Review of commercial VPN provider claims

Anton Scheitler, Lion Steger*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: anton.scheitler@tum.de, stegerl@net.in.tum.de

***Abstract*—Commercial virtual private networks (VPNs) have gained immense popularity because of their claims to provide secure, fast and obfuscated connectivity. This is especially important, as the number of data breaches is on the rise and user's seek to protect themselves [1]. It is the goal of this paper to review the claims made by large commercial VPN providers and determine whether they are correct or not. To this extent, four of the most popular VPN providers and their protocols are evaluated in terms of security, obfuscation capabilities, speed and trustworthyness. Overall, NordVPN offers great security and speed in their service and only suffers from the fact that their custom VPN protcol is not open-sourced. ExpressVPN shares this problem and also logs identifiable information. Surfshark offers a slightly slower VPN experience and shares user data with advertisers. Hide.me uses secure and open-sourced protocols by default and logs very little and non-identifiable data. Their service, however, is also the slowest. None of the VPN providers are able to obfuscate VPN traffic and make VPN usage invisible.**

***Index Terms*—networks, VPN, OpenVPN, IKEv2/IPSec, WireGuard, NordLynx, Lightway**

1. Introduction

The rising number of data breaches and censorship in countries around the world leads to a growing interest in VPN services [1]. VPN providers claim that, with their services, users are able to use the Internet more securely and circumnavigate governmental censorship and geoblocking, while suffering minimal latencies. However, these claims can be incorrect or misleading and might lead consumers to make poor buying decisions. This paper seeks to address this issue by analyzing different providers and their protocols to determine if their claims of security, obfuscation capabilities and speed hold up to reality. The criterium for security will be that all of the protocols used by a provider are either open-sourced or audited regularly and haven't had major security vulnerabilities in the past. To compare speed, the latencies of the connections of the providers are measured. Finally, a VPN provider is considered to offer decent obfuscation, if it can hide the fact that their customers are using their service.

2. Background

A private network is a network that is isolated from other networks. Communication within a private network cannot leak to the outside. This can be achieved by leasing physical private communication lines and connecting hosts with it. A VPN (Virtual Private Network) is a private network, built on top of a public network. In a VPN, hosts are blocked off from a public network and can only be connected to over secure tunnels [2, section 8.6.3]. A tunnel is a special connection between hosts. When a data packet passes through a tunnel, it is encrypted and encapsulated. This is useful, when communication needs to be secure or the tunnel ends at a location other than the final destination of the packet. These tunnels do not have to be formed via private communication lines but instead over the public Internet. This allows any host on the Internet with the necessary credentials to connect to a VPN. [2, section 8.6.1] In order to connect to a VPN, a user first needs to authenticate themselves, often followed by a negotiation of a cipher suite with the VPN server. The client then agrees to a tunneling protocol and exchanges secrets with the server. [3] A tunneling protocol determines how data is encrypted and encapsulated before being sent over a tunnel. It is the backbone of a VPN.

Commercial VPN providers offer a VPN which consists of a set of proxy servers, that their customers can connect to. Thanks to the properties of a VPN, customers can therefore communicate over an encrypted connection, while obfuscating their IP address and physical location.

A single VPN provider may support a number of tunneling protocols which is why it is important to understand them in order to be able to compare providers.

2.1. OpenVPN

OpenVPN is one of the most popular tunnel protocols used by VPN providers. It uses the widespread SSL/TLS mechanisms to authenticate hosts, exchange cryptographic secrects between them and encrypt messages. It uses the OpenSSL library to implement this. In addition, it runs on all major operating systems, including Windows, macOS, Linux, Android, iOS and even OpenBSD [4]. Packets traveling through an OpenVPN tunnel can be encapsulated in TCP, as well as UDP packets [5]. OpenVPN can also be configured to establish connections via the port 443. This is the same port used for HTTPS, which makes it harder for ISPs to use firewalls to block VPN traffic [6, section 8.2.3]. Additionaly, OpenVPN is open-sourced which reduces the risk of unpatched vulnerabilities and backdoors

 doi: 10.2313/NET-2025-05-1_21

2.2. IKEv2/IPSec

This protocol is a combination of two different mechansims. The first is IPSec, which is used for encryption. The second is the the Internet Key Exchange Version 2 (IKEv2), which is used for authentication and the exchange of secrets [6, section 3.1]. Once keys have been generated and exchanged, IPSec is used to encapsulate and encrypt packets. IPSec offers different encapsulation mechanisms, however, for IKEv2/IPSec, the Encapsulation Security Payload (ESP) is used. This works by first encrypting the original message and wrapping it with an ESP header and trailer. The resulting message is wrapped inside another IP packet [6, section 4.1]. This approach of wrapping an entire packet within another IP packet is called the tunnel mode of IPSec. The resulting packet has two IP addresses. The "inner" IP address is that of the original message and the "outer" address is that of the message after encapsulation. One benefit of this protocol is that it supports MOBIKE, which can handle changes in the outer IP address of a device while still preserving the connection to a VPN [6, section 3.9]. This makes IKEv2/IPSec especially well suited for VPN usage on mobile devices and laptops.

2.3. WireGuard

WireGuard is a new and open-sourced VPN Protocol. It uses public keys instead of SSL certificates for authentication and the Noise Protocol Framework, which is based on Diffie-Hellman, for key exchanges [7]. As opposed to the previous protocols, WireGuard does not work with a suite of cryptographic ciphers and instead handles all encryption using the stream cipher ChaCha20-Poly1305. The WireGuard protocol does not specify how to dynamically assign IP addresses to clients connecting to a server. Instead, a naive implementation of WireGuard would simply store the static IP addresses of those clients. All in all, WireGuard is a fast and secure protocol but has some anonymity concerns that come with storing static IP addresses [6, section 8.3]

2.4. SSTP

The SSTP protocol is a closed-source VPN protocol developed by Microsoft. It is similar to OpenVPN in that it uses SSL/TLS for authentication, key exchanges and encryption. SSTP can be configured to use TCP, as well as UDP for encapsulation. SSTP connections can also be set up over port 443, achieving some level of obfuscation, as described in 2.1. Overall SSTP servers are easier to setup than OpenVPN servers. However, the protocol is only supported by Windows [6, section 8.2.1].

2.5. L2TP

The Layer 2 Transport Protocol (L2TP) uses IKE for authentication and key exchange and IPSec for encryption and encapsulation. L2TP is an older VPN protocol and can be configured with IKEv1 which leads to the use of a weak group PSK. Even if an implementation of L2TP is configured correctly, it adds layers of unnecessary encapsulation which increases network issues like packet fragmentation. Also, L2TP does not support AEAD algorithms which leads to an increased CPU usage [6, section 8.5.2].

TABLE 1: VPN Provider Protocol Support

	NordVPN	ExpressVPN	Surfshark	Hide.me
OpenVPN	✓	✓	✓	✓
IKEv2/IPSec	✓	✓	✓	✓
WireGuard			✓	✓
SSTP			✓	✓
L2TP/IPSec			✓	
NordLynx	✓			
Lightway		✓		

[12] [13] [14] [15] [16]

2.6. NordLynx

NordLynx is a VPN protocol built on top of WireGuard and created by the VPN provider NordVPN. It addresses the anonymity issues of WireGuard by constructing a layer of double NATs around a WireGuard server. The first NAT assigns the same IP address to every user, making them indistinguishable to the server. The second NAT assigns a unique address to a user from a pool of IP addresses. This obfuscates traffic. While the NordLynx protocol is not open-sourced, its foundation WireGuard is. This makes it more transparent than completely closed-source protocols, such as SSTP [8].

2.7. Lightway

Lightway is a protocol created by the provider ExpressVPN. Similar to NordLynx, it seeks to address the anonimity issues of WireGuard. Different from NordLynx however, it has no association with WireGuard and is instead built from the ground up. Lightway utilizes SSL/TLS for authentication, key exchange and encryption [9]. A collection of components of the Lightway protocol is also open-sourced under the name lightway-core. However, the protocol itself is not. To assure users of its security, ExpressVPN has also issued independent audits of its protocol [10].

3. Analysis

In order to evaluate VPN providers based on the protocols they offer one needs an overview over which protocol is offered by which provider. In this paper, the focus will be on four VPN providers in total, namely NordVPN, ExpressVPN, Surfshark and Hide.me. The first three were chosen as they are among the largest commercial VPN providers. Hide.me is an another interesting provider as it is free and has been operating with a long and positive track record [11]. An overview over what protocols are supported by them and what their default protocols are, is provided in table 1. As shown by the overview, the most popular protocols such as OpenVPN and IKEv2/IPSec are offered by every provider. However, there are some protocols that are only supported by a single provider. This is especially the case for the custom protocols developed by a provider. The difference between these protocols will be a deciding factor in the evaluation of providers.

 doi: 10.2313/NET-2025-05-1_21

4. Design

In this paper, providers will be evaluated based on four criteria.

The first is security. For many consumers, the main reason of using a VPN is for the additional layer of security provided by it. How secure a protocol, and by extension its provider is, is determined by the security of the key exchange mechanisms and encryption ciphers that they use. Offering outdated protocols to customers can pose a security risk.

The second criterium is obfuscation. Many VPN users suffer from government censorship and use VPNs to work around them. Since VPNs are also deemed illegal in many countries they want to obsucre their traffic as much as possible and avoid their VPN usage being detected.

The third criterium is speed. This is a deciding factor for VPN users when picking a provider. How fast a VPN connection is, is determined by the protocol used but also by the density of a provider's network of VPN servers.

Lastly, customers value transparency in VPN providers. They want to be sure that their VPN provider has their privacy and security interests at heart. Providers can do this by using open-sourced protocols, running frequent and independent audits and avoiding logging user data whenever possible.

5. Findings

The following sections outline the findings of the reasearch into provider claims regarding security, speed, obfuscation and trustworthyness.

5.1. Security

As explained in 2.1, OpenVPN is an SSL-VPN which offers every cipher supported by SSL/TLS. This means that it has access to very secure encryption algorithms such as AES-256, but it also means that it can be misconfigured. In the past there have been instances of OpenVPN implementations using the outdated and insecure hashing algorithm MD5 [17]. However, as long as it is configured properly, OpenVPN is widely considered secure.

IKEv2/IPSec is a secure protocol and all implementations adhere to strong cryptographic standards [18].

WireGuard uses ChaCha20-Poly1305, which does not have any known significant security problems [19, section 4]. Despite this, the encryption algorithm is not approved by NIST [6, section 8.3].

L2TP is considered deprecated by NIST and can be misconfigured quite easily. This is why it is suggested that L2TP implementations should be migrated to IKEv2/IPSec [6, section 8.5.2].

NordLynx uses the same encryption as WireGuard, since it is built on top of it [8].

Lightway can use any cipher, wolfSSL provides, including AES-256 [12]. Independent audits have also confirmed that Lightway is secure [10].

While SSTP offers the encryption and integrity algorithms of SSL/TLS [6, section 8.2.1], it also had severe vulnerabilities in the recent past which allowed for remote code execution [20].

5.2. Obfuscation

While OpenVPN can be configured to use port 443 to form connections, it is still vulnerable to fingerprinting, meaning that OpenVPN traffic can be identified and blocked with a very low false-negative rate [21].

IKEv2/IPSec services can be blocked easily by restricting acces to the ports it uses, namely UDP ports 500 and 4500 [6, section 3.1]

Like with anonomity, WireGuard leaves traffic obfuscation up to the VPN providers that implement it [22]. In this regard, NordVPN, Surfshark and Hide.me all offer obfuscated VPN servers, which they claim make OpenVPN traffic invisible [23] [24] [25]. This claim, however, is false as it has been shown that all of these obfuscated VPN services suffer from insufficient obfuscation over the length of packets [21, section 8]. This allows for the identification of VPN traffic, rendering it anything but invisible.

5.3. Speed

Figure 1: Comparison of OpenVPN UDP speeds across VPN providers

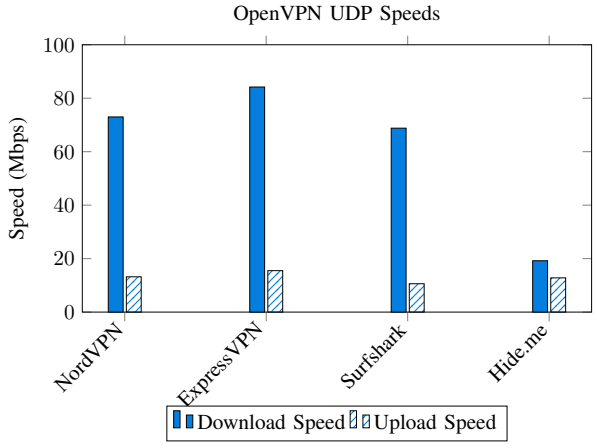
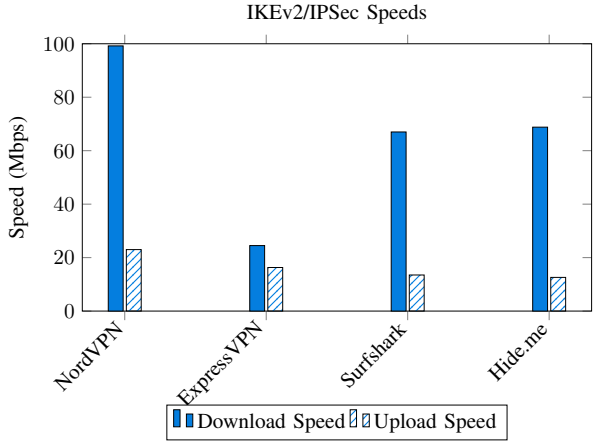
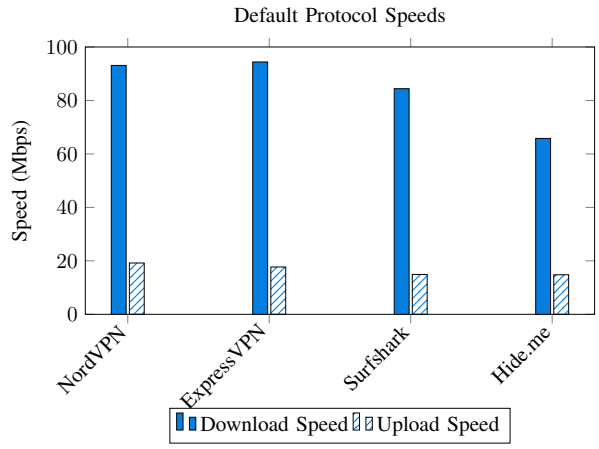


Figure 2: Comparison of IKEv2/IPSec speeds across VPN providers



All providers make claims about the speed of their connections. ExpressVPN and Surfshark both reference third party reviews that give top ratings to their

Figure 3: Comparison of default protocol speeds across VPN providers



speed [26] [27]. NordVPN claims that it is among the fastest VPN providers on the market [28] and Hide.me boldly states that they are the fastest VPN ever seen [29]. To compare the performance of the different protocols on offer by each provider, speed tests were conducted for every provider and their protocols. The protocols that were compared are OpenVPN, IKEv2 and the default protocols for each provider, namely NordLynx, Lightway and WireGuard. These protocols were chosen because they are supported by every provider. For each protocol and provider, a connection was established to the provider's best choice for a server in the United States. Then, speedtest.net was used to determine the the download and upload speed of the connection. The US was chosen as all providers have a high server density there [30] [31] [32] [33]. The result of these speed tests are shown in figures 1, 2 and 3.

5.4. Transparancy and Trustworthyness

As mentioned in 2, OpenVPN and WireGuard are both open-sourced, which makes them trustworthy protcols.

Similarly, IKEv2/IPSec is defined via an RFC standard [34], for which open-source implementations exist.

SSTP on the other hand is a closed-source protocol, which still showed severe vulnerabilities in the past as shown in 5.1. This and the fact that Microsoft has collaborated with governmental institutions, such as the NSA, in the past raises trust issues [35].

While NordLynx itself is not open-sourced, its foundation is, meaning that this protocol offers an acceptable amount of trustworthyness.

The other VPN-provider-made protcol, ExpressVPN is open-sourced in some form, via the lightway-core repository which contains certain components of the protocol. However the documentation of this repository is anything but in-depth and quite incomplete with lots of sections marked as "Coming Soon" [9]. ExpressVPN advertises that they run security audits on their software, including Lightway, [12], however, the last audit was two years ago [10]. Also, reviews online praising Lightway are financed directly by the parent company of ExpressVPN, namely Kape Technologies [36]. While this does not have any impact on the actual security of the protcol it at least raises a few eyebrows.

A trustworthy VPN provider should log as little user data as possible. In this regard, NordVPN stores only usernames and timestamps of their customers connections in order to determine how many concurrent users are active. This information is deleted 15 minutes after the session terminates [37].

ExpressVPN stores more information, including the days, on which a user has established a successful connection to which VPN server location from which country. They also log how much data has been transferred by a given user [38].

Surfshark stores metrics, such as how much data has been transferred by a user and the number of times they have used Surfshark's services. In addition, Surfshark collects data, including their users' mobile device id, the browsers they used and what network was used to access the VPN. They use this data in collaboration with advertisers to provide tailored ads to their customers [39].

Hide.me in comparison stores only very little data. Namely a user's, randomly generated, username and internally assigned IP address. This is only done for troubleshooting purposes and their logs are cleared every few hours. They also log traffic metrics of users in order to bill them properly [40].

6. Evaluation

In terms of security, all of the providers offer secure protocols, such as WireGuard, NordLynx or Lightway as their default. The most insecure protocol on offer by any provider is L2TP/IPSec, which Surfshark still supports. However in order to use L2TP, Surfshark users need to really go out of their way, as it is buried in options and configurations. They also make it clear in their online resources that they strongly advise against it's use [15].

In terms of VPN traffic obfuscation, ExpressVPN is the only provider which does not make wrong claims about obfuscated VPN servers that make traffic invisible. NordVPN [23], Surfshark [24] and Hide.me [25] all make these claims, which gives their customers a false sense of security [21, section 8].

The speed measurements make it clear that NordVPN and ExpressVPN are the fastest VPN providers. Therefore they are the most attractive provider for consumers who value faster connections. Surfshark falls slightly behind in terms of speed and Hide.me is by far the slowest provider among them.

In terms of transparency, NordVPN and ExpressVPN underperform as their custom protocols, NordLynx and Lightway, are both closed-source. Though NordLynx fares a little better as it is based off of WireGuard. Surfshark and Hide.me on the other hand only offer open-sourced protocol as their defaults. The logging policies of ExpressVPN and Surfshark are quite intrusive. ExpressVPN is capable of determining that a given user has accessed their services. This puts customers at risk that live in countries where VPN usage is illegal. Surfshark uses the data they log to collaborate with advertisers which should raise red flags for consumers who seek out VPNs to enhance their privacy online.

7. Related work

Other works have already evaluated VPN providers based on different criteria, such as speed, security, server locations and confidentiality [41] [42]. This paper is different from these evaluations because it focuses on the protocols offered by the providers instead of their general characteristics. It also performs measurements of all the available protcols instead of just using a provider's default. There are also papers which have shown that vpn providers make false claims [21, section 8]. Those are, however, often focused on certain aspects, such as the lack of obfuscation in a particular protocol. This paper instead offers a broad examination of several characteristics and puts them in relation to one another.

8. Conclusion and future work

Even though the set of observed providers is quite small with just four providers, it nevertheless showed that false and misleading claims are not uncommon in this industry. Many providers state that they are able to completely obfuscate VPN traffic or that they log zero information that can trace users back to them. Every provider that has been examined here is guitly of at least one of those claims. In addition, if a provider offers a custom protocol, it is advertised heavily and unrealistic claims about it are made, such that it is the "most secure" protocol in existence [12]. Also, all of the providers mentioned in this work offer at least one proprietary tunneling protocol. In future work, the set of examined providers could be expanded to include smaller providers that have a greater focus on transparency and trust.

References

[1] "Global number of breached accounts," https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/, 2024.

[2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*. Prentice Hall, 2011.

[3] "How Does a VPN Work?" https://www.paloaltonetworks.com/cyberpedia/how-does-a-vpn-work, 2024.

[4] M. Feilner and N. Graf, *Beginning OpenVPN 2.0.9*. Packt Publishing, 2009.

[5] "OpenVPN Protocol," https://openvpn.net/community-resources/openvpn-protocol/, 2024.

[6] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs." NIST, 2020.

[7] J. A. Donenfeld, "Wireguard: Next generation kernel network tunnel." in *NDSS*, 2017, pp. 1–12.

[8] E. Juodytė, "NordLynx protocol – the solution for a fast and secure VPN connection," https://nordvpn.com/blog/nordlynx-protocol-wireguard, Jan 2022.

[9] ExpressVPN, "Lightway Core," https://lightway.com/docs/lightway-core/1.0.0/intro.html, 2024.

[10] "Pentest-Report ExpressVPN Lightway 10.-11.2022," https://cure53.de/pentest-report_expressvpn-lightway.pdf, 2022.

[11] "VPN reviews," https://www.top10vpn.com/, 2025.

[12] "Welche Arten von VPN-Protokollen gibt es?" https://www.expressvpn.com/de/what-is-vpn/protocols, 2024.

[13] "VPN protocols: L2TP/IPsec," https://www.expressvpn.com/what-is-vpn/protocols/l2tp, 2024.

[14] "hide.me VPN Protocols Explained," https://hide.me/en/knowledgebase/hide-me-vpn-protocols-explained, Dec 2023.

[15] "What protocols can I use with Surfshark?" https://support.surfshark.com/hc/en-us/articles/360010324739-What-protocols-can-I-use-with-Surfshark, Apr 2024.

[16] "Next-generation VPN encryption," https://nordvpn.com/features/next-generation-encryption/, 2024.

[17] "OpenVPN Security Advisories," https://openvpn.net/security-advisories/, 2024.

[18] J. Park, T. Ahn, and J. Ryou, "Efficient Analysis Method for IKEv2/IPsec Traffic Visibility: Applications on Mobile Platforms," in *2024 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, 2024, pp. 1–4.

[19] "ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)," https://datatracker.ietf.org/doc/html/rfc7905, 2016.

[20] "Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability," https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21535, 2023.

[21] D. Xue, R. Ramesh, A. Jain, M. Kallitsis, J. A. Halderman, J. R. Crandall, and R. Ensafi, "OpenVPN is Open to VPN Fingerprinting," *Commun. ACM*, Jun. 2024. [Online]. Available: https://doi.org/10.1145/3618117

[22] "Known Limitations," https://www.wireguard.com/known-limitations/, 2022.

[23] "Enable or disable Obfuscated servers," https://support.nordvpn.com/hc/en-us/articles/19615332252561-Enable-or-disable-Obfuscated-servers, 2024.

[24] "Use obfuscated servers for extra privacy," https://surfshark.com/features/obfuscated-servers, 2024.

[25] "VPN Obfuscation Methods: Hide That You Are Using VPN," https://hide.me/en/blog/vpn-obfuscation-methods/, 2024.

[26] "The fastest VPN gets even faster," https://www.expressvpn.com/de/lightway, 2025.

[27] "Get a high-speed VPN," https://surfshark.com/features/fast-vpn, 2025.

[28] "One of the fastest VPN providers on the market," https://nordvpn.com/features/high-speed-vpn/, 2025.

[29] "What makes Hide.me VPN stand out," https://hide.me/en/, 2025.

[30] "NordVPN server locations," https://nordvpn.com/servers/, 2025.

[31] "Full list of ExpressVPN server locations," https://www.expressvpn.com/vpn-server, 2025.

[32] "VPN server list," https://surfshark.com/servers, 2025.

[33] "hide.me's Worldwide VPN Locations," https://hide.me/en/network, 2025.

[34] C. Kaufman, P. E. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, Oct. 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7296

[35] "Microsoft handed the NSA access to encrypted messages," https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, 2013.

[36] K. Hassel, "ExpressVPN Lightway Protocol Review and Comparison 2024," https://www.vpnmentor.com/blog/lightway-protocol-review/, 2024.

[37] "NordVPN Privacy Notice," https://my.nordaccount.com/legal/privacy-policy/nordvpn/, 2023.

[38] "ExpressVPN Privacy Policy," https://www.expressvpn.com/privacy-policy, 2024.

[39] "Surfshark Privacy Policy," https://surfshark.com/privacy, 2024.

[40] "Privacy Policy," https://hide.me/en/privacy, 2023.

[41] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez, "An Empirical Analysis of the Commercial VPN Ecosystem," in *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*. ACM, 2018. [Online]. Available: https://doi.org/10.1145/3278532.3278570

[42] O. Turki, "A comparison of VPN providers focusing on their security and speed." Turku University of Applied Science, 2024.