Analysis of VPNs from a user-centred perspective

Alexandra Neagu
5233194

February 18, 2024

1 Introduction

In the realm of online security and privacy, the selection of a Virtual Private Network (VPN) is pivotal. This essay explores a critical need users may have when selecting a VPN: a clear explanation of logging and data practices, as identified in the Ramesh et al. (2023) paper [8]. Rooted in escalating concerns about privacy, users seek assurance that VPNs won't compromise their data. This need significantly influences VPN selection, impacting the pre-engagement phase. Additionally, the essay delves into users' trust issues in regard to VPN providers, particularly the alarming concern about VPN providers selling user data. Understanding these dynamics is essential for designing secure and privacy-centric technologies in the digital era.

2 User Needs

One important user need identified in the research paper is the clear explanation of logging and data practices. This need is reported by over 17.3% of tpersonally1800mobilehe users, with 216 users ranking it as their number one criterion when selecting a VPN [8].

The importance of a clear explanation of logging and data practices is rooted in users' concerns about privacy and security. VPNs are utilized to enhance online privacy and security by encrypting internet traffic and masking the user's IP address [5]. However, users are increasingly aware of the potential risks associated with VPN services that may log their activities or mishandle their data. In an era where data breaches and privacy concerns are prevalent [7], users want assurance that their online activities are not being logged or misused. A VPN provider that provides a detailed and understandable explanation of its logging policies instils trust in users and helps them assess the privacy implications of using the service.

The user need for a clear explanation of logging and data practices significantly impacts the task of finding a good VPN client. Users who prioritize this criterion are likely to scrutinize VPN providers' privacy policies, terms of service, and logging practices before making a decision. VPN providers that can effectively communicate their commitment to user privacy and provide transparent information about their data handling practices are more likely to attract users who value privacy. Conversely, VPN providers with ambiguous or complex logging policies may struggle to gain the trust of users who prioritize transparency.

3 User Tasks

The user need identified for a clear explanation of logging and data practices may not have a direct impact on the specific VPN tasks outlined in the Binkhorst et al. (2022) paper [6]. The tasks mentioned are more focused on the technical aspects of using a VPN rather than the privacy and logging concerns. However,

it indirectly influences the user's overall VPN experience and decision-making process.

While the acts of connecting to the Internet itself is not directly influenced by the need for a clear explanation of logging and data practices, users who prioritize privacy and transparency in VPN services may adopt a more cautious approach when connecting to unsecured networks. The concern for logging practices often reflects a broader awareness of online privacy and security. Users who are conscious of VPN logging policies may be more vigilant about the security of their internet connection, especially when accessing public Wi-Fi networks. Likewise, launching the VPN software is not directly affected by the user's privacy need, but it may influence their decision to select a particular VPN software in the first place.

The act of entering credentials and 2-factor tokens is more about authentication and security. Although users who are concerned about logging practices might value security, the direct impact on these tasks is also limited. Security features, such as multi-factor authentication, are often seen as standard practices, and users may prioritize these without direct consideration of logging policies.

Lastly, clicking the connect button is the final step in establishing a VPN connection. While users who are privacy-conscious may appreciate providers with transparent logging practices, the act of clicking the connect button is more about ensuring a secure connection. Therefore, this task is less likely to be directly influenced by the chosen user need.

In summary, the user need for a clear explanation of logging and data practices may not have a direct impact on the technical tasks of using a VPN. However, it plays a role in the pre-engagement phase where users select a VPN provider.

4 User Perceptions

One reported perception or trust issue in the research paper is the high level of concern among users regarding VPN providers selling their data (73.2%, 917 of 1,252) [8]. This issue is important because it directly relates to user privacy and trust in the VPN ecosystem. Users are worried about the possibility of their sensitive information being monetized by VPN providers, which undermines the very purpose of using a VPN for privacy protection [3].

Returning to the user tasks introduced above, we can observe that the reported perception affects the user's ability to perform said tasks. Users may hesitate to connect to the Internet through a VPN if they are concerned about the provider's integrity in handling their data. This hesitation could lead to delayed or selective use of VPN services based on perceived trustworthiness. Likewise, users may be reluctant to launch VPN software if they are worried about data selling practices. They might also be hesitant to input sensitive information like credentials and 2-factor tokens into the VPN software if they are concerned about data misuse. This could result in a reluctance to fully engage

with the authentication process. Lastly, users might avoid clicking the connect button. The fear of potential data sales could lead to a lack of confidence in establishing a secure VPN connection.

As to the costs inquired on the user, mental-wise, users may experience increased stress, anxiety, or cognitive dissonance when considering the possibility of their data being sold by the VPN provider [2]. This mental burden could affect decision-making and the overall user experience. On the other side, users may face the physical cost of having to find alternative means of securing their internet connection, potentially resorting to other cybersecurity tools or forgoing the use of a VPN altogether.

In summary, the trust issue of VPN providers selling user data is important due to its direct impact on user confidence in VPN services. This concern can influence users' willingness to perform essential VPN tasks, introducing mental and potential physical costs if users decide to alter their behaviour or seek alternative solutions.

5 Similar Technology

A technology that shares similarities with the use of VPN clients, especially concerning user challenges and preferences, is the use of password management tools. Users choose VPNs to enhance their online security and privacy by encrypting internet traffic and masking their IP addresses, and similarly, they adopt password managers to improve security by generating and storing complex, unique passwords for various online accounts [4]. From an authentication point of view, with VPNs, users authenticate themselves by entering credentials and, in some cases, using 2-factor tokens. In the case of password managers, users authenticate themselves by using a master password to access their stored passwords. Another similarity worth mentioning is the feeling of trust and reliability. Users need to trust that the VPN provider will secure their internet connection and not compromise their data, and they must trust that the password manager will securely store and manage their sensitive credentials [1].

On the other side, the most important difference lies in the nature of the data being protected and the potential consequences of a security breach. In the case of VPNs, the primary concern is the privacy of internet traffic. A breach in VPN security could expose users' online activities, potentially compromising sensitive information such as browsing habits, personal communications, or even financial transactions. As for password managers, the primary concern is the security of login credentials. A breach in a password manager could expose users' passwords, putting multiple online accounts at risk. The consequences may include unauthorized access to email, social media, financial, or other sensitive accounts.

In conclusion, while both VPN clients and password management tools are employed for security and privacy, a compromise in the VPN context could expose a broader range of online activities. On the other hand, a compromise in a password manager may have cascading effects, as it puts multiple accounts at

risk. In the end, it is important to remember that user challenges and preferences may differ based on their priorities. Users who prioritize internet activity privacy may place higher importance on the VPN client's reliability and logging policies. Conversely, users who prioritize the security of their online accounts may be more concerned about the robustness of their password management tool. Therefore, understanding these nuanced differences is essential for designing and selecting technologies that align with users' specific security and privacy needs.

References

[1] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. "A Usability Study and Critique of Two Password Managers." In: *USENIX Security Symposium*. Vol. 15. 2006, pp. 1–16.

[2] Jon D Elhai, Jason C Levine, and Brian J Hall. "Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior". In: *Internet Research* 27.3 (2017), pp. 631–649.

[3] Mohammad Taha Khan et al. "An empirical analysis of the commercial vpn ecosystem". In: *Proceedings of the Internet Measurement Conference 2018*. 2018, pp. 443–456.

[4] Sarah Pearman et al. "Why people (don't) use password managers effectively". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 319–338. ISBN: 978-1-939133-05-2. URL: https://www.usenix.org/conference/soups2019/presentation/pearman.

[5] Mark Smirniotis. *What is a VPN and what can (and can't) it do?* Mar. 2021. URL: https://www.nytimes.com/wirecutter/guides/what-is-a-vpn/.

[6] Veroniek Binkhorst et al. "Security at the End of the Tunnel: The Anatomy of {VPN} Mental Models Among Experts and {Non-Experts} in a Corporate Context". In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, pp. 3433–3450.

[7] Jurgita Lapienytė. *25 million free VPN User Records exposed — Cybernews*. Nov. 2023. URL: https://cybernews.com/security/25-million-free-vpn-user-records-exposed/.

[8] Reethika Ramesh, Anjali Vyas, and Roya Ensafi. "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers". In: *32nd USENIX Security Symposium (USENIX Security 23). USENIX Association*. 2023.