An Empirical Analysis of the Commercial VPN Ecosystem

Mohammad Taha Khan*, Joe DeBlasio*, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich & Narseo Vallina-Rodriguez
Commercial VPN Services

VPNs are a $15 billion growing industry*

VPNs advertise a one stop solution to:
- Achieve online anonymity
- Evade Internet censorship
- Access geo-filtered content

VPNs make several privacy and infrastructural claims

The VPN Ecosystem

VPNs can act ***maliciously***
- Monitor and sell traffic
- Inject ads into pages
- Falsely advertise server locations

VPNs can also be ***careless***
- Buggy clients software

**Prior work*** in the Android VPN space

The VPN Ecosystem

NEWS

Users of free VPN Hola vulnerable to hacking, researchers warn

Free P2P VPN Hola sold users' bandwidth which was then used for botnets; researchers say to uninstall Hola now as it makes users vulnerable to hacking.

VIRTUAL PRIVATE SNOOPING —

FTC must scrutinize Hotspot Shield over alleged traffic interception, group says

VPN service "can intercept and redirect HTTP requests to partner websites."

FTC Urged to Investigate AnchorFree VPN User Data Privacy Risks

By: eWEEK Staff | August 14, 2017

Today's topics include the FTC being asked to investigate privacy risks with AnchorFree's Hotspot Shield VPN; Microsoft updating Outlook.com with a new look and some AI-inspired functionality; T-Mobile offering smartphone users aged 55
The VPN Ecosystem

Lack comprehensive **audit and verification** tools for users to **investigate** VPNs

Users eventually rely on **rating websites**, driven by **affiliate marketing**

Review site **VPNMentor** has **95%** of the ratings **4/5** or higher
**Goal:** Objective and quantifiable evaluation of the commercial VPN ecosystem

1. Evaluated ecosystem with 200 VPN provider websites
   - VPNs have multiple marketing strategies and have varying transparency practices

2. Actively tested 62 VPN services
   - Some VPNs monitor traffic, falsely advertise server locations and also leak traffic
Data for Ecosystem Analysis

• VPNs which truly reflect the ecosystem

• Various online data sources:
  ▪ Crawled Google search for “top VPNs”
  ▪ VPN subReddit
  ▪ Personal recommendations

• Further filtered on low costs, vantage points and diversity of users

• Mined information of 200 VPN services
Ecosystem – Marketing

VPNs make use of social media for promotion

- 63% had a Facebook page
- 65% had Twitter account

44% of the VPNs offered affiliate marketing
Ecosystem – Marketing

How affiliate marketing affects users?

1. Users select top VPNs on review sites
2. Top VPNs get more subscriptions
3. More revenue generated by VPN
4. VPNs continue high payoffs and stay on top
Ecosystem – Marketing

IPVanish

Website: AddictiveTips
VPN Rank: #2
Discount: 60%

Website: CNet
VPN Rank: #5
Discount: 25%
Ecosystem – Transparency

25% VPNs did not have a privacy policy

VPN privacy policies varied significantly

Only 23% VPNs claimed a no logs policy
Active Testing of VPNs

Actively tested 62 VPN services

For each service:
1. Register account/install VPN
2. Connect and run test suite
3. Repeat for multiple VPN server locations

Tested 1046 vantage points
VPN Testing Suite

1. Traffic monitoring and manipulation
2. Infrastructural evaluation
3. Traffic leakage
Traffic Monitoring

Do VPNs monitor or modify traffic?

Detecting transparent proxies.
Traffic Monitoring

Do VPNs monitor or modify traffic?

Detecting transparent proxies.

GET/page

To: Website
From: Website

VPN

GET/page

Browser

Proxy

Website
Traffic Monitoring

GET /page
Host: foo
Accept: */*

GET /page
Host: foo
Accept: */*

GET /page
Host: foo
Accept: */*

GET /page
Host: foo
Accept: */*

GET /page
Host: foo
Accept: */*

GET /page
Host: foo
Accept: */*
Traffic Monitoring

At least 5 of 62 VPNs use proxies
Do VPNs advertise accurate server locations?

1. Geo-IP Databases
   - **Problem:** They are inaccurate*

2. Measure RTT to known hosts
   - Look for inconsistencies
   - Evaluate using RTT fingerprints

VPN Server Geolocations

MyIP.io

Set of pinged hosts
VPN Server Geolocations

MyIP.io

Set of pinged hosts

Ping (ms)
VPN Server Geolocations

MyIP.io

Set of pinged hosts

Ping (ms)

Belgium
Canada
Finland
France
Germany
USA
VPN Server Geolocations

HideMyAss

Claims 280+ locations

Set of pinged hosts
At least 6 of 62 VPNs use false geolocations
Traffic Leakage

2 VPNs leak DNS requests
12 VPNs leak IPv6 traffic
Traffic Leakage

VPN Client → VPN Tunnel → Internet
Traffic Leakage

25 VPNs leak traffic due to tunnel failure
Summary Findings

- VPNs marketing creates a biased view of the ecosystem.

- Lack of privacy regulation in the industry

- Some VPNs fail to stand up to their claims:
  - 5 VPNs monitor traffic through proxies
  - 6 VPNs falsely advertise geolocations
  - Over 20 VPNs leak traffic due to misconfigurations
An Empirical Analysis of the Commercial VPN Ecosystem

Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich & Narseo Vallina-Rodriguez