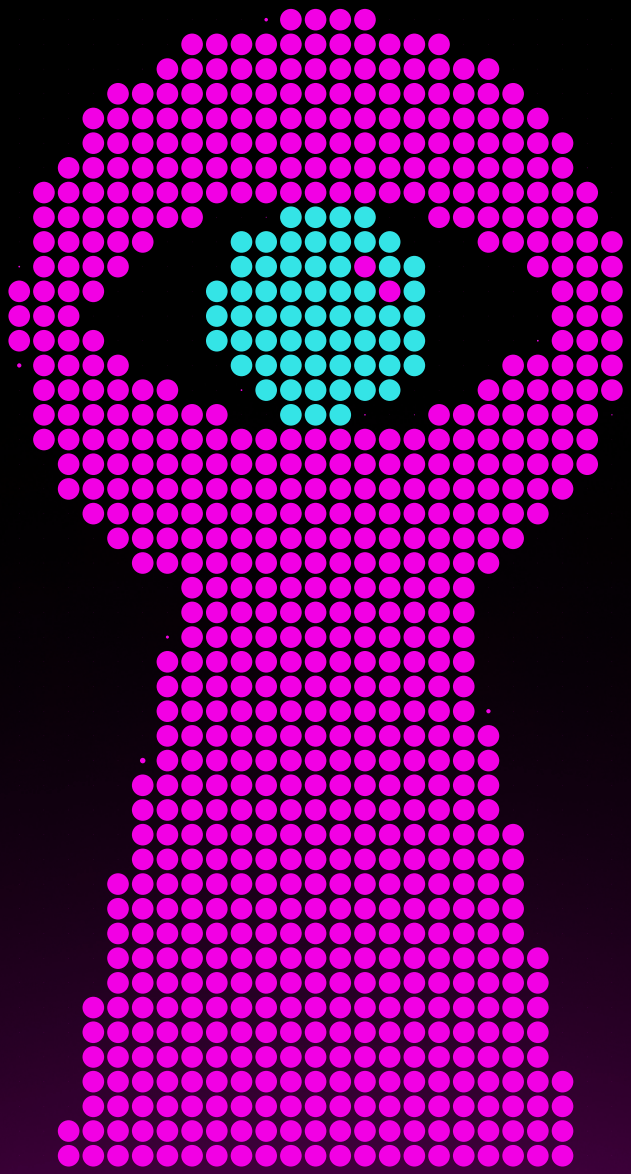
VPN TRANSPARENCY REPORT 2025

# Who owns, operates, and develops your VPN matters

An Analysis of Transparency Vs. Anonymity in the VPN Ecosystem, and Implications for Users



Benjamin Mixon-Baca | Dr. Jeffrey Knockel | Dr. Jedidiah R. Crandall

BREAKPOINTING BAD

# Table of contents

# Executive Summary

Virtual Private Networks (VPNs) are critical security and privacy infrastructure used by people all over the world to bypass geo-blocking, protect their connections on public WiFi, and hide their data from snooping internet service providers (ISPs). They have grown significantly in popularity, especially in repressive country contexts where authoritarian governments block access to websites and applications.

Commercial VPN providers operate with varying degrees of transparency and users must determine whether they value transparency more than anonymity when choosing a provider, as there are trade-offs with each. The benefit of a transparently operating provider is that the user knows who can view their communications. The limitation is that such a provider can be easily identified by authorities and subpoenaed or targeted by cyber criminals, which could put the user at risk. The benefit of an anonymously operating provider is that it cannot be easily targeted by cyber criminals or subpoenaed by authorities, which provides a level of protection for the user. The downside is that the user does not know who can view their communications, which could increase their risk of surveillance or exploitation.

Key information about VPN providers that would help users make informed decisions about the VPN they choose is often inaccessible or hard to find, though. To fill this gap, this VPN Transparency Project aims to provide VPN users with information about the degree to which providers in the VPN ecosystem operate transparently versus anonymously. In this research, I, in collaboration with Dr. Jeffrey Knockel and Dr. Jedidiah R. Crandall, used open source intelligence[1] (OSINT) collection and analysis methods to identify candidate VPNs and generate a list of providers that appeared to use anonymizing techniques to obfuscate their ownership information. We then performed static and dynamic reverse engineering to ascertain the privacy and security practices of their VPN applications. This report presents a multifactor transparency versus anonymity score for 32 VPN applications collectively exceeding nearly one billion downloads, distributed by 21 “distinct” providers. The score is modeled after FIRST Inc.'s CVSS score for quantifying software vulnerabilities, but to assess Software Provider transparency versus anonymity practices. The results within this report are intended to support informed decision making when a user selects a VPN provider.

From the 32 VPN applications and 21 VPN providers, we identified two clusters of VPN providers (consisting of three and five providers, respectively) that appear to be connected within their respective clusters. They appear to use obfuscation techniques to obscure who actually owns and operates their services and their inter-cluster relationship. The applications distributed by these providers also contain privacy and security issues that put users at risk of surveillance.

1. Open source intelligence (OSINT) is a method of collecting and analyzing data that is publicly available for purposes of research.

These eight providers distribute a total of 16 VPN applications on the Google Play Store and collectively have more than 700 million downloads.[2] Neither cluster discloses that they are related or operate together. Both sets of providers use the Shadowsocks tunneling protocol (which is not designed for confidentiality) to build the VPN tunnel, and claim their users' connections are secure. Alarmingly, both groups of providers distribute their applications with the hard-coded password embedded in their applications. Because Shadowsocks uses symmetric encryption, this means a network attacker can decrypt all communications between the VPN client and VPN server—putting the traffic of over 700 million users at risk.

## Highly Concerning VPN Providers (and Their Apps) from a Transparency and Security Perspective

| Provider Name | VPN Name | Google Play Downloads (millions) |
|---|---|---|
| INNOVATIVE CONNECTING LIMITED | **Turbo VPN** | **100** |
| | **Turbo VPN Lite** | **50** |
| | **VPN Monster** | **10** |
| LEMON CLOVE PTE. LIMITED | **VPN Proxy Master** | **100** |
| | **VPN Proxy Master - Lite** | **10** |
| AUTUMN BREEZE PTE. LIMITED | **Snap VPN** | **50** |
| | **Robot VPN** | **10** |
| | **SuperNet VPN** | **1** |
| MATRIX MOBILE PTE. LTD. | **XY VPN** | **100** |
| | **Global VPN** | **10** |
| ForeRaya Technologies PTE LTD | **Super Z VPN** | **10** |
| Hong Kong Silence Technology | **Touch VPN - Stable & Secure** | **50** |
| Yolo Technology Limited | **3X VPN - Smooth Browsing** | **100** |
| | **VPN ProMaster - Secure your net** | **50** |
| Wildlook Tech Pte Ltd | **Melon VPN - Secure Proxy VPN** | **50** |
| | **VPN Inf** | **10** |

2. We focused on Google Play Store, because the majority of downloads come from this app store, and because more than half the VPN apps we identified initially were not on Apple's App Store.

# I

# Introduction

Virtual Private Networks (VPNs) are critical security and privacy infrastructure used by people all over the world to bypass geo-blocking, protect their connections on public WiFi, and hide their data from snooping internet service providers (ISPs). VPNs have grown significantly in popularity, including in repressive country contexts. However, some VPN providers, particularly the commercial VPN services that monetize user data and serve ads, use ethically questionable practices when developing, marketing, and operating their VPNs. Moreover, key information about VPN providers that would help users make informed decisions about the VPN they choose to use is not easily accessible.

But transparency matters when choosing your VPN provider. When these applications have security vulnerabilities, such as hard-coded passwords, they potentially expose users to surveillance by digital autocrats or an attacker intercepting their data. **In contexts where individuals are criminalized for expressing themselves online or accessing information that authorities blacklist, the consequences of having their identity or online activity exposed as a result of using an insecure VPN can be devastating.**

The VPN ecosystem is large and dynamic. There are currently well over 100 VPNs across various app stores, such as the Google Play and Apple ecosystems, with new VPNs and providers being constantly added. While the owner or developer of the VPN is often documented accurately, there are a number of VPNs with tens to hundreds of millions of downloads that appear to obfuscate who actually runs them. Researchers have addressed this in the past in different ways, including security audits[3] and interviewing the VPN providers directly.[4] Google has taken steps to address security concerns for VPNs by including a badge for those that have had a security audit. Unfortunately, verifying the identity of developers is labor intensive. A lack of adequate identity verification makes it easy for potentially nefarious or malicious parties to distribute VPNs through legitimate app stores.[5] Security analysis is labor intensive as well, often leading to privacy and security issues going unnoticed.

3. See the eExternal sSecurity aAudit report from ProtonVPN: Yen, A. (2024) 'Proton VPN's no-logs policy confirmed by an external audit.' ProtonVPN. Available here: https://protonvpn.com/blog/no-logs-audit. Date accessed: 2 July 2025.
4. See the Transparency report from ProtonVPN: Proton Team (2018) 'Proton VPN Transparency Report and Warrant Canary.' Available here: https://protonvpn.com/blog/transparency-report. Date accessed: 2 July 2025.
5. An example of this is the recently discovered family of VPNs that were used to create malicious proxy networks. See Arntz, P. (2024) 'Free VPN apps turn Android phones into criminal proxies.' Malware Bytes. Available here: https://www.malwarebytes.com/blog/news/2024/04/free-vpn-apps-turn-android-phones-into-criminal-proxies. Date accessed: 4 June 2025.

II

# Why Transparency Matters When Choosing Your VPN Provider

While VPNs have a range of applications, from protecting your traffic on open WiFi networks, to circumventing censorship in repressive countries, they were not designed for truly anonymous communications. Using a VPN requires you to entrust your communications to the VPN provider. As such, while they do provide additional security through obscurity by masking a user's true IP address,[6] their security measures are not without limitations. These limitations are also not easily mitigated, because they are fundamental to VPN design.[7] This section provides an overview of how VPNs work, and describes the benefits and limitations of transparent and anonymous VPN providers.

## VPN Overview: What Happens When You Use a VPN?

VPNs are systems that change the IP address of whoever connects to them. One type of VPN is used to access resources not connected directly to the internet. These VPNs are often used in corporate, academic, or work-from-home environments. Another type of VPN, and the type considered in this report, are the type that people use to protect their private data when connecting to public WiFi, stream Netflix in other countries, or access blocked news and social media websites. There are several variations of this VPN type, but the one commonality between them all is that it encrypts your data and sends it to a proxy (VPN) server first. The proxy server then decrypts your data, changes your IP, and forwards your data to the server with which you actually want to communicate.

Because you send your data to the VPN first, the VPN can view with whom you are communicating. It can even potentially view your conversation, in the event that the server does not use Transport Layer Security (TLS).[8] It is generally understood that free services and products are not actually free; you become the product when you use them. The same is true of VPNs.

## VPN Provider Overview: Just Who Are You Transferring Your Trust To?

When selecting a VPN provider, you are implicitly transferring trust from your ISP to your VPN provider. This transfer — despite often being overlooked or ignored — carries with it significant security implications, given the access they have to your data. Furthermore, many mobile applications do not use TLS, which has serious surveillance and exploitation implications. Knowing who operates the VPN service permits the user to better understand who has access to their data and under what legal jurisdiction their data falls.

VPN providers that operate transparently are readily identifiable and can easily be subpoenaed by legal entities. They can also be targeted by attackers,

6. An Internet Protocol (IP) address is a unique numeric identifier assigned to every device that connects to the Internet.
7. For more information on the security vulnerabilities of VPNs, see our previous research, Crandall, J., Kujath, B. and Tolley, W. (2020) 'Vintage Protocol Nonsense: Annoying the TCP Stack to Uncover Tunnelled VPN Connections.' Breakpointing Bad. Available here: https://www.breakpointingbad.com/2020/05/25/Vintage-Protocol-Nonsense.html. Date accessed: 5 June 2025. See also, Mixon-Baca, B. and Crandall, J. (2021) 'Port Shadows via Network Alchemy: (CVE-2021-3773).' Breakpointing Bad. Available here: https://www.breakpointingbad.com/2021/09/08/Port-Shadows-via-Network-Alchemy.html. Date accessed: 5 June 2025.
8. Transport Layer Security (TLS) is a protocol that encrypts data sent over a network, thereby providing secure communication.

including censors. The primary benefit of a provider who is operating anonymously is that such a provider is hard to identify, and cannot be easily targeted by cyber criminals or legal entities—this can be beneficial to the user depending on the country in which they have citizenship and the legal jurisdiction of the VPN provider and server. The main drawback to using an anonymous provider, however, is that the user is trusting a total stranger, who could be leveraging their access to the user's data for any number of goals.

Oftentimes, you are able to check who the VPN provider is by visiting the developer web page posted on Google Play or iTunes. Unfortunately, because of the high volume of apps published to Google Play, iTunes, and other app stores, these distributors cannot (or do not) thoroughly review every developer. Even if they did, their legal frameworks do not condemn, nor address, the practice of obfuscating the true owners and operators of VPNs. This can be beneficial to a provider operating in a country where offering VPN services are monitored or prohibited, but makes it challenging for users who wish to know who owns the service they are using.

Some VPN providers use a lack of identity verification in app stores and their ability to set up shell corporations to their advantage, and attempt to hide who controls their services. For example, VPN apps[9] from INNOVATIVE CONNECTING LIMITED, AUTUMN BREEZE PTE. LIMITED andLEMON CLOVE PTE. LIMITED were recently found[10] to be linked to Qihoo 360, a Chinese cybersecurity company. China has highly invasive privacy laws,[11] but a user might conclude from what is stated as their country of origin on an app store that they originate from Singapore, a country with strong privacy laws. Taken at face value, Innovative Connecting PTE. Limited, Lemon Clove PTE. Limited, and Autumn Breeze are distinct VPN developers. However, closer inspection of various artifacts, such as their privacy policies and application binary code,[12] calls into question their independence.

Therefore, there are a number of considerations a person should make before choosing their VPN. These include: What are they using the VPN for? Is it for protecting financial transactions on an untrusted WiFi network, is it to bypass geo-blocking of streaming services, or is it to look at news or websites that are blocked in the country in which they reside? In the former case, using a transparent VPN provider is likely preferred. If it is the latter, perhaps it is preferred to use a provider who is not easily identified and harder for authorities to subpoena. A person may also want to consider under what legal jurisdiction the provider falls, whether the provider discloses who owns the VPN and who operates the VPN infrastructure (including the servers across the globe), and whether they disclose who develops the application.

9. These included Turbo VPN - Secure VPN Proxy, Unlimited Free VPN Monster, Hot VPN, SnapVPN, Signal Secure VPN, VPN Proxy Master, Free VPN Proxy, and Free VPN & Security.
10. See Jovanoska, A. (2025) 'What is a VPN and Why You (REALLY) Need One in 2025.' VPN Mentor. Available here: https://www.vpnmentor.com/blog/vpns-101-vpnmentors-vpn-guide-newbies/. Date accessed: 5 June 2025.
11. Tech Transparency Project (2025) 'Apple Offers Apps with Ties to Chinese Military.' Tech Transparency Project. Available here: https://www.techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military. Date accessed: 26 June. 2025.
12. Binary code is machine-readable code that consists of zeros and ones.

## Users should consider whether their use case (e.g., financial transactions on untrusted WiFi versus geoblocked streaming services) when choosing between a more transparent versus more anonymous VPN provider.

**The lack of readily organized and accessible information about transparency versus anonymity in the VPN ecosystem results in users choosing providers that may be inappropriate for their intended use case.** This research was undertaken to support users in making more informed decisions when selecting a VPN, by uncovering who owns, operates, and develops some of the most popular VPN apps downloadable via the Google Play Store.

# Unprotected Request

No VPN, user accessing a website normally

**Your Device**

Your device sends a request directly to the website (e.g., https://voanews.com).

**Firewall**

Firewall may inspect the traffic. If it's HTTP (unencrypted), it can read everything — the site, your data, and even passwords. If it's HTTPS, it sees metadata (like the domain, timing, and size) but not the contents.

**Website**

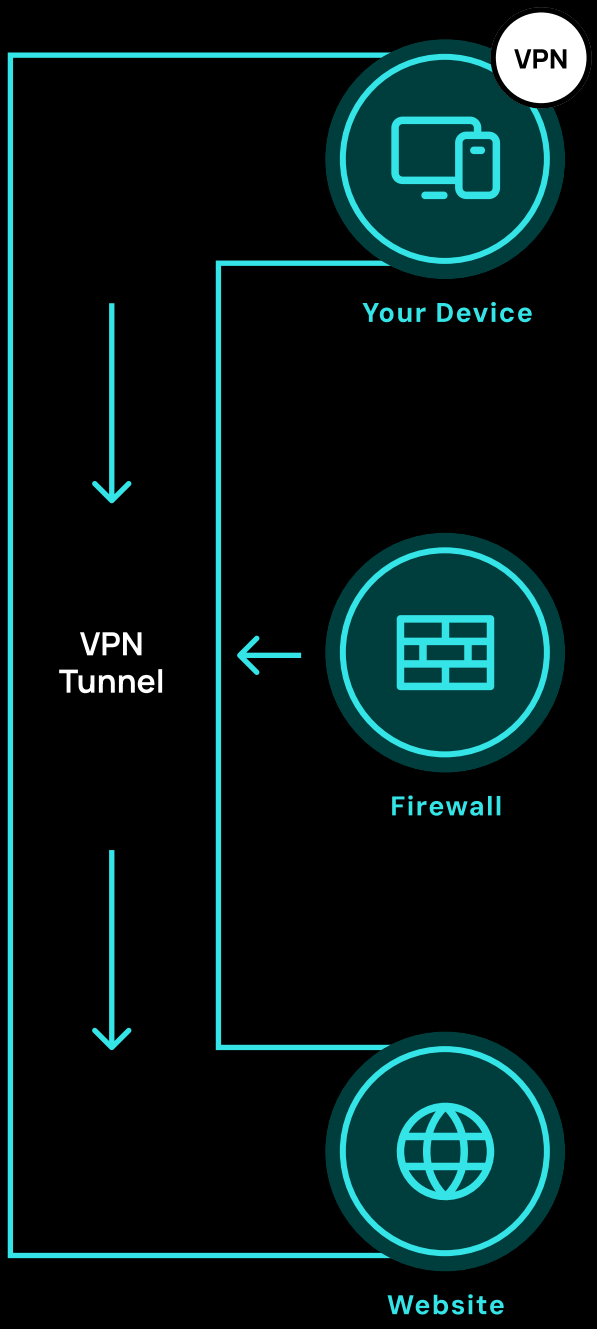
Website sees your real IP address, location, and device fingerprint.

**Summary:**

You are fully exposed. Your internet service provider (ISP) or firewall can log everything, and the website knows exactly who and where you are.

# Protected Request

VPN on, normal firewall




Your device encrypts your traffic and sends it through a VPN tunnel.

Firewall sees that you're using a VPN, but **can't see** the website you're visiting or the content of your request.

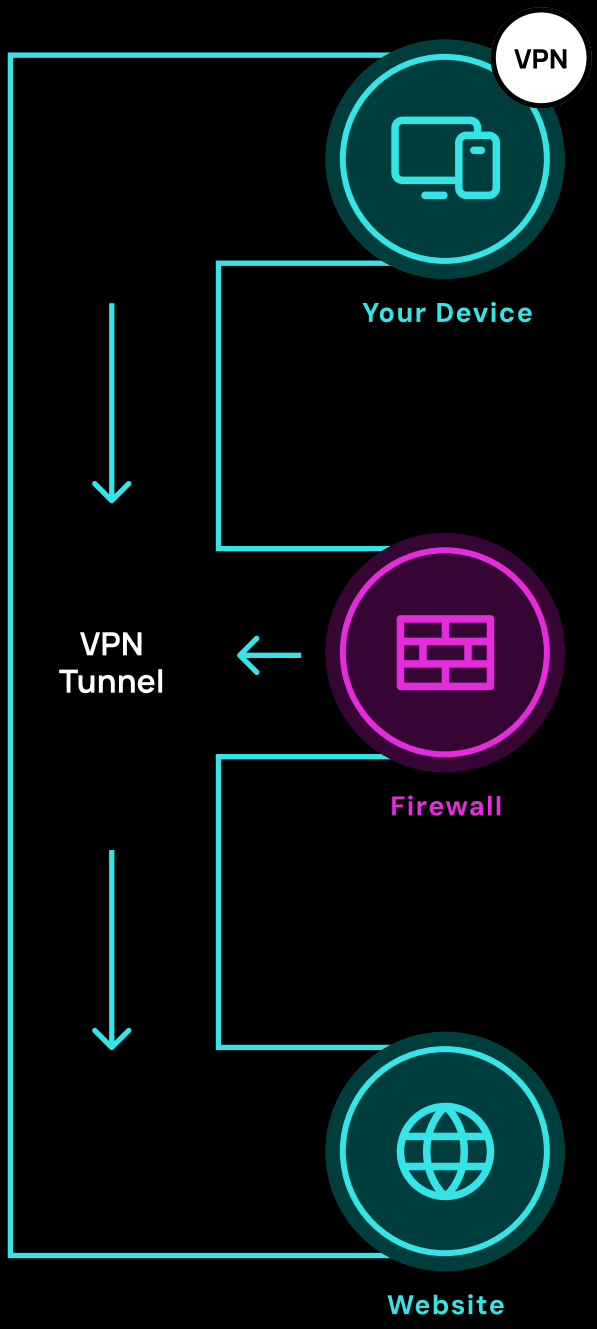
Website sees the IP address of the VPN server, not yours. Your identity and location are hidden.

**Summary:**

A normal firewall can't read your traffic, and the website only sees your VPN's IP. You're protected from local spying and basic tracking.

# Compromised Request

VPN On, firewall with hardcoded key




Your device encrypts your traffic and sends it through a VPN tunnel.

Firewall is supposed to only pass encrypted traffic — but because it has a hardcoded key, someone (e.g., the vendor, attacker, or government) may be able to:

- decrypt the VPN traffic;
- log or alter your request; and/or
- break the tunnel's confidentiality without knowledge.

VPN Server and Website behave as normal — but your traffic was already exposed earlier in the chain.

**Summary:**

You think you're protected by the VPN, but a firewall with a hardcoded key can secretly break the tunnel, exposing or altering your traffic before it ever gets to the internet.

# Project Overview

The primary goal of this project is to provide information about the degree to which VPN providers operate more transparently or more anonymously by identifying who owns, operates, and develops popular VPNs.[13] The second goal is to identify vulnerabilities and privacy and security risks in these VPN apps.

There are hundreds of millions of VPN downloads evident across app stores. Active users place a lot of trust in VPN operators, and rely on VPNs as critical security software. It is therefore vital that users understand whether a VPN provider is focused on transparent versus anonymous operation. Unfortunately, such information is not readily organized, nor easily accessible to users. There is minimal research addressing ownership transparency versus anonymity of the actors in the broader VPN ecosystem. This includes research extended to uncovering the different cloud providers in which VPN services run, the developers of VPN applications, the social media and advertising footprint of VPNs, and related business units that underpin VPN operations.

To address this gap in the research, and to achieve our first goal, we investigated and compiled this information to demonstrate the extent to which the owners, operators, and developers of the VPNs selected for this study operate transparently versus anonymously. Towards our second goal, we conducted a deep technical analysis to determine whether there is a connection between VPN provider transparency and security practices. The ranking enabled us to develop a case study, which provides a comparative analysis between VPNs with high transparency (low anonymity) and those with low transparency (high anonymity). Lastly, this report also presents recommendations on which apps to use and which to avoid (depending on their specific use case), and which have privacy and security issues.

13. Identified as those with over one million downloads.

# Project Objectives

Given that VPN user security is dependent on the owners, operators, and developers of these systems, this research aimed to:

a) **Identify** the owners, operators, and developers of VPN software used by people in repressive countries to bring transparency to this area;

b) **Inform** users about the degree to which VPN services are operating transparently; and

c) **Encourage** large organizations like Apple and Google to prioritize user privacy, security, and safety take user safety seriously vis-a-vis VPN privacy and security.

In the near term, this project seeks to improve the safety of users by providing high quality information about the owners, developers, and operators of widely used VPN service providers and report vulnerabilities in their software. In the long term, this project aims to motivate and inspire commercial application distributors like Google and Apple to change how owner/operator transparency (or the lack thereof) is verified within the VPN ecosystem.

Google and Apple profit off of the apps they feature in multiple ways, from the subscriptions they sell, to the ad libraries apps use. It is in their financial interest to protect their brand integrity and revenue streams by protecting their user base. Considering that certain companies developing apps are tied to foreign intelligence servers, or that certain VPNs have major security flaws, maintaining these apps on their platforms exposes users to high levels of risk of surveillance and exploitation.

For many applications, such as games or productivity apps, transparency is arguably less important. However, VPNs, anti-virus, and other security tools, given their goals and the extent of trust that users place on them, should be held to higher levels of scrutiny prior to distribution, both in terms of ownership, transparency, and application security. Ideally, distributors would consider transparency as much of a priority as they do security when assessing VPN provider utility and viability.

# IV

# Common Transparency Scoring System (CTSS)

For the purposes of this report, "transparency" means that the VPN provider is not doing anything to obscure their identity. The biggest risks a user faces when using a VPN are unintentionally handing over their data to an anonymous VPN provider that they assume is operating transparently, or using an insecure application that compromises their privacy. We presume an entity to be "anonymous" when its actual legal jurisdiction is different from what a reasonable person would conclude from a cursory examination of the provider's app store profile and website. For example, this study discovered that there are VPN providers that claim their legal jurisdiction is Singapore, when in reality it is China. This is a major violation of trust, because the data protection laws applied to businesses in Singapore are significantly different from those applied to Chinese businesses.

In order to examine VPN provider transparency robustly, after taking into account potential OSINT limitations, data was collected based on five combined transparency factors:

1) **Business Operations Transparency**
2) **Code Transparency**
3) **Social Media Transparency**
4) **Network/Domain Transparency**
5) **Manual Analysis**

Manual Binary Analysis was included for VPN applications with particularly high or particularly low transparency scores based on the initial four combined transparency factors. The Common Transparency Scoring System is modeled after the Common Vulnerability Scoring System (CVSS),[14] developed by the Forum of Incident Response and Security Teams, Inc. (FIRST) corporation to communicate how serious computer vulnerabilities are to different stakeholders (from security analysts to C-Suite executives).

These five components are explained below, including why each factor is important and how it contributes to an application's overall transparency score.

14. First.org (no date) 'Common Vulnerability Scoring System version 4.0: Specification document.' First.org. Available here: https://www.first.org/cvss/v4-0/specification-document. Date accessed: 11 July 2025.

# 01. Business Operations Transparency

## What Is This Factor?

This scoring factor combines available information about the owner, developer, and operator of a VPN application. We used the website, the terms of service, and the privacy policy listed on the Google Play Store as the starting points for ascertaining this information. From here, other information, such as social media accounts, and information about the operating organization, and development and management teams, populate the remaining sections of this scoring factor.

## Why Is It Important?

The jurisdiction in which the VPN operates plays a major role in a VPN's capacity to offer a secure service. This is because there are policies specific to each jurisdiction with which a VPN operator must comply. These include policies requiring VPNs to log user data, comply with law enforcement in the jurisdiction in which the provider is based, and comply with foreign law enforcement organizations, such as, the International Criminal Police Organization (INTERPOL). A VPN provider based in the United States, Switzerland, or the U.S. Virgin Islands, compared to Russia or China, for example, would be required, by law, to comply with very different data retention and data disclosure policies.

When a VPN provider discloses information about their jurisdiction on the Google Play Store or their website, for example, a user might assume they know under what jurisdiction their data would be subject, and can assess the risk accordingly. However, this information is sometimes obfuscated, whereby a VPN provider purporting to be based out of Singapore is in fact headquartered in Beijing, for example. Such obfuscation makes it harder for law enforcement or attackers to target the specific provider, but also prevents the user from knowing under what jurisdiction their data falls, and whether they can expect their data to be logged or the provider to comply with law enforcement.

## Business Operation Transparency Subfactors

Specifically, Business Operation Transparency is composed of five subfactors that contribute to the overall Business Operation transparency score. They are:

**Does the VPN Have a Website?**

This factor indicates whether the VPN has a credible website. In some cases, the website provided on distributor platforms can barely be regarded as a reliable source of information about the VPN provider.[15]

15. For example, Cookie Devs, developers of Ciao Proxy Pro and other VPN/Proxy solutions' web page is absent of any content except for the phrase "hello man."

### Does the VPN Have a Privacy Policy?

This factor can be useful to a user wanting to understand the logging and data collection policies of a VPN.

### Are Portions of the Privacy Policy Text Shared with Other VPNs?

Shared text between the privacy policies of two or more VPNs can be an indication of deception if the VPN providers in question do not disclose the relationship.

### Does the VPN Have an About Section?

This factor indicates that the VPN provider has information about who is operating the VPN service. A total lack of such a section is a clear indication that the VPN operates more anonymously than transparently.

### Are There Additional Business Filings?

This factor indicates whether information beyond what is provided on the website is available. This can include information such as tax, copyright, or similar legal records. Such documentation can provide valuable insight about the degree to which a provider operates transparently versus anonymously.

### Are the Legal Jurisdictions between Website, App Store, and Business Filings Consistent?

This factor indicates whether there are inconsistencies between the jurisdiction claimed on the website, app store, and legal documentation.

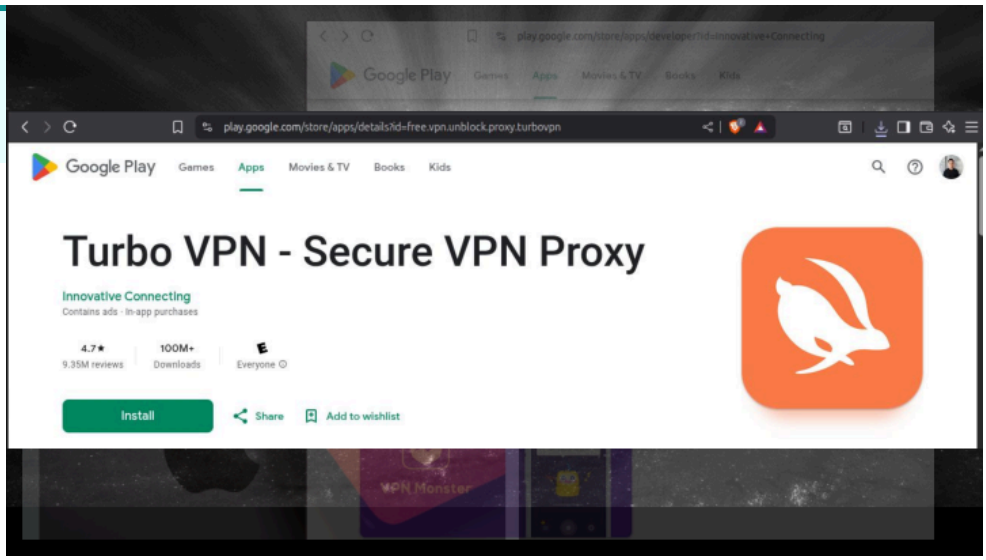



**Figure 1.**
Turbo VPN Google Play page by Innovative Connecting.

**Figure 2.**
Turbo VPN's website

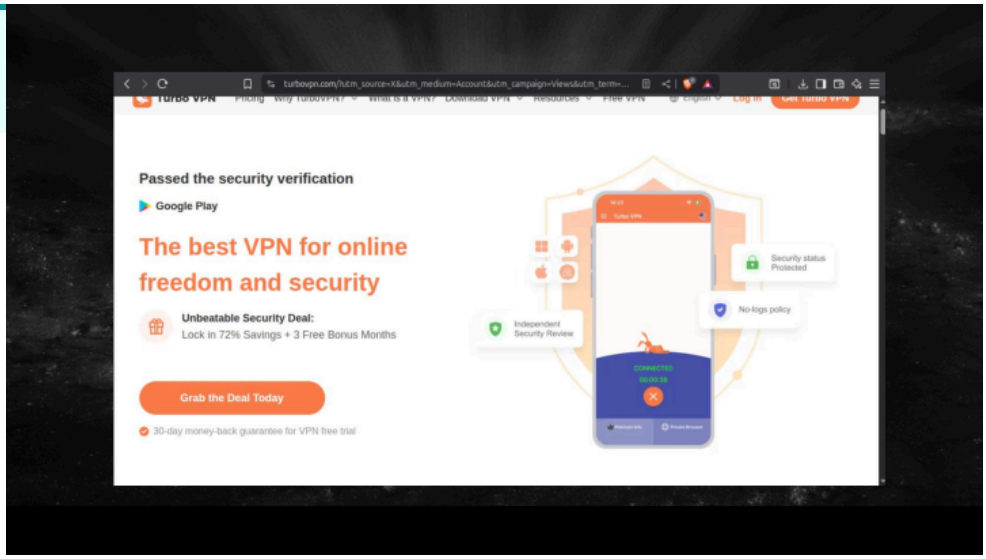



**Figure 3.**
Turbo VPN claims (incorrectly) that it passed security verification and that it is designed for security. Shadowsocks was not designed to enforce confidentiality.

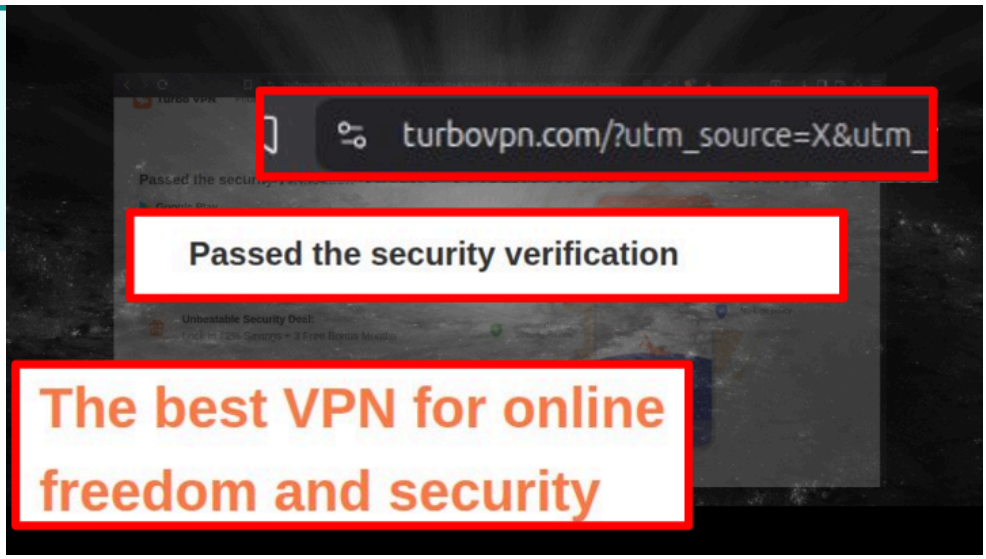



**Figure 4.1**
Innovative Connecting, Autumn Breeze, and Lemon Clove have business records on OpenCorporates. They were incorporated within days of one another and in the same business district in Singapore.

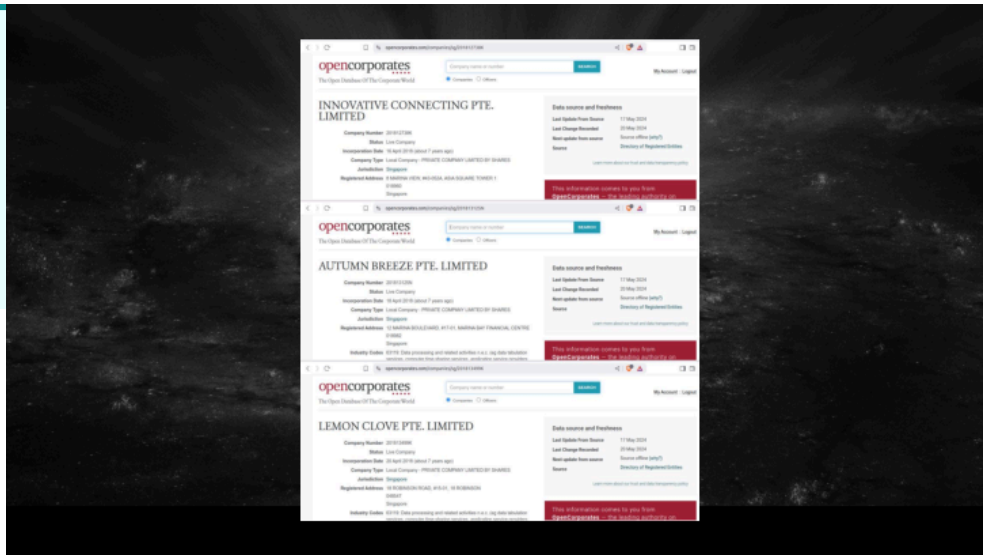


**Figure 4.2**

Innovative Connecting, Autumn Breeze, and Lemon Clove, were incorporated within days of one another and in the same business district in Singapore.


**Figure 5.**

Innovative Connecting claims to be based out of Singapore but is really run out of Beijing, China.

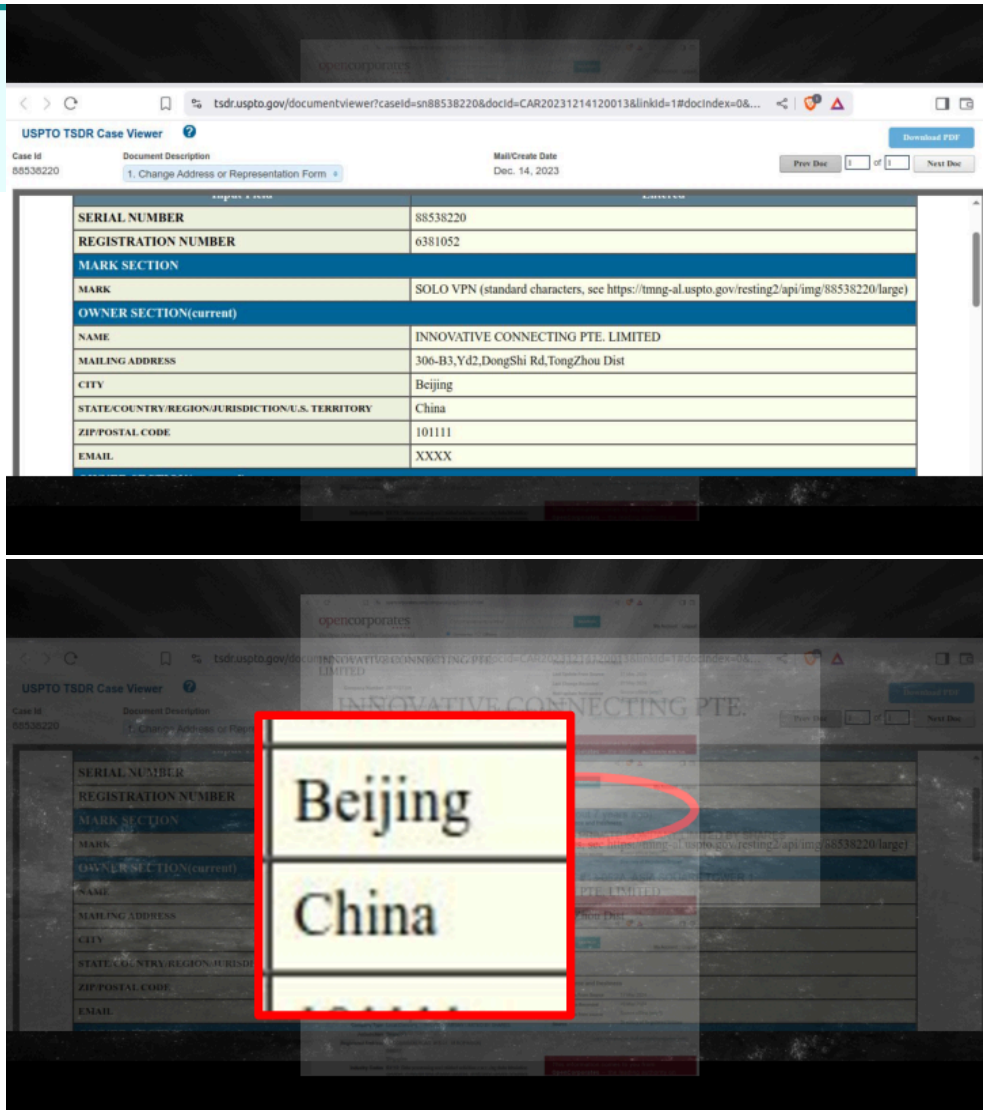


**Figure 6.**
Google Play Store page for Global VPN by Matrix Mobile.

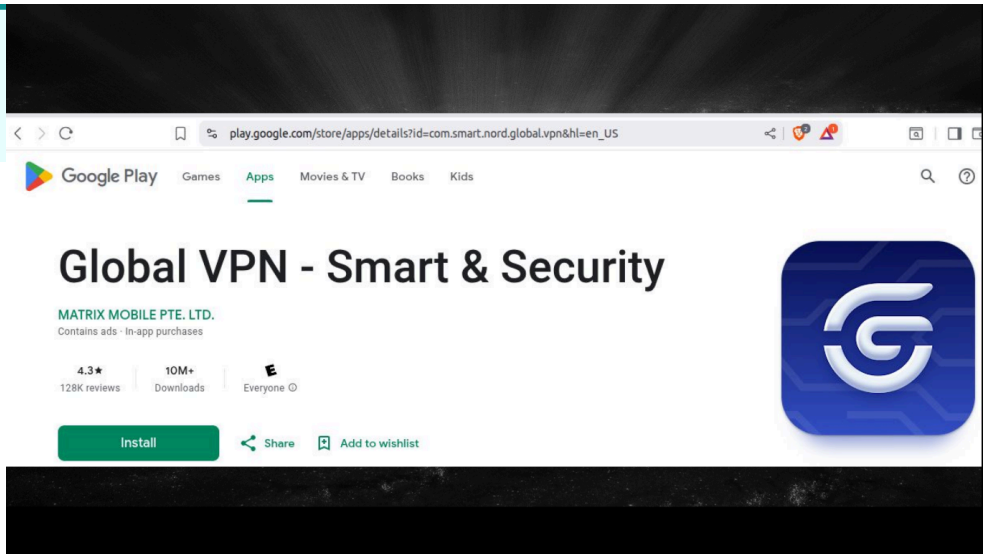



**Figure 7.**
Matrix Mobile. was incorporated in Singapore in 2020.

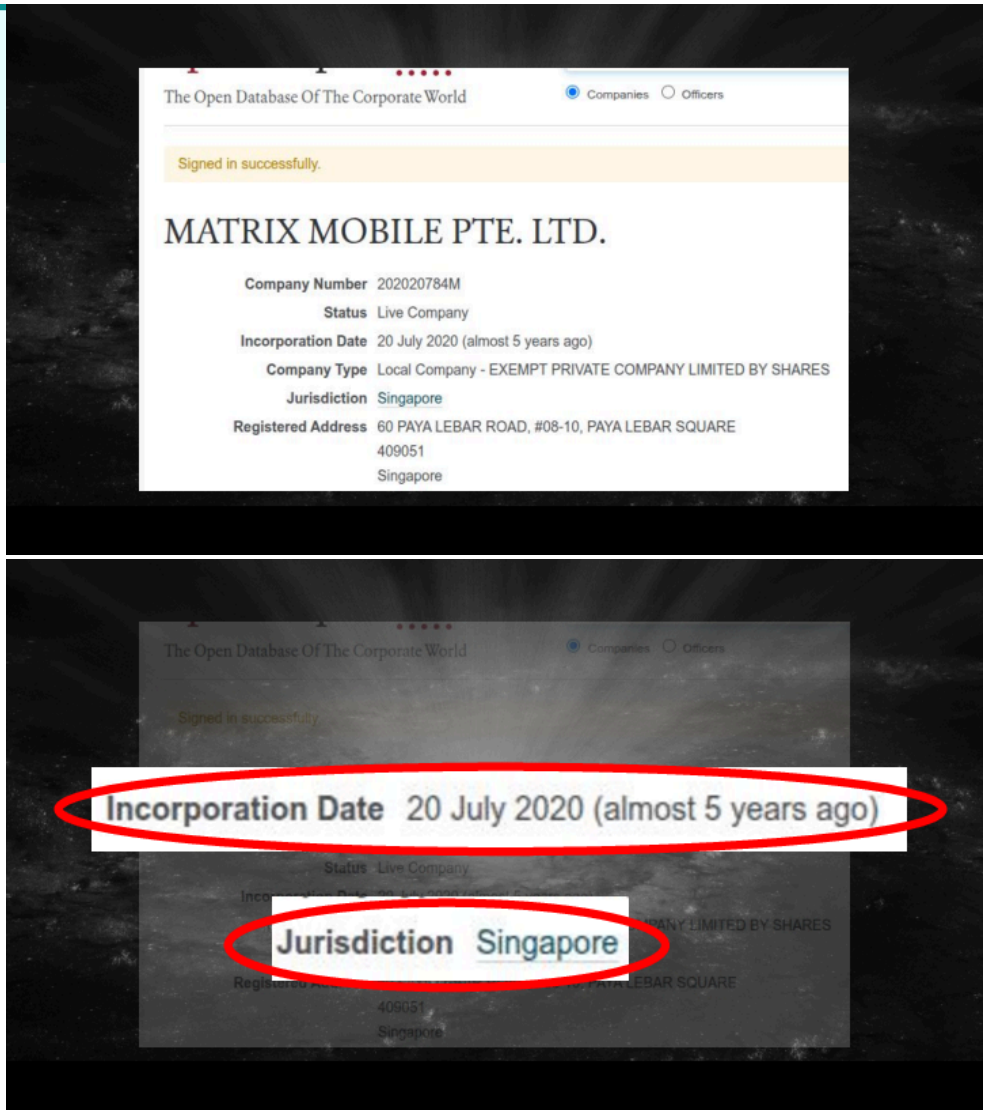


**Figure 8.**

Super Z VPN, based out of Hong Kong, China (and provided by ForeRaya Technologies), is related to Matrix Mobile's Global VPN based on our findings through reverse engineering that they—along with the six other VPNs in this family— share highly similar binary APK code, hardcoded Shadowsocks credentials, and VPN server infrastructure. None of this is clear from the information provided on their Google Play Store page.

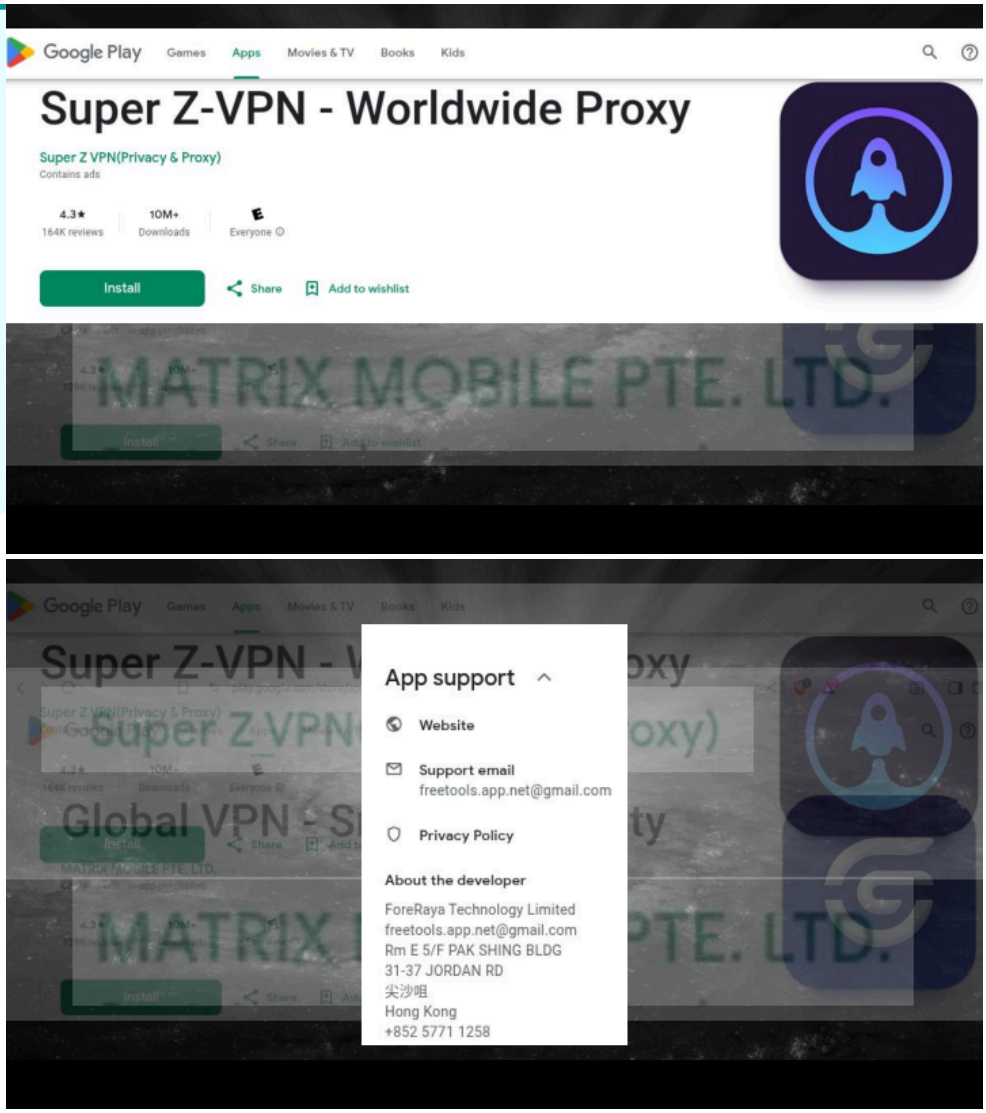



**Figure 9.**

Super Z VPN's website is essentially non-existent.

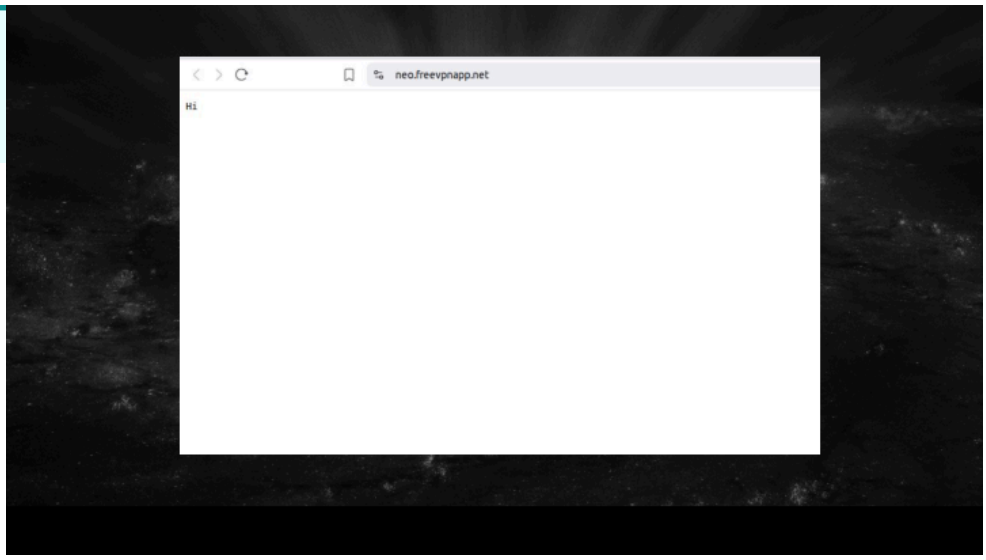


**Figure 9. (continued)**
Super Z VPN's website is essentially non-existent.

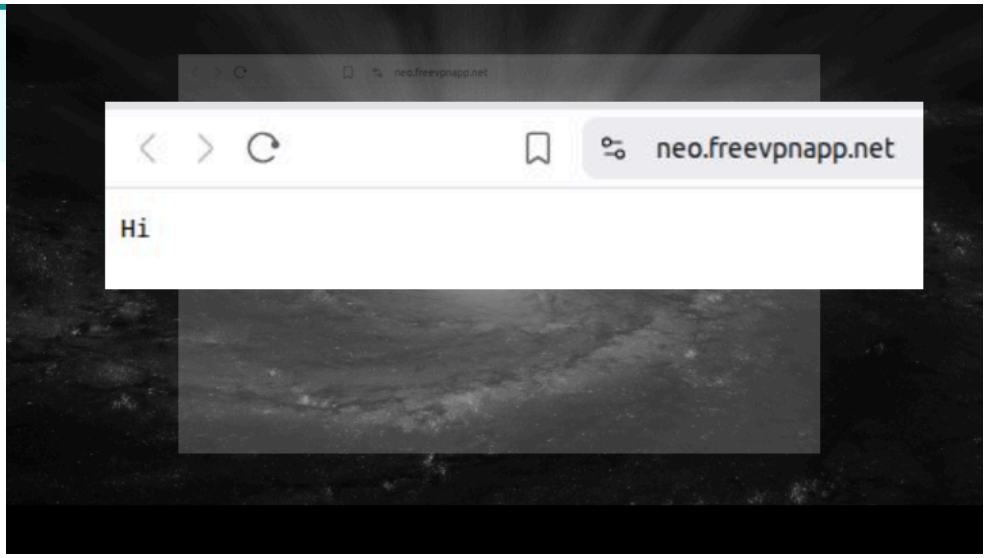



**Figure 10.**
Super Z VPN's provider, ForeRaya Technology, has no business records available on OpenCorporates.

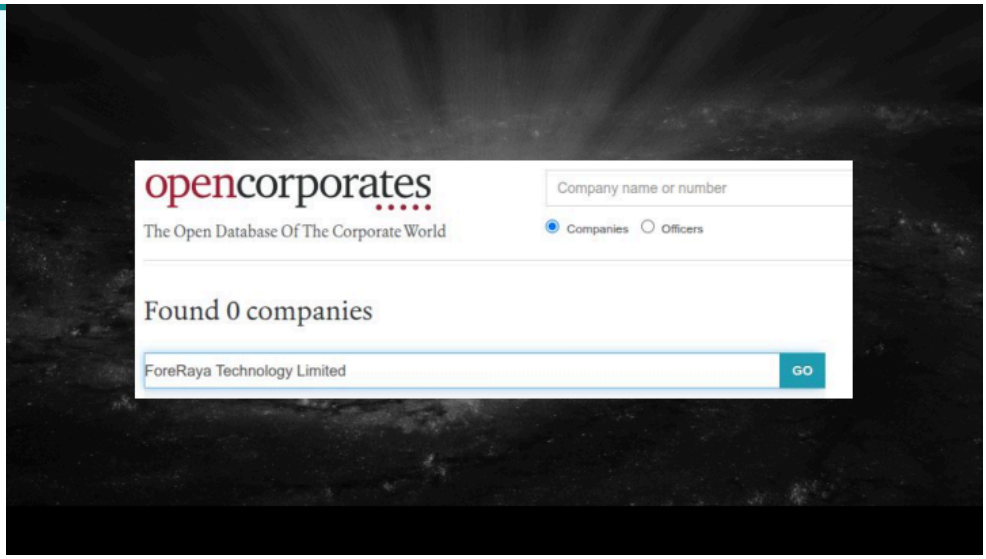
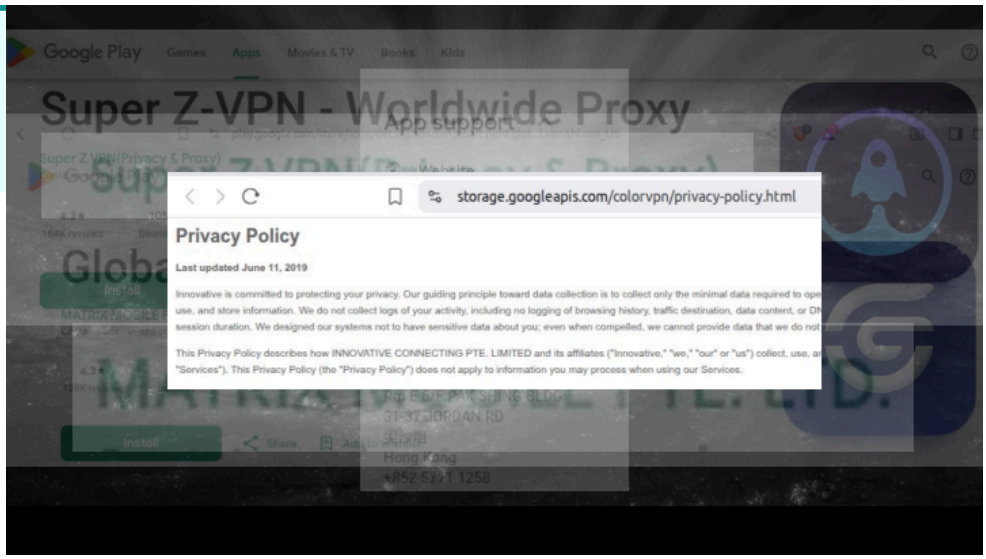



**Figure 11.**
Super Z VPN's privacy policy references the VPN provider Innovative Connecting.



## Factor Weight

This combined factor has a *high* impact on the application's transparency score. This impact was determined primarily by the fact that when a VPN provider obfuscates their operational jurisdiction, it is a major indicator of anonymous-focused operation. It can also signify deception.[16]

## Limitations

There are three limitations to this methodology. First, not every VPN provider has a website, which makes identifying other information, such as business filings, challenging to find. In several instances, we were unable to identify any business filings.

Another limitation of this methodology is that some providers may have business filings, but they are only accessible through expensive third-party services who charge for business records. While OpenCorporates[17] has a large volume of such documents, it is impossible for them, or similar business transparency firms, to guarantee they will have documentation for a given business. There may also be business filings that we were unable to identify due to limitations in our search methodology.

Finally, in relation to subfactor 6, **"Are the legal jurisdictions between website, app store, and business filings consistent?",** it is not uncommon for businesses to be based out of one country and have leadership with diverse nationalities, or to be a subsidiary of a holding company. For example, Kape Technologies is a major holding company that owns over five VPN services, including ExpressVPN, Private Internet Access (PIA VPN), and others. Even if a VPN provider's ownership is inconsistent between website and business filings, this alone is not an indicator of deceit. We ameliorate this by factoring in the data privacy laws of the countries that ultimately control VPN providers. We also consider the other scoring factors when making a determination about transparent versus anonymous operation.

16. It is important to note that this decision was informed by the research performed and is based on the opinion of the author. Readers should take this into account when using the information herein to determine whether they believe this is a major issue.
17. Available here: https://opencorporates.com/. Date accessed: 5 June 2025.

# Results: Business Operations Transparency

| VPN APP | Does the VPN have a developer website? | Does the VPN have a privacy policy? | Are portions of the privacy policy text shared with other VPNs? | Does the VPN have an 'About' section? | Are there additional business filings? | Are legal jurisdictions between website and business filings consistent? |
|---|---|---|---|---|---|---|
| Mullvad | 2 | 2 | 1 | 1 | 1 | 1 |
| TunnelBear | 2 | 2 | 1 | 1 | 1 | 1 |
| Lantern | 2 | 2 | 0 | 1 | 1 | 1 |
| Psiphon | 2 | 2 | 0 | 1 | 1 | 1 |
| Proton VPN | 2 | 2 | 0 | 1 | 1 | 1 |
| Turbo VPN – Secure VPN Proxy | 2 | 1 | 1 | 1 | 1 | 0 |
| Turbo VPN Lite – VPN Proxy | 2 | 1 | 1 | 1 | 1 | 0 |
| VPN Monster – Secure VPN Proxy | 2 | 1 | 1 | 1 | 1 | 0 |
| SnapVPN | 2 | 1 | 1 | 1 | 0 | 0 |
| SuperNet VPN | 2 | 1 | 1 | 1 | 0 | 0 |
| Signal Secure VPN – Robot VPN | 2 | 1 | 1 | 1 | 0 | 0 |
| VPN Proxy Master Pro | 2 | 1 | 1 | 1 | 0 | 0 |
| VPN Proxy Master Lite | 2 | 1 | 1 | 1 | 0 | 0 |
| Hot VPN | 1 | 1 | 1 | 0 | 0 | 0 |
| Secure VPN – Safer Internet | 2 | 1 | 1 | 1 | 0 | 0 |
| Thunder VPN Fast, Safe VPN | 2 | 1 | 1 | 1 | 0 | 0 |
| Lets VPN | 2 | 1 | 1 | 1 | 0 | 0 |
| Astrill VPN | 2 | 2 | 1 | 1 | 0 | 0 |
| Cookie | 0 | 0 | 0 | 0 | 0 | 0 |
| Ciao Proxy Pro | 0 | 0 | 0 | 0 | 0 | 0 |
| Ciao Proxy | 0 | 0 | 0 | 0 | 0 | 0 |
| VPN – Super Unlimited Proxy | 0 | 0 | 0 | 0 | 0 | 0 |
| PureVPN | 2 | 1 | 1 | 1 | 1 | 0 |
| Potato VPN | 2 | 1 | 1 | 1 | 1 | 0 |
| Global VPN | 0 | 0 | 0 | 0 | 0 | 0 |
| Melon VPN | 1 | 1 | 1 | 0 | 1 | 1 |
| Super Z VPN | 1 | 1 | 2 | 0 | 0 | 0 |

| VPN APP | Does the VPN have a developer website? | Does the VPN have a privacy policy? | Are portions of the privacy policy text shared with other VPNs? | Does the VPN have an 'About' section? | Are there additional business filings? | Are legal jurisdictions between website and business filings consistent? |
|---|---|---|---|---|---|---|
| Touch VPN - Stable & Secure | 1 | 1 | 2 | 0 | 0 | 0 |
| VPN ProMaster-Secure your net | 1 | 1 | 2 | 0 | 0 | 0 |
| 3X VPN - Smooth Browsing | 1 | 1 | 2 | 0 | 0 | 0 |
| VPN Inf | 1 | 1 | 0 | 0 | 1 | 0 |
| Melon VPN - Secure Proxy VPN | 1 | 1 | 0 | 0 | 1 | 0 |

**Score explanation:**

For each Business Operations Transparency Subfactor, a VPN Provider can receive a score of 0, 1, or 2.

- 0 = Suspicious.
- 1 = Worth Consideration.
- 2 = OK.

Color coding

- Dark shading indicates the provider operates more anonymously.
- White indicates transparent operation.
- Red indicates suspicious findings.

# 02. Code Transparency

## What Is This Factor?

The code transparency factor summarizes information about the coding practices and footprint of the VPN provider. This can provide supplemental information about the transparency versus anonymity practices of the VPN provider, such as whether their code is open source, and on what repositories the code is stored.

## Why Is It Important?

The code is ultimately what dictates the behavior of a VPN application. For example, the code might collect various identifiers for a user, such as their device ID, location information, and other hardware and software identifiers. One way to tell whether a VPN provider focuses on transparency versus anonymity is whether their code is open source or otherwise broadly accessible. Open source code is the gold standard for transparency. This does not mean that the application running on the device is necessarily derived from the same code as that which is made open source, but it at least demonstrates that the VPN provider is making accessible the details of how they are handling users' information. The absence of an open source code base is not in and of itself a risk factor, but having deeper insight into how the application works is a good starting point for transparency.

## Code Transparency Subfactors

The code transparency subfactors are by no means exhaustive but through preliminary analysis, have served as indicators about the transparency with which VPN providers operate. Some VPN providers choose to make their application open source, and typically distribute that code on at least one Git repository (where software developers can access, share, and track changes to code). The subfactors contributing to code transparency are:

**Is the Application Open Source?**
In the context of this project, open source means that the code is publicly available for anyone to view, audit, or modify.

**Does the Provider Have a GitHub?**
This factor indicates that the provider has made their code available on GitHub.[18]

18. GitHub is an online version control system frequently used by programs to keep track of changes to the software in addition to making it publicly available in some cases. GitHub is currently owned by Microsoft.

**Does the Provider Have GitLab?**
This factor indicates that the provider has made their code available on GitLab.[19]

**Does the Provider Have Gitee?**
This factor indicates that the provider has made their code available on Gitee.[20] While it is less likely that VPN providers will distribute their code via Gitee, it was included for completeness.

**Other?**
This factor indicates that the provider has made their code available by some other means, such as an SVN or CVS server,[21] or their website.

## Factor Weight

This combined factor has a *medium* impact on the application's transparency score. This impact was determined by observing the practices of multiple VPN providers in the ecosystem. Generally, we found the most transparent providers make their code open source or at least publicly available, although there are many reasons why a VPN provider would choose not to do so. However, an open source VPN, or more broadly, a publicly available code-base, demonstrates that the provider has made efforts to permit public auditing of their codebase. In general, the application will score high on transparency if it is freely available for inspection, analysis, and download. It will score low if not publicly available.

## Limitations

There is one key limitation to this scoring factor. In the event that a VPN provider's code is accessible for third-party analysis, the code in the repository may differ from the application code distributed by the app store or website and installed on users' devices. We addressed this by analyzing the "ground truth," by reverse engineering the application as installed on a device.

19. GitLab is an alternative online version control system owned primarily by VanGuard Group, Incorporated.
20. Gitee is a Chinese-owned online Git repository.
21. Both Subversion (SVN) and Concurrent Versions System (CVS) servers act as repositories where software developers can access, share and track changes to code and other project files.

# Results: Code Transparency

| VPN App | Is It open source? | Has GitHub? | Has GitLab? | Has Gitee? | Other? |
|---|---|---|---|---|---|
| Mullvad | 1 | 1 | 0 | 0 | 0 |
| TunnelBear | 0 | 1 | 0 | 0 | 0 |
| Lantern | 0 | 1 | 0 | 0 | 0 |
| Psiphon | 0 | 1 | 0 | 0 | 0 |
| Proton VPN | 1 | 1 | 0 | 0 | 0 |
| Turbo VPN – Secure VPN Proxy | 0 | 0 | 0 | 0 | 0 |
| Turbo VPN Lite – VPN Proxy | 0 | 0 | 0 | 0 | 0 |
| VPN Monster – Secure VPN Proxy | 0 | 0 | 0 | 0 | 0 |
| SnapVPN | 0 | 0 | 0 | 0 | 0 |
| SuperNet VPN | 0 | 0 | 0 | 0 | 0 |
| Signal Secure VPN – Robot VPN | 0 | 0 | 0 | 0 | 0 |
| VPN Proxy Master Pro | 0 | 0 | 0 | 0 | 0 |
| VPN Proxy Master Lite | 0 | 0 | 0 | 0 | 0 |
| Hot VPN | 0 | 0 | 0 | 0 | 0 |
| Secure VPN – Safer Internet | 0 | 0 | 0 | 0 | 0 |
| Thunder VPN Fast, Safe VPN | 0 | 0 | 0 | 0 | 0 |
| Lets VPN | 0 | 0 | 0 | 0 | 0 |
| Astrill VPN | 0 | 0 | 0 | 0 | 0 |
| Cookie | 0 | 0 | 0 | 0 | 0 |
| Ciao Proxy Pro | 0 | 0 | 0 | 0 | 0 |
| Ciao Proxy | 0 | 0 | 0 | 0 | 0 |
| VPN – Super Unlimited Proxy | 0 | 0 | 0 | 0 | 0 |
| PureVPN | 1 | 1 | 1 | 1 | 1 |
| Potato VPN | 1 | 1 | 1 | 1 | 1 |
| Global VPN | 0 | 0 | 0 | 0 | 0 |
| Melon VPN | 0 | 0 | 0 | 0 | 0 |
| Super Z VPN | 0 | 0 | 0 | 0 | 0 |
| Touch VPN – Stable & Secure | 0 | 0 | 0 | 0 | 0 |
| VPN ProMaster-Secure your net | 0 | 0 | 0 | 0 | 0 |

| VPN App | Is it open source? | Has GitHub? | Has GitLab? | Has Gitee? | Other? |
|---|---|---|---|---|---|
| 3X VPN - Smooth Browsing | 0 | 0 | 0 | 0 | 0 |
| VPN Inf | 0 | 0 | 0 | 0 | 0 |
| Melon VPN - Secure Proxy VPN | 0 | 0 | 0 | 0 | 0 |

**Score explanation:**

For each Code Transparency subfactor, a VPN provider can receive a score of 0 or 1.

- 0 = False.
- 1 = True.

Color coding:

- Dark indicates more anonymous operations.
- White indicates more transparent operations.

# 03. Social Media Transparency

## What Is This Factor?

The social media scoring factor characterizes the social media footprint of VPN providers online. Information for this scoring factor is collected from social media links, which are either available on the application's linked website, and from using social media Application Programming Interfaces (APIs)[22] to search for associated accounts.

## Why Is It Important?

Social Media Transparency can provide insight into the degree to which VPN providers engage with the public. A VPN provider may make announcements about updates to their product, offer direct support, or engage in discussion about privacy-related issues. Additionally, VPN providers may use various advertising services, such as Facebook advertising, to appeal to various user demographics about their applications and services.

## Social Media Transparency Subfactors

**Does the VPN Have Contact Information Publicly Available?**
A provider that does not offer such contact information operates more anonymously than transparently.

**Does the VPN Have a Facebook Page?**

**Does the VPN Have an Instagram Profile?**

**Does the VPN Have an X Profile?**

**Does the VPN have a Telegram account?**

**Does the VPN Provider Have a Discord Channel?**

**Are There Suspicious Claims or Complaints About the VPN Provider From Users on a Platform?**
This indicator is important from a transparency perspective, as users may

22. Social media APIs are a set of tools that allow applications to interact with social media platforms.

complain about certain characteristics and practices of the VPN. Care should be taken when interpreting such negative comments, however, because it could be a competitor VPN attempting to harm the reputation of a legitimate provider.

**Does the VPN Use Advertisements for Suspicious Targeting?**
This is another subtle, but important, indicator from a transparency standpoint. For example, a VPN could be targeting users for legitimate purposes, but they could also be targeting children or minors, which is potentially suspicious and worth further investigation.

It is important to note that not having social media profiles, such as on Facebook, Instagram, X, Telegram, or Discord, is not necessarily an indication of deception. In fact, having one might be an attempt to seem legitimate. The subfactors are nonetheless included, because either way, it gives the user insight about the social media footprint of the provider.

**Figure 12.**
Innovative Connecting's LinkedIn profile.

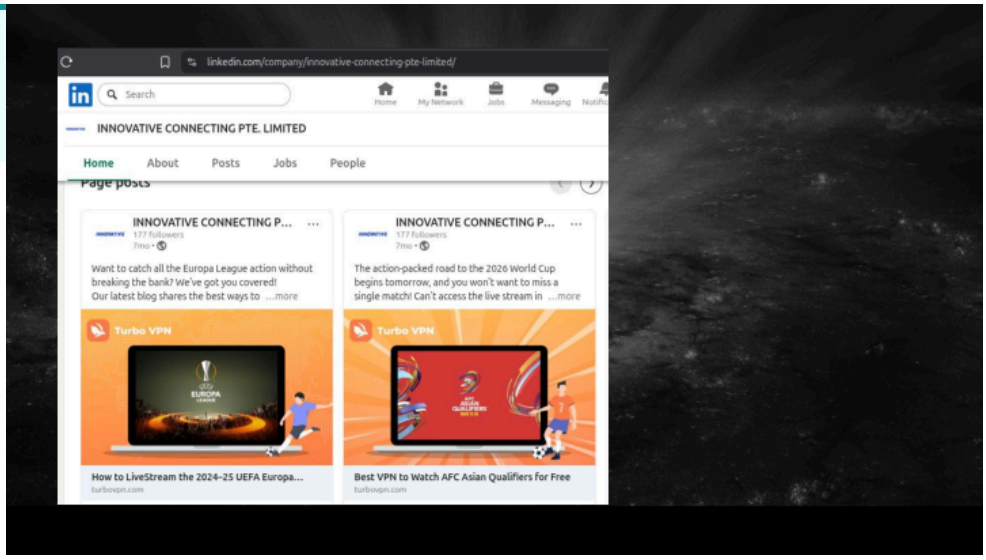



**Figure 13.**
TurboVPN's X profile page.

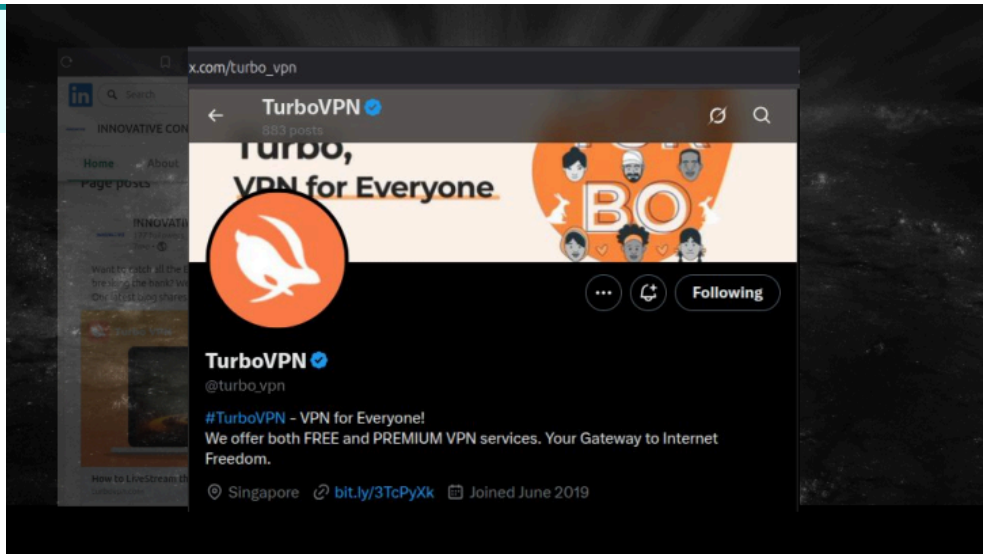
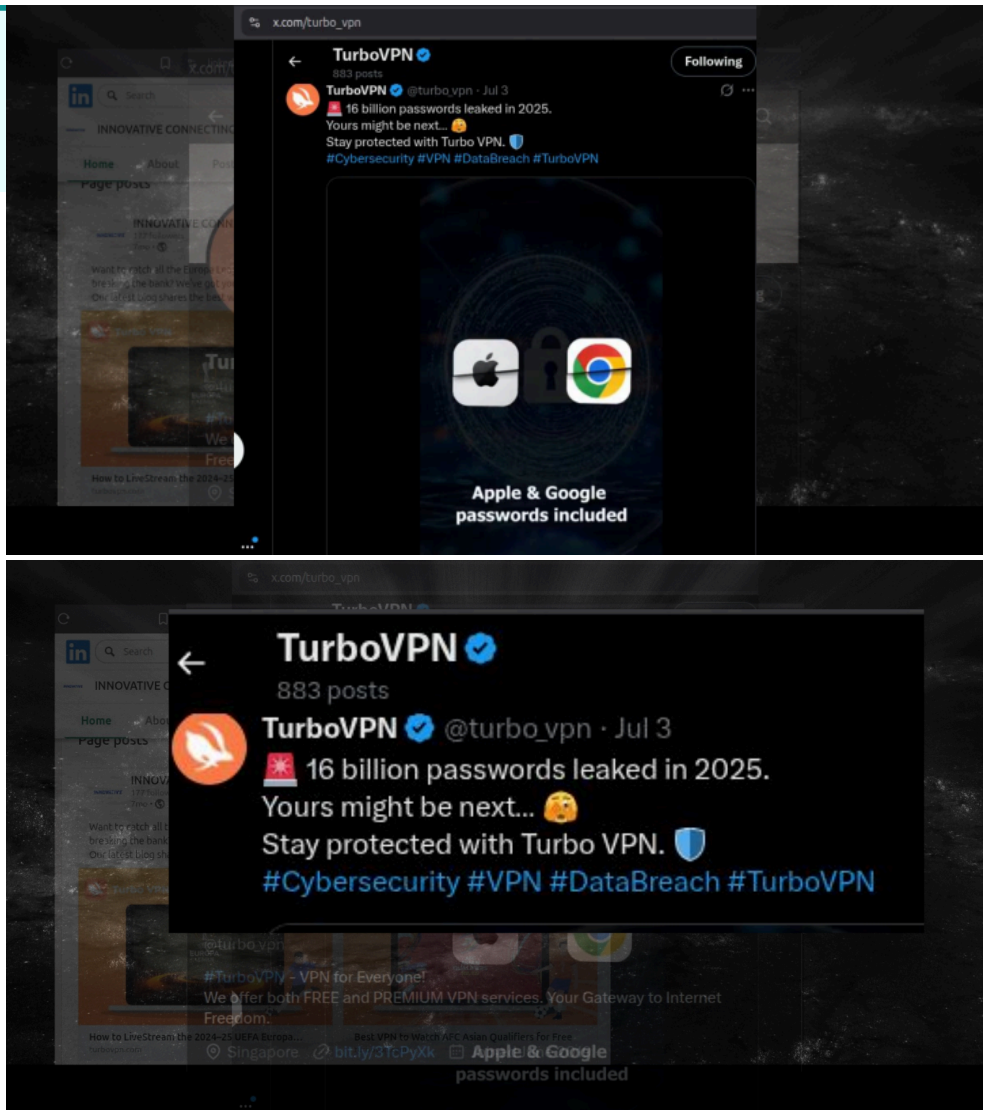


**Figure 14.**
TurboVPN advertising their security after a recent leak of 16 billion passwords.




## Factor Weight

This combined factor has a *low* impact on the application's transparency score. This impact level was determined based on the observation that some providers we found to be operating deceptively, actually actively posted on social media.

## Limitations

There is one key limitation to this factor. Attackers, especially sophisticated, well-resourced ones, are likely to build social media accounts to appear legitimate. By contrast, some providers may choose to have no social media presence to minimize their own exposure and protect their privacy. This is especially true for smaller providers or local providers operating directly in repressive countries where VPNs are illegal. Though we did not investigate smaller VPN providers in this work, future researchers replicating this methodology should consider this when factoring in the social media footprint of VPNs to ascertain a VPN's transparency.

# Results: Social Media Transparency

| VPN App | Does the VPN have contact information? | Does the VPN have Facebook? | Does the VPN have Instagram? | Does the VPN have X? | Does the VPN have Telegram? | Does the VPN use ads for suspicious targeting? |
|---|---|---|---|---|---|---|
| Mullvad | 2 | 1 | 1 | 1 | 0 | 0 |
| TunnelBear | 2 | 1 | 1 | 1 | 1 | 0 |
| Lantern | 2 | 0 | 1 | 1 | 0 | 0 |
| Psiphon | 2 | 0 | 1 | 1 | 0 | 0 |
| Proton VPN | 2 | 1 | 1 | 1 | 1 | 0 |
| Turbo VPN – Secure VPN Proxy | 1 | 1 | 1 | 1 | 1 | 1 |
| Turbo VPN Lite – VPN Proxy | 1 | 1 | 1 | 1 | 1 | 1 |
| VPN Monster – Secure VPN Proxy | 1 | 0 | 0 | 0 | 0 | 0 |
| SnapVPN | 1 | 0 | 0 | 0 | 0 | 0 |
| SuperNet VPN | 1 | 0 | 0 | 0 | 0 | 0 |
| Signal Secure VPN – Robot VPN | 1 | 0 | 0 | 0 | 0 | 0 |
| VPN Proxy Master Pro | 1 | 0 | 0 | 1 | 0 | 0 |
| VPN Proxy Master Lite | 1 | 0 | 0 | 1 | 0 | 0 |
| Hot VPN | 1 | 0 | 0 | 0 | 0 | 0 |
| Secure VPN – Safer Internet | 1 | 0 | 0 | 0 | 0 | 0 |
| Thunder VPN Fast, Safe VPN | 1 | 0 | 0 | 0 | 0 | 0 |
| Lets VPN | 1 | 1 | 1 | 1 | 1 | 0 |
| Astrill VPN | 1 | 1 | 1 | 1 | 0 | 0 |
| Cookie | 1 | 0 | 0 | 0 | 0 | 0 |
| Ciao Proxy Pro | 1 | 0 | 0 | 0 | 0 | 0 |
| Ciao Proxy | 1 | 0 | 0 | 0 | 0 | 0 |
| VPN – Super Unlimited Proxy | 1 | 0 | 0 | 1 | 0 | 0 |
| PureVPN | 1 | 1 | 1 | 1 | 0 | 0 |
| Potato VPN | 1 | 0 | 0 | 1 | 0 | 0 |
| Global VPN | 1 | 0 | 0 | 0 | 0 | 0 |
| Melon VPN | 1 | 0 | 0 | 0 | 0 | 0 |

| VPN App | Does the VPN have contact information? | Does the VPN have Facebook? | Does the VPN have Instagram? | Does the VPN have X? | Does the VPN have Telegram? | Does the VPN use ads for suspicious targeting? |
|---|---|---|---|---|---|---|
| Super Z VPN | 1 | 0 | 0 | 0 | 0 | 0 |
| Touch VPN – Stable & Secure | 1 | 0 | 0 | 0 | 0 | 0 |
| VPN ProMaster–Secure your net | 1 | 1 | 0 | 0 | 0 | 0 |
| 3X VPN – Smooth Browsing | 1 | 1 | 0 | 0 | 0 | 0 |
| VPN Inf | 1 | 1 | 0 | 0 | 0 | 0 |
| Melon VPN – Secure Proxy VPN | 1 | 1 | 0 | 0 | 0 | 0 |

**Score explanation:**

For each Social Media Transparency Subfactor, a VPN Provider can receive a score of 0, 1, or 2.

- 0 = no information
- 1 = some information
- 2 = useful information

Colour coding:

- Red indicates suspicious information on social media.
- White indicates a profile on at least one major social media platform (transparent).
- Black indicates no profile on any major social media platform (anonymous).

# 04. Network/Domain Transparency

## What Is This Factor?

Information for this scoring factor is derived from domain information collected using WHOIS records[23] and dig.[24] Information about a VPN's controlling company may be available in the 'Registrant Org' field. Admin names, emails, phone numbers, and addresses may also be contained within these records, which can be used for further profiling.

## Why Is It Important?

Network/Domain Transparency was selected as a factor, because a VPN provider can make their information available for public analysis. However, it is not uncommon for providers, knowingly or otherwise, to use privacy services when registering their domain names. Such services act as an intermediary between the actual VPN provider and the domain registrar. There are valid reasons why a VPN provider would do this, such as if the provider is trusted or has a good reputation in the community, but nonetheless operates in an environment hostile towards privacy-enhancing tools like VPNs.

## Factor Weight

This combined factor has a *low* impact on the application's CTSS score. An application's score for this factor will have minimal impact on its overall CTSS score. Network/Domain Transparency would not reduce an application's overall score, but could increase the score if present. This minimal impact level was determined based on the amount of information present in the domain records. For example, a provider is not penalized if they use a privacy enhancing service, but it can increase if direct contact information is made available through the domain name system.

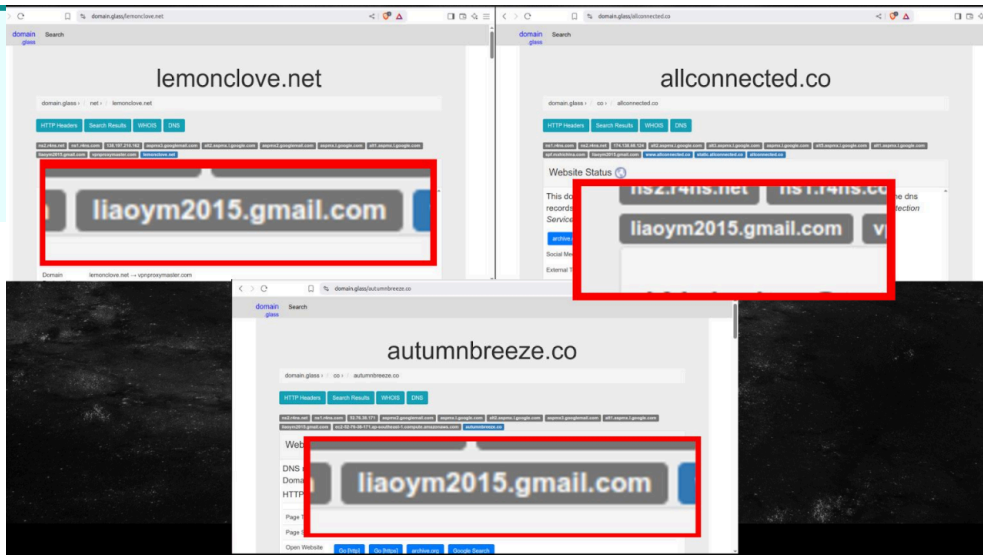
## Limitations

There is one key limitation to this factor. In all but one case, the VPN provider used an anonymizing service, such as Domains By Proxy Incorporated, to obfuscate information about the provider. Just as with social media, there are legitimate reasons why a person or entity would use such an anonymizing service. Attackers could use information on the WHOIS records of a domain, such as the identity of the administrator, for social engineering purposes. Researchers reproducing this methodology should take this into consideration

23. WHOIS records are public databases that provide information about domain name registrations, including who owns a domain, their contact details, the registration date, and other details.
24. dig is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

when evaluating a VPN's transparency. Having said this, in the case of at least three VPN providers — Innovative Connecting, Lemon Clove, and Autumn Breeze — the same email address was found in the DNS SOA records,[25] suggesting they have the same owner. For this reason, it is still worth including the Network/Domain factor when collecting information.

**Figure 15.**
An example of three VPN providers using the same email address, linking Innovative Connecting, Lemon Clove, and Autumn Breeze.




25. DNS 'start of authority' (SOA) records store important information about a domain or zone, such as the email address of the administrator, when the domain was last updated, and how long the server should wait before refreshes. Source: Cloudfare. Date accessed: 2 July 2025.

# Results: Network Domain Transparency

| VPN App | Does the VPN have information on WHOIS? | Does the WHOIS record contain information that cross references with other VPNs? | Does the VPN have a Registrant Org? |
|---|---|---|---|
| Mullvad | 2 | 0 | 2 |
| TunnelBear | 1 | 0 | 0 |
| Lantern | 2 | 0 | 2 |
| Psiphon | 0 | 0 | 0 |
| Proton VPN | 2 | 0 | 2 |
| Turbo VPN – Secure VPN Proxy | 0 | 2 | 0 |
| Turbo VPN Lite – VPN Proxy | 0 | 2 | 0 |
| VPN Monster – Secure VPN Proxy | 0 | 2 | 0 |
| SnapVPN | 0 | 2 | 0 |
| SuperNet VPN | 0 | 2 | 0 |
| Signal Secure VPN – Robot VPN | 0 | 2 | 0 |
| VPN Proxy Master Pro | 0 | 2 | 0 |
| VPN Proxy Master Lite | 0 | 2 | 0 |
| Hot VPN | 0 | 0 | 0 |
| Secure VPN – Safer Internet | 0 | 0 | 0 |
| Thunder VPN Fast, Safe VPN | 0 | 0 | 0 |
| Lets VPN | 0 | 0 | 0 |
| Astrill VPN | 0 | 0 | 0 |
| Cookie | 0 | 0 | 0 |
| Ciao Proxy Pro | 0 | 0 | 0 |
| Ciao Proxy | 0 | 0 | 0 |
| VPN – Super Unlimited Proxy | 0 | 0 | 0 |
| PureVPN | 0 | 0 | 0 |
| Potato VPN | 0 | 0 | 0 |
| Global VPN | 0 | 0 | 0 |
| Melon VPN | 0 | 0 | 0 |
| Super Z VPN | 0 | 0 | 0 |

| VPN App | Does the VPN have information on WHOIS? | Does the WHOIS record contain information that cross references with other VPNs? | Does the VPN have a Registrant Org? |
|---|---|---|---|
| Touch VPN - Stable & Secure | 0 | 0 | 0 |
| VPN ProMaster-Secure your net | 0 | 0 | 0 |
| 3X VPN - Smooth Browsing | 0 | 0 | 0 |
| VPN Inf | 0 | 0 | 0 |
| Melon VPN - Secure Proxy VPN | 0 | 0 | 0 |

**Score explanation:**

For each Network/Domain Transparency subfactor, a VPN Provider can receive a score of 0, 1, or 2.

- 0 = no information.
- 1 = some information.
- 2 = useful information.

Color coding:

- Red indicates suspicious information present in domain records.
- White indicates more transparent operations.
- Dark indicates more anonymous operations.

# 05. Manual Analysis

## What Is This Factor?

Manual analysis is the process whereby a human analyst develops an understanding about a program. This form of analysis is used during a security audit for applications. It involves identifying function names, functionality (how the app behaves), and interesting strings (such as domain names, email addresses, and passwords). The goal is often to either identify security weaknesses, or verify that an application is safe to use.

Information for this combined scoring factor is derived from static and dynamic analyses. These were performed on the client code and from tests conducted against the VPN server when possible. Static analysis provides insight about data collection practices, whether the code of a VPN application is shared by multiple VPN providers, identifiers like email addresses and API keys present in the source code, and hard-code credentials stored in the application. Dynamic analysis provides information about what servers the application talks to, what information it sends or receives from other servers, whether its communication practices are secure, and to which VPN servers it can connect.

## Why Is It Important?

Certain information about the VPN provider can be gleaned from such analyses that may not be obvious from conventional OSINT search techniques. For example, the only way to determine whether different VPN providers share servers is to try connecting to them. Furthermore, the only way to determine if the application is using proper encryption during communication is with dynamic testing. Manual analysis of an application downloaded onto a device is effectively the ground truth about the communication practices of the application and whether it is secure or not.

## Factor Weight

This combined factor has a *high* impact on the application's transparency score. This impact was determined based on the information gleaned during analysis. Specifically, we identified several instances where multiple VPN providers, which on the surface appear to be independent organizations, not only shared server infrastructure, but shared the exact same VPN servers, and used the exact same credentials for VPN connections.

## Limitations

The key limitation to this methodology is that we cannot guarantee that we have explored every possible code path within the code. There may be code paths that lead to privacy and security issues that only occur in rare circumstances, or under conditions that we did not identify, and hence, did not explore.

## Ethical Considerations

Some VPN providers have terms of service, end-user licenses, or acceptable user policies which explicitly forbid reverse engineering of their application. For this study, we are not attempting to profit off of any code that is reverse-engineered, gain access to private user data, or compromise the security of provider services. We are also not attempting to access systems not under direct control of the VPN provider, send unreasonably high volumes of traffic to or through the VPN server,[26] or access VPN services in ways that a normal VPN client application would not use when accessing the VPN server. Furthermore, any dynamic analysis conducted at this point in our investigation was motivated by the existence of other strong indicators that the operator is operating deceptively. Hence, it is in the public interest that we determine whether serious privacy and security violations are present.

26. Our data rates are on the order of kilobytes to megabytes, at most.

# Results: Manual Analysis

| VPN App | APK Indicators |
|---|---|
| Mullvad | |
| TunnelBear | |
| Lantern | |
| Psiphon | |
| Proton VPN | |
| Turbo VPN – Secure VPN Proxy | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| Turbo VPN Lite – VPN Proxy | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| VPN Monster – Secure VPN Proxy | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| SnapVPN | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| Signal Secure VPN – Robot VPN | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| SuperNet VPN | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| VPN Proxy Master Pro | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| VPN Proxy Master Lite | The binary code reference VPN Monster, SnapVPN, Secure Signal VPN – Robot VPN, SuperNet VPN, VPN Proxy Master |
| Hot VPN | |
| Secure VPN – Safer Internet | |
| Thunder VPN Fast, Safe VPN | |
| Lets VPN | |
| Astrill VPN | |
| Cookie | |
| Ciao Proxy Pro | |
| Ciao Proxy | |
| VPN – Super Unlimited Proxy | |
| PureVPN | |
| Potato VPN | |

| VPN App | APK Indicators |
|---|---|
| Global VPN | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| Melon VPN | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| Super Z VPN | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| Touch VPN – Stable & Secure | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| VPN ProMaster–Secure your net | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| 3X VPN – Smooth Browsing | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| VPN Inf | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |
| Melon VPN – Secure Proxy VPN | The binary References Melon VPN, Super Z VPN, Touch VPN, VPN ProMaster 3X VPN, VPN Inf, and Melon VPN |

**Score explanation:**

- Green indicates good/positive findings.
- Red indicates an explicit connection between two or more VPN providers.
- No color indicates no indicators were identified.

# V

# Transparency Score Results

Of the 21 VPN providers assessed for this report, five were determined to be transparent to users. Eight were determined to be non-transparent, due to lack of information available about the organizations running them. Finally, eight were confirmed to be operating their VPNs in ways that should be highly concerning from both a transparency and security perspective.

The eight VPN providers that we confirmed are operating their services in ways that should be highly concerning from both a transparency and security perspective, are grouped into two clusters based on their connections to each other. Both clusters have suspicious indicators across one or more of the scoring factors. The following sections cover the specific factors most relevant to our determination: Business and Manual Analysis. The first cluster of VPN providers is Innovative Connecting, Autumn Breeze, and Lemon Clove. The second provider cluster is Matrix Mobile, Wildlook Tech, Yolo Technology, Hong Kong Silence Technology and ForeRaya Technologies.

# CTSS Result

| Provider Name | Provider Name | VPN App |
|---|---|---|
| Operates more transparently. No concerning findings identified. | Mullvad | Mullvad |
| | TunnelBear | TunnelBear |
| | Lantern | Lantern |
| | Psiphon | Psiphon |
| | ProtonVPN | Proton VPN |
| Operates more anonymously. Potentially concerning, but no definitive findings. | HotVPN | HotVPN |
| | LetsVPN | LetsVPN |
| | Astrill VPN | Astrill VPN |
| | CookieDevs | Cookie |
| | | Ciao Proxy Pro |
| | | Ciao Proxy |
| | VPN Super Inc | VPN – Super Unlimited Proxy |
| | PureVPN | PureVPN |
| | Potato VPN | Potato VPN |
| Concerning and suspicious findings (users should avoid). | Innovative Connecting | Turbo VPN – Secure VPN Proxy |
| | | Turbo VPN Lite – VPN Proxy |
| | | VPN Monster – Secure VPN Prox |
| | Autumn Breeze | SnapVPN |
| | | Signal Secure VPN – Robot VPN |
| | | SuperNet VPN |
| | Lemon Clove | VPN Proxy Master Pro |
| | | VPN Proxy Master Lite |
| | Matrix Mobile | Global VPN |
| | | Melon VPN |
| | ForeRaya Technologies | Super Z VPN |
| | Hong Kong Silence Technology | Touch VPN – Stable & Secure |
| | Yolo Mobile Technology | VPN ProMaster – Secure your net |
| | | 3X VPN – Smooth Browsing |
| | Wild Tech | VPN Inf |
| | | Melon VPN – Secure Proxy VPN |

**Results explanation:**

- White indicates transparent operation.
- Dark indicates anonymous operation.
- Red indicates concerning privacy and security findings.

# Innovative Connecting, Autumn Breeze, Lemon Clove

## Business Level

As previously reported by VPNpro,[27] Tech Transparency Project (TTP),[28] and others, Innovative Connecting PTE. Limited is associated with multiple other VPN providers, including Autumn Breeze and Lemon Clove. VPN pro linked these groups together when they discovered similar text in the privacy policies of these VPN providers. We replicated these findings to confirm that these different VPN providers are actually operated by the same organization. Autumn Breeze's Signal Secure - Robot VPN's privacy policy explicitly states that Innovative Connecting PTE. Limited is the representative organization, but the privacy policy linked to its website is different.

**Figure 16.**
Autumn Breeze's Signal Secure - Robot VPN privacy policy referencing Innovative Connecting.

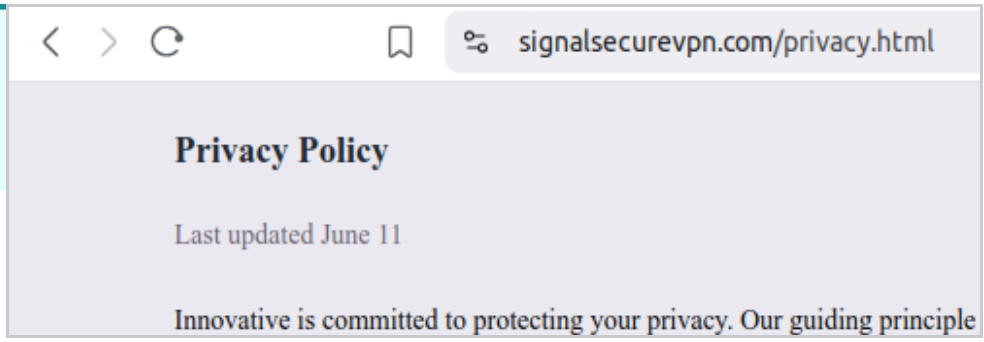
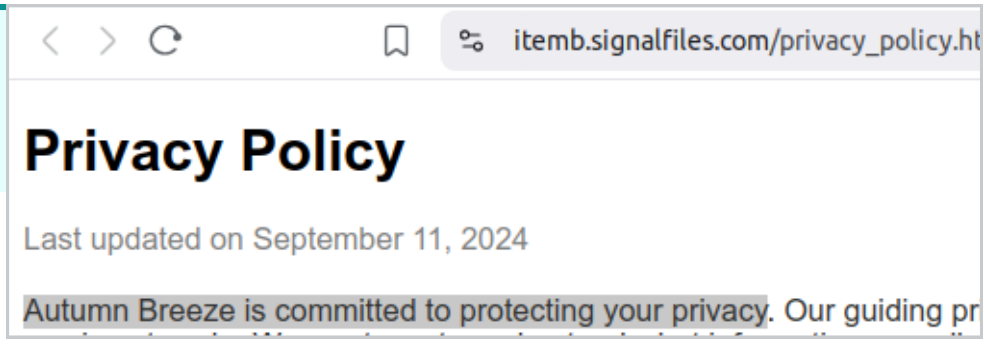



**Figure 17.**
Autumn Breeze's privacy policy linked on their Google Play app page.




We next used the names provided by these developers as search terms on OpenCorporates. Our findings are consistent with that of other researchers, that these VPNs' copyright filings indicate they are actually controlled by a Chinese national, and hence subject to Chinese information control laws.

27. Vėsa, D. (2024) 'Who owns your VPN? 105 VPNs run by just 24 companies.' VPNpro. Available here: https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/. Date accessed: 6 June 2025.
28. Tech Transparency Project (2025) 'Apple offers apps with ties to Chinese military.' Tech Transparency Project. Available here: https://www.techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military. Date accessed: 6 June 2025.

**Figure 18.**
OpenCorporates' records for Innovative Connecting, Autumn Breeze, and Lemon Clove.

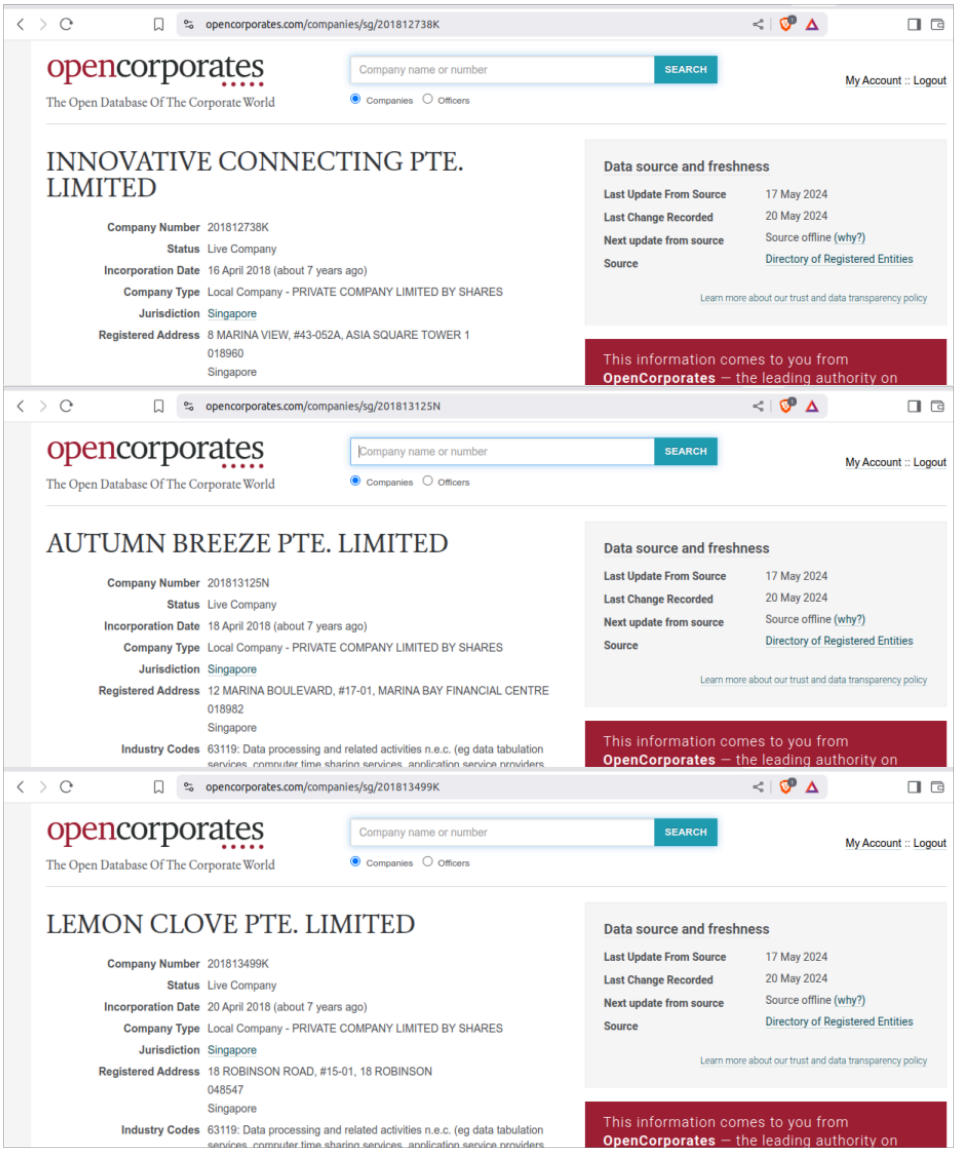
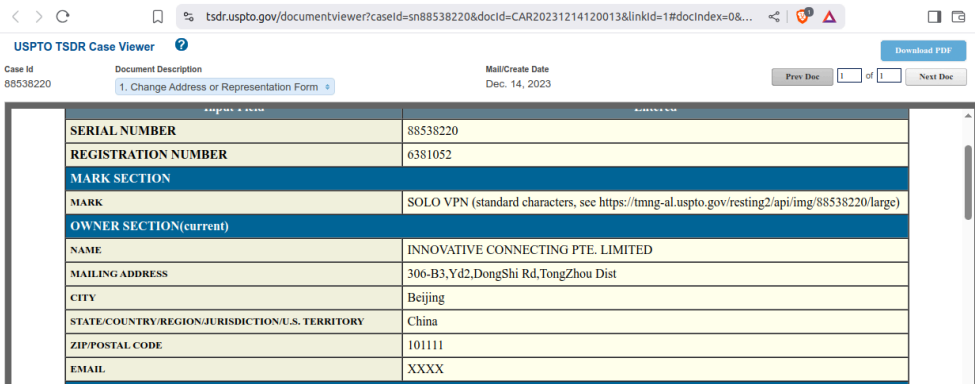



**Figure 19.**
Copyright filings showing that Innovative Connecting's controlling entity lives in Beijing.



Unfortunately, the connection between Innovative Connecting, Lemon Clove, and Autumn Breeze is not as convincing as it could be. For example, unrelated VPN providers could simply copy and paste the text of a competitor's privacy policy for their own. Additionally, unrelated VPN providers may have hired the same third-party developer for their websites, and that developer may have copy-pasted this information. For example, Fruit Security Studios (Yolo Mobile Technology Limited), which develops 3X VPN, also has a connection to China based on its Google Play profile, and members on LinkedIn (重庆哈希智能科技有限公司). Its privacy policy also references Innovative Connecting.

**Figure 20.**
Fruit Security Studios' 3X VPN privacy policy linked from its Google Play account.

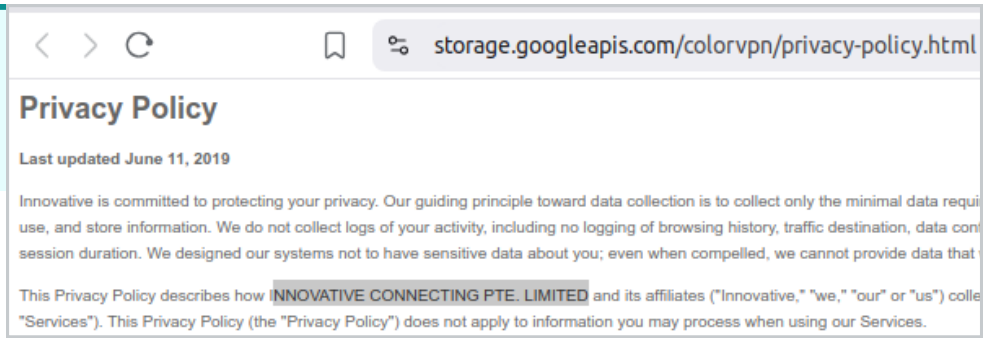
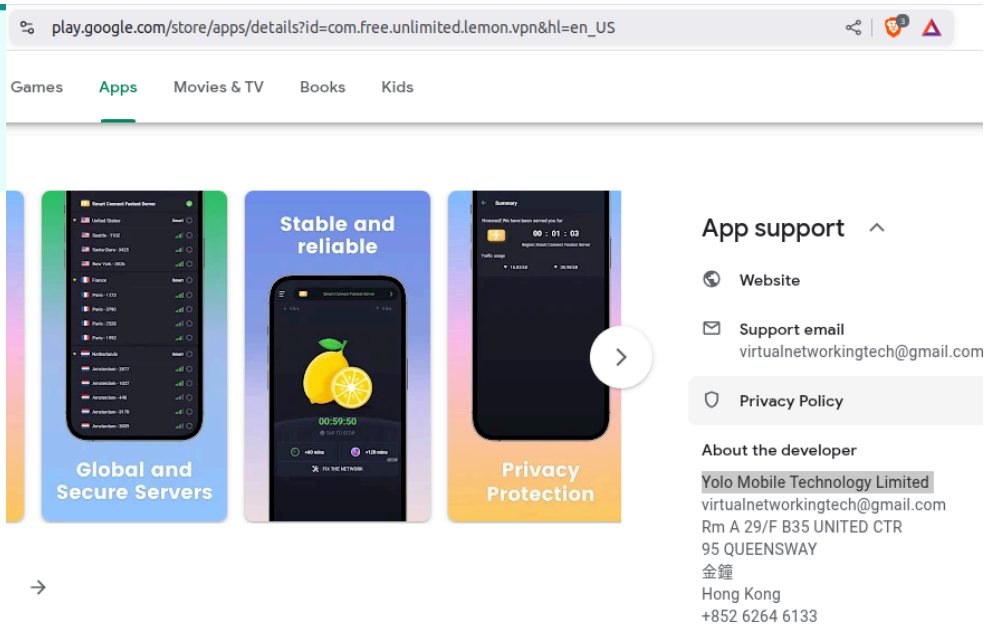



**Figure 21.**
Fruit Security Studios' 3X VPN application references Hong Kong as the developer's origin.




Multiple other VPN providers also reference Innovative Connecting PTE. Limited in their privacy policy in similar ways, but we found through manual analysis that the VPNs for Innovative Connecting, Autumn Breeze, and Lemon Clove, specifically, are substantially more deeply connected.

## Manual Analysis

After identifying the suspicious characteristics for these providers, we downloaded each application onto a Google Pixel 7a device. At the code level, we identified at least eight VPNs associated with these three companies. We found this by applying the Linux "strings"[29] command to files in the shared libraries. The specific file containing this information is "libopvpnutils.so." Through our manual analysis we were able to identify a number of key security concerns.

**Figure 22.**
Multiple VPNs from Innovative Connecting, Autumn Breeze, and Lemon Clove referenced in a common shared library, libopvpnutil.so.


Each provider's application supports Internet Protocol Security (IPsec)[30] and Shadowsocks[31] typically. When the application starts, it decides whether to dynamically download a configuration file from an API endpoint or use a pre-installed version.

In the case of IPsec, one strange behavior we identified was that even when the API seemed operable, the application opted to use the pre-installed "offline" configuration stored in the "assets" directory of the application. When connecting to either IPSec or Shadowsocks in this fashion, the application called a function in native code to generate an Advanced Encryption Standard (AES) key to decrypt a VPN public key (for IPsec) or a configuration file (for Shadowsocks).

One reason for this might be to increase user security by preventing a security analyst from trivially retrieving these credentials. Unfortunately, this does not provide much security, as we were able to extract both the decryption keys for IPsec and Shadowsocks, as well as extract the configuration files and digital certificates directly using Frida.[32] The fact that these credentials are hard-coded[33] has serious security implications for the users of these VPN applications. Most concerning is that these credentials are shared by all of the 300 million-plus users who have downloaded these eight VPNs.

29. "strings" is a utility function that searches for American Standard Code for Information Interchange (ASCII)/printable characters in a file. During static analysis, strings is often used to identify file names, user names, email addresses, passwords, or other useful information.
30. Internet Protocol Security (IPSec) is a suite of protocols and services that provide security for IP networks.
31. Shadowsocks is an open source proxy project designed to bypass internet censorship and restrictions.
32. Frida is a toolkit used by developers and security researchers to conduct tasks such as reverse engineering, security research, and penetration testing.

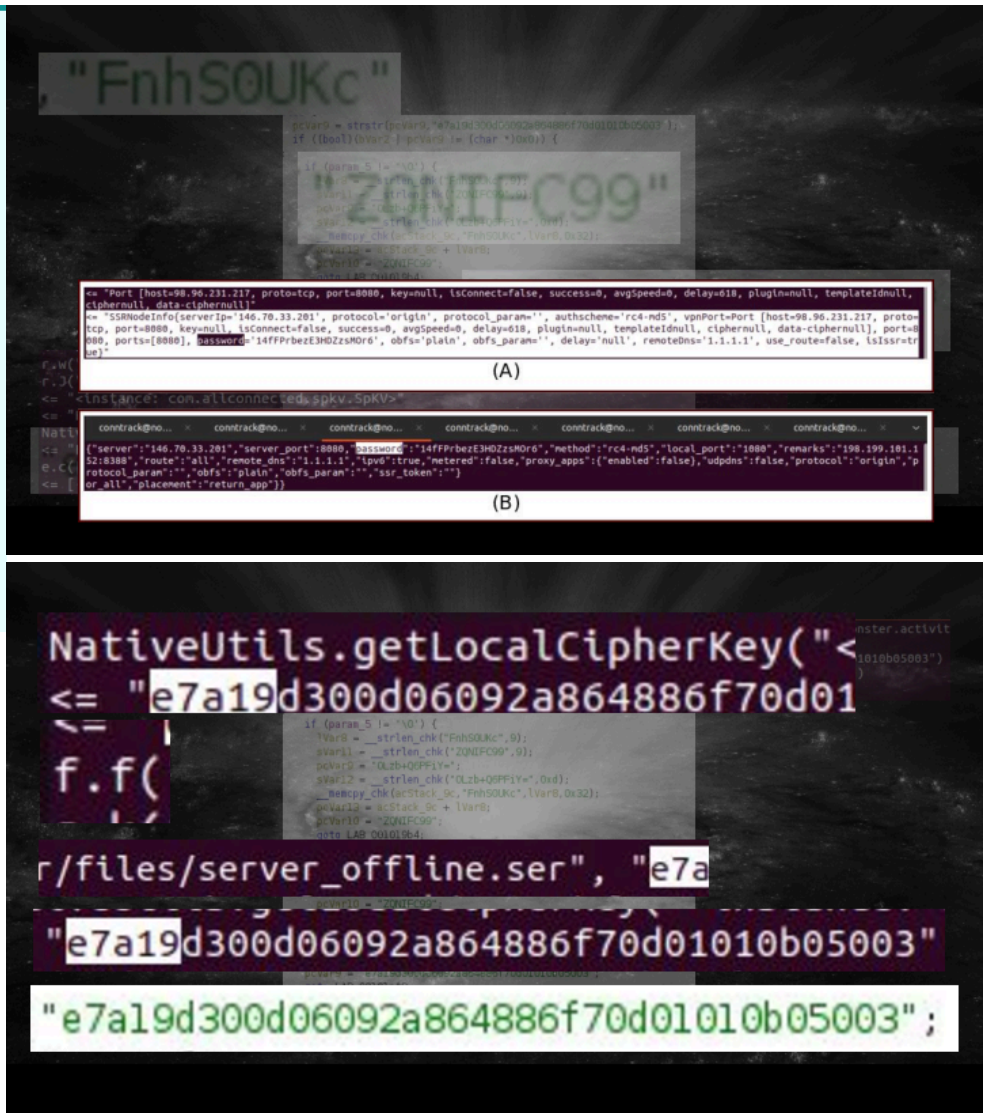



**Figure 23.**
VPN Monster (from provider Innovative Connecting) contains a hard-coded password in its embedded Shadowsocks configuration file, as well as deprecated rc4-md5 stream cipher encryption method.

Rc4-md5 is an insecure stream cipher offered by Shadowsocks for encrypting communications. The stream ciphers of Shadowsocks are not authenticated which means an attacker can modify previously sent communications from a legitimate client and cause the Shadowsocks server to decrypt the communications for the attacker.

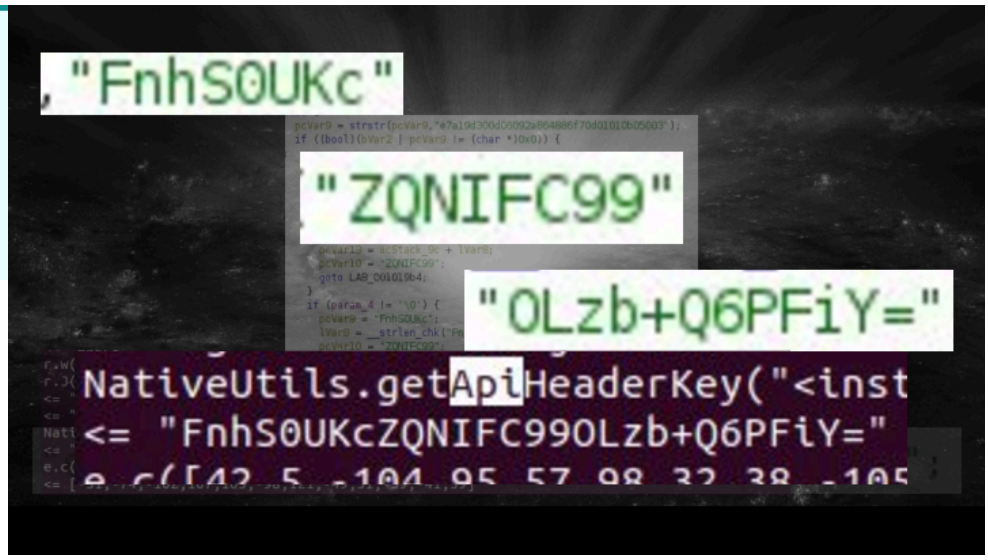
When these VPNs use Shadowsocks, the configuration file contains multiple security issues. First, each app offers only insecure and deprecated stream ciphers when connecting via Shadowsocks. We found that the stream ciphers are implemented insecurely, such that an attacker can decrypt packets sent by users.[34] This exposes all 300 million-plus users to attack, because their "secure" tunnel is no longer secure.

Second, and most concerning, is the fact that all 300 million-plus users share the same password. We confirmed this by downloading the apps using different devices and in different locations, and then compared the SHA256 hash of these files. Hash functions, such as SHA256, are cryptographic functions that convert a long string of bytes to a fixed length. They are often used to compare files for changes. Files that are the same have the same SHA256 hash, whereas different files have a different SHA256 hash. They are identical, implying that the embedded configuration files are also identical. This is a major problem, because an attacker who knows the password can trivially decrypt the VPN's encryption.

34. GitHub user, wkrp (2020) Decryption vulnerability in Shadowsocks stream ciphers #24. GitHub. Available here: https://github.com/net4people/bbs/issues/24. Date accessed: 6 June 2025.

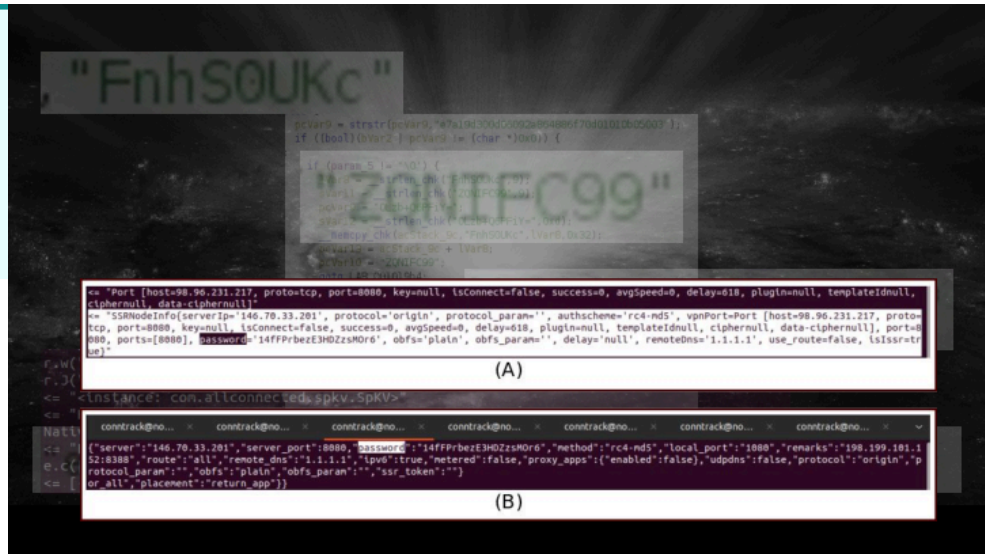
**Figure 24.**

The API Header key (green text) is built dynamically and used when downloading configuration files. Frida was used to identify the NativeUtils.getApiHeaderKey function call.




**Figures 25.**

Frida trace (A) showing the hardcoded Shadowsocks key **(14FPrbezE3HDZzsMOr6)** used to connect to the Shadowsocks server. Image B is the output of the fridump tool.



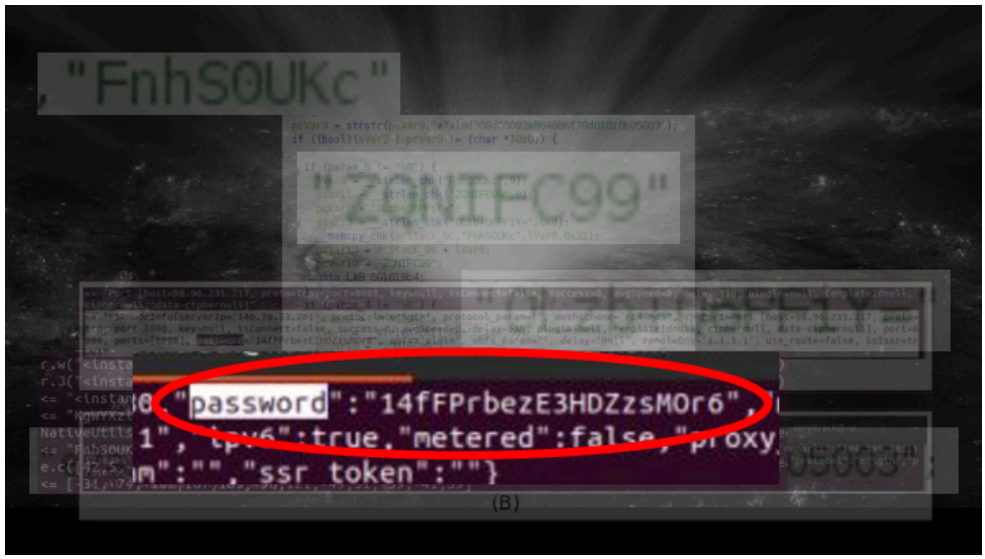



**Figure 26.**

Frida trace showing the encrypted Shadowsocks configuration file embedded in the application being decrypted with key (**FnHS0UKcZQNIFC99atzc+76PabTH**).

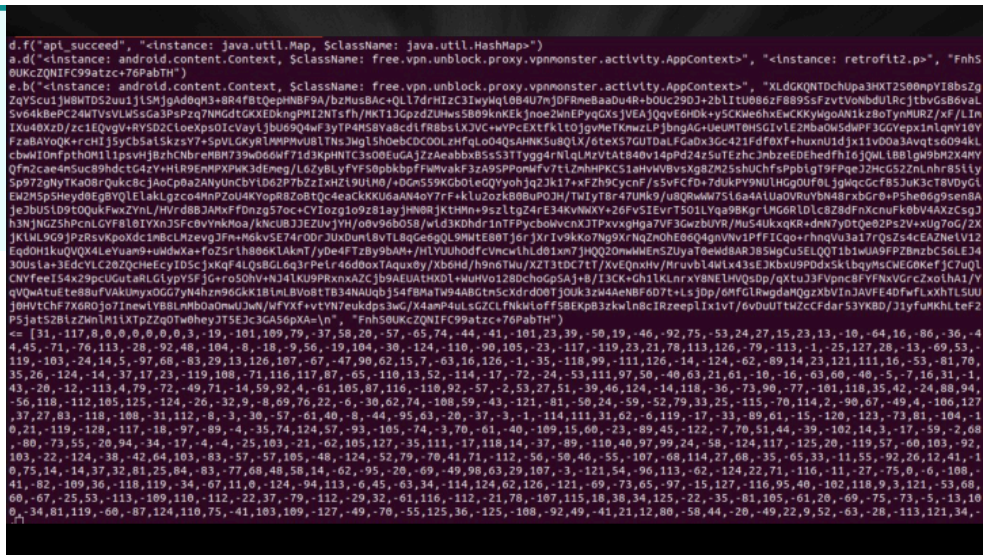



**Figure 27.**

Hard-coded keys in VPN Proxy Master enable a network eavesdropper to decrypt traffic. (Top: encrypted data. Bottom: encircled in red is the decrypted version of the same data).


Third, given that the apps all share the same credentials, as well as privacy policy text, it seemed possible that these apps also share infrastructure. To test this, we collected the IP addresses of the VPN servers offered by these apps. We then used the Shadowsocks credentials to connect to each of the VPN servers. Testing confirmed that the providers do, indeed, share infrastructure. Shared infrastructure presents two possibilities. It is possible that one provider is free-loading off of another provider's service. In this case, it isn't really free-loading, since ultimately, they are controlled by the same organization. At the same time, it provides compelling evidence that the VPN providers are directly connected with each other and complements the findings from VPNpro and TTP. While there is a plausible argument for why these providers might not be linked when using the privacy policy connections, there is not a good reason to justify why seemingly different VPN providers would share substantially similar code-bases, much less VPN server infrastructure, or worse, hard-coded credentials that an attacker can use to completely remove the tunnel's encryption.

In addition to the issues associated with using Shadowsocks, we also identified other concerning behaviors. We found that the VPNs are also susceptible to blind-in/on-path attacks.[35] Such attacks permit an attacker to infer which end-servers and websites a user is communicating with, even when they use a VPN. Furthermore, in the case of IPsec, it is also possible that users are susceptible to connection injection attacks[36] via the server-side version of the blind-in/on-path attacks.

In the case of VPN Proxy Master, we found that it does not use certificate pinning.[37] This made it possible for us to use the MITM proxy[38] to identify the services and API endpoints with which it was communicating. Specifically, we found that it makes requests to "https://ip-api.com." The value returned was the postal code associated with the client's public IP address. This value was then uploaded to a Firebase[39] endpoint.

Finally, all the apps from Innovative Connecting, Autumn Breeze, and Lemon Clove also have code for Huawei analytics, similar to Firebase, for monetization. This is especially concerning in the case of SnapVPN, SuperNetVPN, RobotVPN, VPNMonster, and TurboVPN, because their AndroidManifest.xml files do not request location permission. The privacy policy for all of the apps also states explicitly that they do not collect geographic information of their users, but they all reach out to this API endpoint.

35. Tolley, W., Kujath, B., Khan, M., Vallina-Rodriguez, N. and Crandall, J. (2021) 'Blind in/on-path attacks and applications to VPNs.' Usinex, The Advanced Computing Systems Association. 3129-3146. Available here: https://www.usenix.org/system/files/sec21-tolley.pdf. Date accessed: 6 June 2025.
36. Injection attacks are a type of attack where an attacker exploits vulnerabilities in an application by inserting malicious code or data into a system, causing it to execute unintended commands or access sensitive information.
37. Certificate pinning is a security technique where an application or browser is configured to only accept connections from servers using a specific certificate or public key.
38. The 'man-in-the-middle' (MITM) proxy is a tool that can be used to intercept and decrypt TLS connections.
39. Firebase is part of an advertising platform used by mobile developers for analytics and monetization. Information about a user, such as their name, email or location, are often uploaded to Firebase for targeted advertising.

This cluster of VPN providers has over 300 million downloads collectively on Google Play Store alone. They all claim to offer privacy and security, yet the fact that they offer Shadowsocks is misleading to users because Shadowsocks was not designed for confidentiality. The apps contain hard-coded Shadowsocks credentials that are easy to extract. An attacker could use the credentials to remove the encryption between the VPN client and server for this family of providers. Additionally, they all also claim they do not collect user location information but in fact do, further misleading users.

# MATRIX MOBILE PTD. LTD, ForeRaya Technologies PTE LTD, WILDLOOK TECH PTE. LTD., Hong Kong Silence Technology, Yolo Mobile Technology Limited

## Business Level

According to their Google Play profiles, Matrix Mobile. and Wildlook Tech operate out of Singapore. By contrast, ForeRaya Technologies, Hong Kong Silence Technology and Yolo Mobile Technology operate out of Hong Kong. Only MATRIX MOBILE PTE LTD and Wildlook Tech had profiles on OpenCorporates.[40]

This group of developers collectively operate eight separate VPN products and have more than 400 million downloads on the Google Play Store. Similar to the previous developers, we were able to connect all eight by running "strings" on a shared library that contained the APK names of eight APKs from these providers. Specifically, in libcore.so.

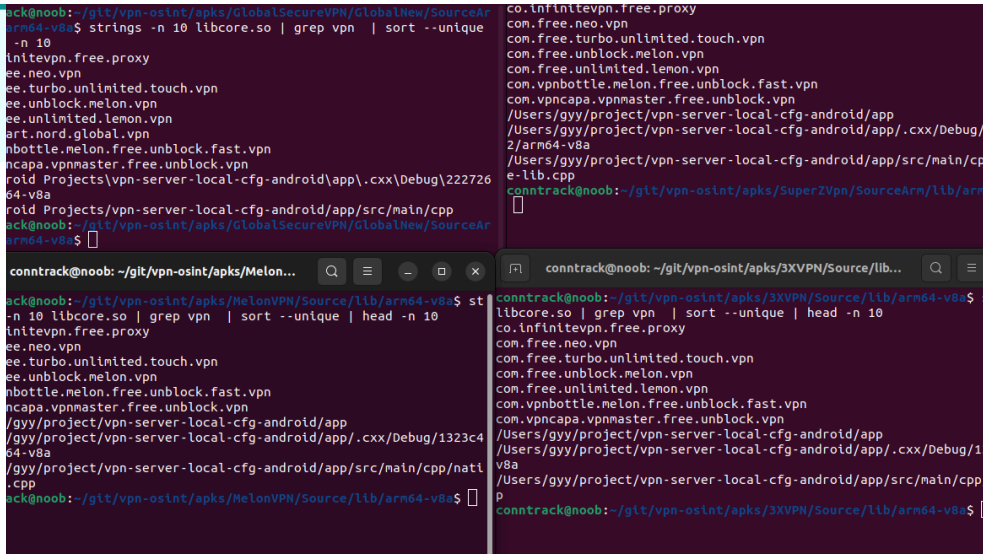



**Figure 28.**
APK file names for the eight VPN apps in Family B.

## Manual Analysis

Our manual analysis surfaced three key concerns. Similar to the first cluster, each of these VPN apps offer Shadowsocks as the tunneling protocol and share credentials for all users of the service. Like Innovative Connecting, Autumn Breeze, and Lemon Clove, these credentials are hard-coded and obfuscated with the 256-bit Advanced Encryption Standard. These credentials were found in the file lib/arm64-v8a/libcore.so. This library is unique to this cluster of providers and serves both as a mechanism for clustering the providers and differentiating them from other providers analyzed.

40. We did not find documentation linking these companies to Qihoo 360, but given the fact that their privacy policies also reference Innovative Connecting PTE. Limited, their shared objects reference VPN applications of other "distinct" providers, and some of the providers in this cluster are run by Chinese nationals, it seems plausible that they are related. Furthermore, both clusters of VPN providers share libraries (libopvpnutil.so for Innovative Connective, Autumn Breeze, and Lemon Clove PTE. Limited; libcore.so for MATRIX MOBILE et al.) that contain a list of VPN apps that are used to determine the specific set of credentials to use.

Furthermore, the built-in Shadowsocks configuration files contain connection parameters for 33 servers. Each server has a total of approximately 19 open ports. While each app appears to connect to one of these ports when establishing the Shadowsocks tunnel, we only saw the VPNs establish connections to a subset of them. It was surprising to see that all of the servers are hosted by a single provider, GTHost (GlobalTeleHost Corp.), a Canadian-based hosting company. Generally, VPN providers will configure their servers across a broad range of cloud providers to increase their network presence. Deploying VPN servers to a single hosting provider introduces a single point of failure; if censors block the hosting service then all of the VPN provider's servers would be wiped out.

Lastly, the apps use one of 14 distinct passwords that appear to be assigned to one of the ports per server. Fortunately, these VPNs use aes-256-gcm as the Shadowsocks encryption method, so they are not vulnerable to the decryption oracle attack.[41] However, Shadowsocks does not have perfect forward secrecy,[42] and the use of symmetric encryption makes it possible for a network attacker to decrypt the client traffic using the hard-coded credentials—or credentials that an attacker can retrieve by observing API calls—since the credentials are shared by all users of the service. The above findings, coupled with the fact that the apps collectively service over 400 million people who share these credentials, create serious privacy concerns for those users.

Unlike the previous cluster of providers, no one that we are aware of has previously identified transparency or security issues with this cluster of providers and is one of the main contributions and new findings in this report. While we could not definitively link these providers to Qihoo 360, some of the providers explicitly state they are operated out of Hong Kong. It is therefore reasonable to conclude that since all of these providers share code and VPN server infrastructure, they are likely operated by a single Chinese national.

**This group of previously unexamined providers have several deceptive practices and security issues, and based on the evidence, it is reasonable to conclude that they are all operated by a single Chinese national—and subject to Chinese information control laws.**

41. The aes-256-gcm encryption method of Shadowsocks adds a checksum to the protocol format which allows the receiver to authenticate the sender and prevents an attacker from manipulating communications, thus preventing the decryption oracle attack.
42. "Perfect forward secrecy" is a property of secure communication protocols in which compromise of long-term keys (the Shadowsocks password) does not compromise past session keys and passed communications. Because Shadowsocks doesn't have this property, an attacker can easily attain the passwords and compromise user communications.

**Figure 29.**

Raw output of strings command from memory dump of Global VPN (from provider Matrix Mobile) showing the Shadowsocks configuration used by these providers. The passwords are shared by the providers and can be used by a network attacker to compromise the confidentiality of the VPN tunnel.


esc":"Smart Connect","group_id":"auto","iso_code":"AUTO","normal_show_cnt":0,"responseSource":null,"serverItemType":2,"servers":[
mit":1000000,"bypass":false,"city":"Atlanta","dirty":false,"disconnect_time":0,"gip":"US","group_id":"us","server":"38.22.17.163"
vidual":"","ipv6":false,"is_auto":true,"is_vip":false,"iso_code":"US","isp":"gthost","limit_rate":0,"metered":false,"method":"aes
de":"tcp_and_udp","name":"Atlanta - 380","password":"pKEW8JPByTVTLtM","plugin":null,"proxyApps":false,"remoteDns":"dns.google","s
43,"route":"all","rx":0,"score":0,"ss_url":"","subscription":"UserConfigured","tx":0,"udpFallback":null,"udpdns":true,"userOrder"
5},{"app_conn_limit":1000000,"bypass":false,"city":"Atlanta","dirty":false,"disconnect_time":0,"gip":"US","group_id":"us","server
.191","id":0,"individual":"","ipv6":false,"is_auto":true,"is_vip":false,"iso_code":"US","isp":"gthost","limit_rate":0,"metered":f
:"aes-256-gcm","mode":"tcp_and_udp","name":"Atlanta - 139","password":"g5MeD6Ft3CWlJId","plugin":null,"proxyApps":false,"remoteDn
e","server_port":5004,"route":"all","rx":0,"score":0,"ss_url":"","subscription":"UserConfigured","tx":0,"udpFallback":null,"udpdn
Order":0,"weight":75},{"app_conn_limit":1000000,"bypass":false,"city":"Seattle","dirty":false,"disconnect_time":0,"gip":"US","gro
server":"38.89.70.195","id":0,"individual":"","ipv6":false,"is_auto":true,"is_vip":false,"iso_code":"US","isp":"gthost","limit_ra
d":false,"method":"aes-256-gcm","mode":"tcp_and_udp","name":"Seattle - 867","password":"cdBIDV42DCwnfIN","plugin":null,"proxyApps
teDns":"dns.google","server_port":8118,"route":"all","rx":0,"score":0,"ss_url":"","subscription":"UserConfigured","tx":0,"udpFall
dpdns":true,"userOrder":0,"weight":75},{"app_conn_limit":1000000,"bypass":false,"city":"Atlanta","dirty":false,"disconnect_time":
"group_id":"us","server":"172.111.36.221","id":0,"individual":"","ipv6":false,"is_auto":true,"is_vip":false,"iso_code":"US","isp"
mit_rate":0,"metered":false,"method":"aes-256-gcm","mode":"tcp_and_udp","name":"Atlanta - 259","password":"XKFKl2rULjIp74","plugi
yApps":false,"remoteDns":"dns.google","server_port":8008,"route":"all","rx":0,"score":0,"ss_url":"","subscription":"UserConfigure
pFallback":null,"udpdns":true,"userOrder":0,"weight":75},{"app_conn_limit":1000000,"bypass":false,"city":"Ashburn","dirty":false,
ime":0,"gip":"US","group_id":"us","server":"142.202.49.92","id":0,"individual":"","ipv6":false,"is_auto":true,"is_vip":false,"iso
isp":"gthost","limit_rate":0,"metered":false,"method":"aes-256-gcm","mode":"tcp_and_udp","name":"Ashburn - 82","password":"TEzjfA
lugin":null,"proxyApps":false,"remoteDns":"dns.google","server_port":6679,"route":"all","rx":0,"score":0,"ss_url":"","subscriptio
gured","tx":0,"udpFallback":null,"udpdns":true,"userOrder":0,"weight":75},{"app_conn_limit":1000000,"bypass":false,"city":"Ashbur
lse,"disconnect_time":0,"gip":"US","group_id":"us","server":"38.107.226.100","id":0,"individual":"","ipv6":false,"is_auto":true,"
,"iso_code":"US","isp":"gthost","limit_rate":0,"metered":false,"method":"aes-256-gcm","mode":"tcp_and_udp","name":"Ashburn - 1017
"pKEW8JPByTVTLtM","plugin":null,"proxyApps":false,"remoteDns":"dns.google","server_port":4444,"route":"all","rx":0,"score":0,"ss_
cription":"UserConfigured","tx":0,"udpFallback":null,"udpdns":true,"userOrder":0,"weight":74},{"app_conn_limit":1000000,"bypass":
"Chicago","dirty":false,"disconnect_time":0,"gip":"US","group_id":"us","server":"38.128.66.182","id":0,"individual":"","ipv6":fal
true,"is_vip":false,"iso_code":"US","isp":"gthost","limit_rate":0,"metered":false,"method":"aes-256-gcm","mode":"tcp_and_udp","na
- 117","password":"XKFKl2rULjIp74","plugin":null,"proxyApps":false,"remoteDns":"dns.google","server_port":8008,"route":"all","rx"
"ss_url":"","subscription":"UserConfigured","tx":0,"udpFallback":null,"udpdns":true,"userOrder":0,"weight":74},{"app_conn_limit":
ss":false,"city":"Atlanta","dirty":false,"disconnect_time":0,"gip":"US","group_id":"us","server":"172.111.36.212","id":0,"individ
":false,"is_auto":true,"is_vip":false,"iso_code":"US","isp":"gthost","limit_rate":0,"metered":false,"method":"aes-256-gcm","mode"
","name":"Atlanta - 845","password":"cdBIDV42DCwnfIN","plugin":null,"proxyApps":false,"remoteDns":"dns.google","server_port":8119
","rx":0,"score":0,"ss_url":"","subscription":"UserConfigured","tx":0,"udpFallback":null,"udpdns":true,"userOrder":0,"weight":74}
imit":1000000,"bypass":false,"city":"Dallas","dirty":false,"disconnect_time":0,"gip":"US","group_id":"us","server":"23.150.248.20

**Figure 30.**

Associated passwords and server IPs extracted from Global VPN's memory.

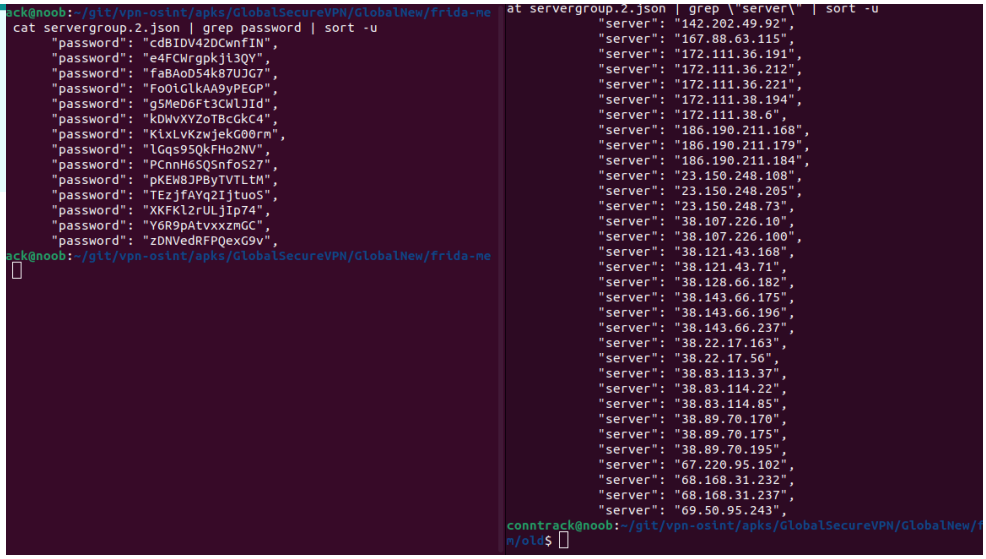
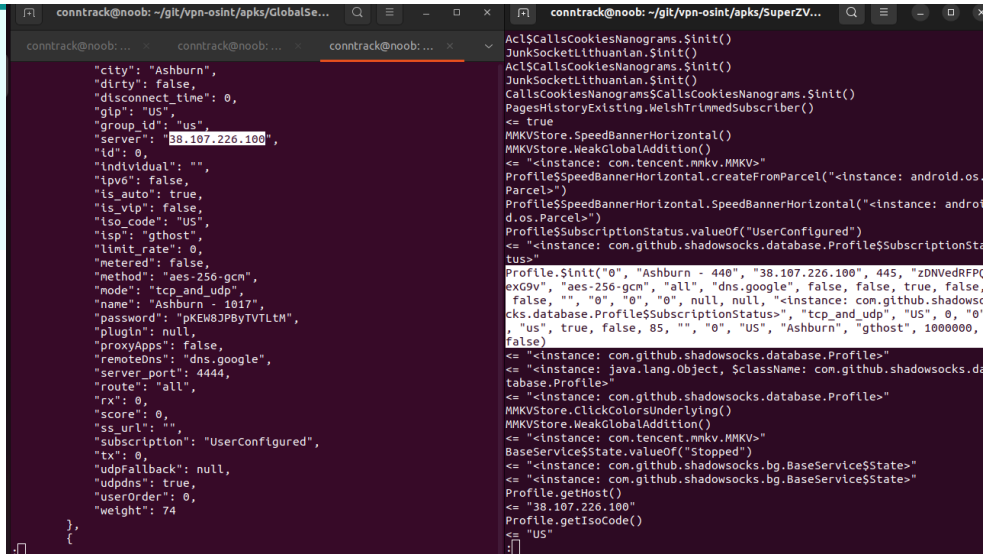



**Figure 31.**

Global VPN (left) and Super Z VPN (right) connected to the same Shadowsocks server (38.107.226.100) but on different ports and with different passwords.



# Limitations

The primary limitation of these analyses was that we cannot guarantee that every privacy or security issue was identified. While we did identify major privacy and security issues, there is always the possibility that other vulnerabilities still exist in the application. We focused primarily on the privacy and security issues related specifically to VPN services (hard-coded passwords, blind-in/on-path attacks) but there may be other issues not yet known.

# VI

# Recommendations & Conclusion

It is already well-established that people should not use free commercial VPNs if their goal is to avoid being tracked, as these providers typically contain advertising libraries that collect detailed information on the user for targeted advertising. The findings in our research lead us to echo this verdict. As for the tunneling protocols in use, Shadowsocks was designed for censorship circumvention. It does not attempt to satisfy confidentiality or other security properties.[43] This design and its use of symmetric encryption invites programming mistakes, such as hardcoding the Shadowsocks password in the APK, as demonstrated in this report.

Furthermore, and importantly, while we recognize and acknowledge the technical challenges that distributors face when identifying and authenticating software developers, distributors (such as Google and Apple) should consider additional vetting for developers of security-critical applications like VPNs across multiple levels—from business to code. One solution is for these app stores to offer an identity verification badge similar to the security badge that VPN apps can receive. Such a policy needs to be carefully considered because there are valid reasons why a developer might need anonymity. In the censorship circumvention space, for example, developers have faced governmental pressure and transnational repression.[44] It is essential to recognize the importance of developer anonymity, and that anonymity is distinct from deception. Software distributors could respect authors' anonymity while still taking action against those who have misrepresented their corporate associations.

**While challenging, technically, distributors should consider additional vetting for developers of security-critical applications like VPNs and possibly include badges to denote such vetting. Such vetting needs to be tempered with care given that developers in some countries may be targeted simply for developing certain kinds of apps.**

43. Fifield, D. (2023) 'Comments on certain past cryptographic flaws affecting fully encrypted censorship circumvention protocols.' Cryptology ePrint Archive. Available here: https://eprint.iacr.org/2023/1362. Date accessed: 27 June 2025.
44. gfw-report (2023) 'Many popular censorship circumvention tools deleted or archived since November 2, 2023. GitHub. Available here: https://github.com/net4people/bbs/issues/303. Date accessed: 2 July 2025.

# Recommendations For Researchers

We have three recommendations for researchers. First, we found that most of the factors considered for scoring, while helpful to a degree, were only marginally so for the purposes of determining provider identity verification. The most revealing information came from combining business names provided on Google Play and the provided website (in the event that one existed), with corporate filings from OpenCorporates and analyzing the application binary (i.e., APK). We recommend that future researchers focus their efforts on cross-referencing business names and similar information with OpenCorporates and other sources of business records. While the other scoring factors were not as impactful, it is still a good idea to use those for supplementary information, as there may be information disclosed accidentally, which we found to be in our case. Second, we strongly encourage researchers with the ability to perform manual analysis of the applications to pay special attention to those that offer Shadowsocks as a tunneling protocol given that there is a chance the password will be hard-coded in the application.

**We strongly encourage researchers with the ability to perform manual analysis of the applications to pay special attention to those that offer Shadowsocks as a tunneling protocol given that there is a chance the password will be hard-coded in the application.**

We also recommend that as a starting point, researchers identify VPN configuration files, certificates for OpenVPN, IPsec, or WireGuard, or passwords for Shadowsocks-based VPNs.

# Recommendations For VPN Users

VPNs can provide increased security and privacy, particularly when users are located in countries with limited privacy protections and repressive information control laws. Unfortunately, VPNs can also provide a false sense of security at best, and at worst, completely compromise privacy and security. In the case of Innovative Connecting, Autumn Breeze, Lemon Clove, Matrix Mobile, ForeRaya Technologies, Wildlook Tech, Hong Kong Silence Technology, and Yolo Mobile Technology Limited, any user of those applications is putting themselves at great risk, because the applications have serious privacy and security issues.

While it may be tempting to use a free commercial VPN such as these, paid VPNs can be generally considered more reliable and secure. For example, we did not identify any serious privacy or security issues with Lantern, Psiphon, ProtonVPN, or Mullvad and it was easy to determine who owns and operates those providers. Their code is either accessible for third-party analysis, or they have audits done by third parties who have vetted their code. They are also active participants in the internet freedom community. We did find that TunnelBear has a hard-coded Shadowsocks configuration, but it was not possible for us to use Shadowsocks to build a tunnel. Shadowsocks, as mentioned earlier, is designed for censorship circumvention and not confidentiality. The hard-coded credentials make it possible for someone between the TunnelBear client and server to decrypt the tunnel encryption and view whatever the client sends or receives. This is an important fact for people who choose to use Shadowsocks for access.

Users should carefully consider what they are using the VPN for. If they plan to use one to connect to their bank or brokerage account on an insecure WiFi, then using VPNs that operate transparently and securely should be prioritized over free VPN services or those that attempt to anonymize their identity and ownership information. If they plan to use Shadowsocks, they should avoid using applications that distribute hard-coded passwords that are shared by every user of the application. For Shadowsocks, if possible, users should use a solution like Google's Project Jigsaw,[45] or have a tech savvy friend whom they trust to set up a proxy server to which they can connect.

Users can also replicate the business-level transparency analysis by searching for the provider's name as stated on their Google Play page or website on OpenCorporates. They can use that information to make a more informed decision about whether they trust the provider. Finally, they can send questions to one of the researchers at Breakpointing Bad or another security team to perform an analysis on their behalf.

45. For more information on Jigsaw, see here: https://jigsaw.google.com/. Date accessed: 2 July 2025.

# Transparency vs. Anonymity table

| Provider Name | VPN name |
|---|---|
| Mullvad | Mullvad |
| TunnelBear | TunnelBear |
| Lantern | Lantern |
| Psiphon | Psiphon |
| ProtonVPN | Proton VPN |
| HotVPN | HotVPN |
| LetsVPN | LetsVPN |
| Astrill VPN | Astrill VPN |
| CookieDevs | Cookie |
| | Ciao Proxy Pro |
| | Ciao Proxy |
| VPN Super Inc | VPN – Super Unlimited Proxy |
| PureVPN | PureVPN |
| Potato VPN | Potato VPN |
| Innovative Connecting | Turbo VPN – Secure VPN Proxy |
| | Turbo VPN Lite – VPN Proxy |
| | VPN Monster – Secure VPN Prox |
| Autumn Breeze | SnapVPN |
| | Signal Secure VPN – Robot VPN |
| | SuperNet VPN |
| Lemon Clove | VPN Proxy Master Pro |
| | VPN Proxy Master Lite |
| Matrix Mobile | Global VPN |
| | Melon VPN |
| ForeRaya Technologies | Super Z VPN |
| Hong Kong Silence Technologies | Touch VPN – Stable & Secure |
| Yolo Mobile Technologies | VPN ProMaster – Secure your net |
| | 3X VPN – Smooth Browsing |
| Wild Tech | VPN Inf |
| | Melon VPN – Secure Proxy VPN |

**Score explanation**:

- White indicates a more transparent provider.
- Dark indicates a more anonymous provider.
- Red indicates serious privacy and security issues identified.

# Recommendations For VPN Providers

VPN providers should consider the jurisdiction under which they operate and the threats they face. Providers that operate in countries with strong privacy laws might consider disclosing their true ownership information. If they do disclose this information, however, they may face increased risk of legal action or targeted attacks by cyber criminals. Providers operating in repressive countries, or where VPNs are not legal, face additional risk of repercussion (such as fines or imprisonment) and may opt not to disclose the ownership information for this reason. While this may minimize legal or cyber crime risks, it could negatively impact trust in their brand.

Regardless of the operator's choice to operate transparently or anonymously, making their code accessible to researchers and third parties for security audits demonstrates a level of openness and value in privacy and security, even if the provider identity is not disclosed. Making third-party security audits freely available for users to review before downloading their applications is another step towards developing rapport with their client base and increasing brand trust.

From a security standpoint, we recommend that developers take measures to harden the VPN server infrastructure against as many of the VPN-specific attacks as possible.[46] Unfortunately, in the case of the server-side blind-in/on-path attack, there is not currently any known mitigation. Providers and developers should be aware of these vulnerabilities and limitations, and monitor their services as much as possible to detect if attacks are occurring (such as exorbitantly large columns of DNS traffic).

If they are using Shadowsocks for transport, we recommend that configuration files be downloaded to the VPN client application dynamically instead of hard-coded in the applications. The passwords should also not be shared across the entire user base, as a compromise of one user's credentials compromises all users.

46. For more information on such attacks, see Mixon-Baca, B., Knockel, J., Xue, D., Ayyagari, T., Kapur, D., Ensafi, R. and Crandall, J. (2024) 'Attacking Connection Tracking Frameworks as used by Virtual Private Networks.' Proceedings on Privacy Enhancing Technologies Symposium (3). 109-126. Available here: https://petsymposium.org/popets/2024/popets-2024-0070.php. Date accessed: 6 June 2025.

# Recommendations For App Store Administrators

We have several comments and recommendations for app store administrators. First, the VPN badge available in Google Play may lead to a false sense of security for users. If one researcher or audit does not uncover any security issues, it does not mean that issues are not present.

Second, app stores in the United States should require developers to list their legal name and address, similar to the European Union's policy. At the very least, this should be required for VPN applications, given their security-critical nature and potential for their abuse. Third, the search results for VPNs need to be fixed, such that VPN apps and their developers are not promoted to the top of the search results. While we did not analyze all of the VPNs when searching for "VPN" in Google Play, many of the top results, such as TurboVPN, appeared near the top of the list — yet this developer has demonstrated repeatedly to be operating deceptively. This report clearly outlines significant security issues with the applications associated with Innovative Connecting PTE. Limited, Autumn Breeze, and Lemon Clove PTE. Limited.

Fourth, a more stringent review of the privacy policies and the behavior of VPN applications needs to be enforced. In the case of VPN Proxy Master, the privacy policy explicitly states it does not collect geographic information, yet the application does collect that information using a third-party API. Fifth, at the very least, VPNs, and potentially other applications with concerning permissions (such as anti-virus software) should be held to much higher security and privacy standards given the vast amounts of data to which they have access, and the value of that data. For example, it is against Apple developer guidelines to collect data from a VPN. However, Innovative Connecting PTE. Limited has been exposed for breaching data, but remains on the Apple App Store.

More generally, these developers are violating a number of rules on both Google Play and the Apple App Store, who, in turn, are failing to adequately enforce their terms. This is especially concerning given their compliance with recent takedown requests of VPN applications in countries such as Russia and China.[47] Google and Apple's compliance calls into question what is truly motivating their lack of enforcement of their privacy rules. Why is it that they promptly remove transparent VPN applications (at the behest of authoritarian governments) from user bases in countries that significantly violate user privacy and security (putting those users at risk), while simultaneously

47. See Apple Censorship's App Store Monitor: Global Unavailability Map. Date accessed: 6 June 2025. See also AppCensorship.org.

allowing questionable apps to remain on their stores — putting users in the United States and abroad at undue risk of digital security and privacy violations?

It is in the public interest that app store administrators put user security and privacy first, above profit.

# VII

# About the Authors and Project Funding

# About the Authors

**Benjamin Mixon-Baca** is a PhD student at Arizona State University (ASU). He has been working in the security space for ~10 years in various capacities. Early in his career, Mixon-Baca served as an Information Controls Fellowship Program (ICFP) fellow with Open Technology Fund (OTF). During this time, he worked with The Citizen Lab helping NGOs defend against targeted threats by deploying and maintaining intrusion detection systems (IDS) and analytics software. In 2016, he held a seasonal fellowship at ICSI where he worked on developing Zeek scripts to fingerprint Tor based on byte patterns of the TLS four-way handshake. Mixon-Baca finished his master's degree in computer science in 2017.

From 2017 to 2020, he worked in the private sector leading different research efforts. This included automated attack frameworks similar to the Metasploit framework; machine learning projects to rank vulnerabilities from most to least exploitable using open source intelligence (OSINT) from the national vulnerability database (NVD), Twitter, and similar. At the end of 2019, Mixon-Baca and his colleagues from the University of New Mexico (UNM) founded Breakpointing Bad, a nonprofit focused on internet freedom research.

In spring 2020, he left the private sector to pursue his PhD and transferred to ASU under the mentorship of Dr. Jedidiah Crandall. His current research has focused broadly on developing attacks and defenses against computer systems. During this time, he and Dr. Crandall developed multiple attacks against VPNs, called **Network Alchemy**. These attacks allow the attacker to place himself between a VPN client and server from an initially off-path position, break the VPN anonymity, or reroute VPN client packets to an attacker. From 2021-2022 he worked as an OTF ICFP fellow with the University of Michigan where they developed CryptoSluice, a tool for automatically identifying weak and unencrypted traffic at scale in an ethical way. CryptoSluice allows an analyst to process real network traffic at high speed and generate a list of candidate applications that an analyst can reverse engineer while protecting the privacy of the network being analyzed. Mixon-Baca conducted the research presented in this report during his third fellowship with OTF.

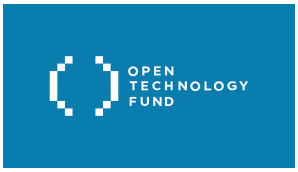
**Contact Information**

- Email: ben@breakpointingbad.com
- Signal: bmixonbaca.22

**Dr. Jedidiah R. Crandall** is an Associate Professor at Arizona State University, in the Biodesign Center for Biocomputation, Security and Society and the School of Computing and Augmented Intelligence. He has been fighting for Internet freedom through teaching, outreach, and research for nearly two decades. This includes Internet measurements, reverse engineering, and attacks on low-level network tracking and routing primitives (e.g., as used by VPNs).

**Dr. Jeffrey Knockel** is an assistant professor at Bowdoin College. Knockel is also a member of Breakpointing Bad.

# About the Funder




**Open Technology Fund (OTF)** is an independent nonprofit organization committed to advancing global Internet freedom. OTF supports projects focused on counteracting repressive censorship and surveillance, enabling citizens worldwide to exercise their fundamental human rights online.

This project was funded by OTF's **Information Controls Fellowship Program**, which supports examination into how governments in countries, regions, or areas of OTF's core focus are restricting the free flow of information, impeding access to the open internet, and implementing censorship mechanisms — thereby threatening the ability of global citizens to exercise basic human rights and democracy. Work focused on mitigation of such threats is also supported. The program supports fellows to work within host organizations that are established centers of expertise by offering competitively paid fellowships for three, six, nine, or twelve months in duration.