Beyond the Price Tag: Examining User Behavior and Trust in Free VPN Services

Kurudunje Deekshith Shetty | Shitil Shetty

9th May, 2025

Abstract

This study investigates user trust in free Virtual Private Network (VPN) services through a primary survey of 94 general users, complemented by a secondary survey of 16 security-aware users with cybersecurity expertise. Results reveal a pronounced privacy paradox: general users, driven by cost, adopt free VPNs despite low trust and limited understanding of data practices, while security-aware users, critical of technical vulnerabilities, prefer paid alternatives. Detailed analysis of usage patterns, trust levels, motivations, issues, and perceived risks underscores the need for enhanced transparency and user education to align VPN usage with privacy goals.

1 Introduction

Virtual Private Networks (VPNs) are critical for enhancing online privacy and security by encrypting traffic and masking IP addresses to mitigate surveillance and data breaches [11, 2]. Free VPN services, while popular, raise concerns due to their reliance on data monetization or compromised security [8, 9]. This research examines user trust in free VPNs through a primary survey of 94 general users conducted in April 2025, supplemented by a secondary survey of 16 security-aware users (April 11–19, 2025) offering technical insights [4]. The study addresses four key research questions:

- To what extent do users understand and trust free VPN providers' data handling practices?
- What motivates users to choose free VPNs over paid alternatives?
- What issues do users commonly experience with free VPN services?
- What are users' perceptions of risks associated with free VPNs and how import is data privacy to them?

By contrasting general and security-aware user perspectives, this study provides a nuanced understanding of trust dynamics, informing strategies to improve the VPN ecosystem.

2 Background and Related Work

Global VPN adoption has surged amid growing privacy concerns [5, 12]. Research identifies a "privacy paradox," where users prioritize convenience over security, often choosing free VPNs

despite risks [19, 13]. Free VPNs frequently monetize user data or exhibit vulnerabilities like weak encryption [9, 20].

Technical analyses highlight implementation flaws, such as inadequate encryption or data logging [1, 15], while user studies explore adoption factors like cost and ease of use [18, 3]. Foundational surveys provide insights into VPN technologies [6, 10], and recent work examines specific use cases, such as secure communications [7, 17].

This study builds on these efforts by integrating general user data with security-aware perspectives from a complementary survey [4], offering a comprehensive view of trust and behavior in free VPN usage.

3 Methods

The study utilized a dual-survey methodology:

1. **General User Survey**: Conducted in April 2025 with 94 participants , this survey included 22 questions on demographics, VPN usage, trust, motivations, issues, and risks. It featured multiple-choice, Likert-scale, and open-ended questions, capturing diverse user experiences which was shared through social media platforms like reddit and LinkedIn.

2. **Security-Aware User Survey**: Conducted April 11–19, 2025, with 16 participants/students undertaking Human Factors in Security course, this survey focused on technical evaluations, trust factors, and security concerns[4].

Quantitative data were analyzed using descriptive statistics, while qualitative responses were thematically coded to identify recurring patterns. Participants were anonymized (P1–P94 for general users, aliases like “cranky-wilbur” for security-aware users).

4 Results and Analysis

The following subsections address the research questions, integrating insights from both surveys and highlighting key trends from the general user data.

4.1 Demographic Characteristics

The general user sample was predominantly young (61.7% aged 18–24, 24.5% 25–34, 13.9% other), gender-balanced (46.8% male, 51% female, 2.2% non-binary), and moderately educated (43.6% bachelors, 26.6% masters or higher). Technical proficiency was mostly intermediate (67%), with 18.1% beginners and 14.9% advanced.

Security-aware users were with higher proficiency (25% advanced, 12.5% expert) and roles such as cybersecurity analysts, software developers, and students [4]. Their technical expertise shaped their critical stance on free VPNs.

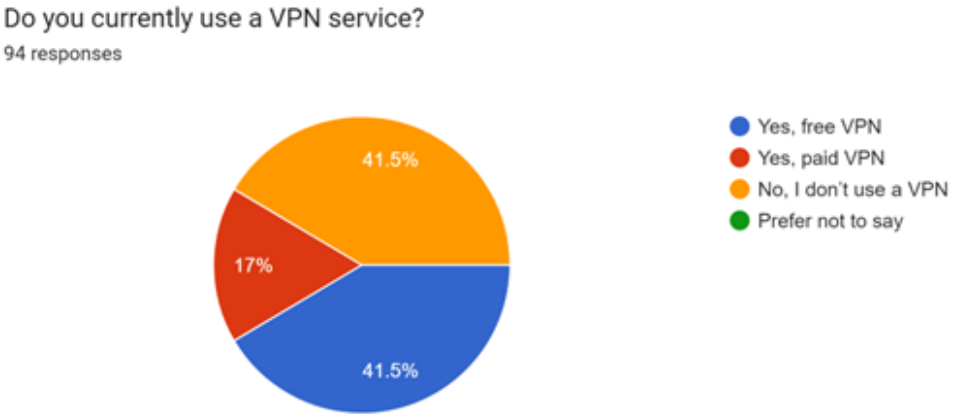
4.2 VPN Usage Patterns

Among general users, 41.5% (39) used free VPNs, 17% (16) used paid VPNs, and 41.5% (39) used none. Usage frequency varied: 40% of free VPN users were daily users, 35% weekly, and 25% monthly or less. Common activities included anonymous browsing (52.6%, 41 responses),

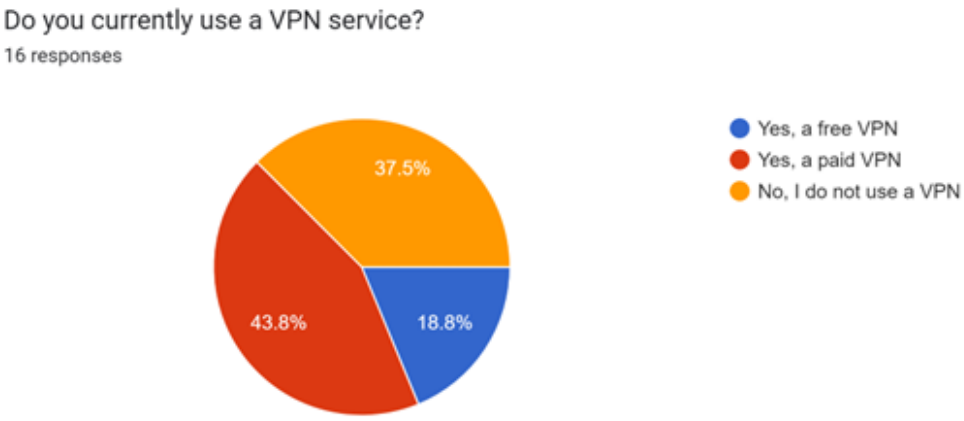
streaming geo-restricted content (34.6%, 27), remote work (17.9%, 14), gaming (17.9%, 14), and accessing restricted websites (19.2%, 15). Notably, 63.8% (60) never used VPNs for sensitive tasks (e.g., online banking), with only 3.2% (3) reporting frequent use, indicating limited trust in free VPNs for critical tasks.

Survey responses revealed specific use cases, such as P8 using free VPNs for "international shows" and P6 for "remote work," reflecting entertainment and professional needs. Non-users cited reasons like perceived illegality (P7: "Its illegal") or lack of need (P18: "Not really sure what it is").

Security-aware users showed a distinct pattern: 43.8% (7) used paid VPNs, 18.8% (3) used free VPNs, and 37.5% (6) used none [4]. They prioritized secure communications and restricted network access, using free VPNs only for low-risk tasks, as noted by "goofy-liskov": "a quick and easy solution" for non-critical scenarios.



(a) General Users



(b) Security-Aware Users

Figure 1: VPN usage distribution: general users (41.5% free, 17% paid, 41.5% none) versus security-aware users (18.8% free, 43.8% paid, 37.5% none), highlighting technical users' preference for paid services.

Figure 1 underscores security-aware users preference for paid VPNs, driven by reliability

concerns [16].

4.3 Trust and Understanding of Data Practices

Trust in free VPN providers was low among general users: 30.9% (29) reported minimal trust, 37.2% (35) were neutral, 16% (15) had moderate trust, and 1.1% (1) expressed complete trust on a 5-point scale. Understanding of data practices was limited, with 48.9% (46) unsure of providers handling, 19.1% (18) believing data is collected and shared with third parties, 19.1% (18) assuming collection without selling, and 9.6% (9) believing no data is collected.

Engagement with terms and conditions was minimal, with 46.5% (40) never reviewing them. Among the 34.9% (30) who did, comprehension varied: 24% (22) reported partial understanding (2–3/5), and 8.8% (5) reported full understanding (4–5/5). For example, P17, who reviewed terms thoroughly, noted a clear need for "A transparent privacy policy that states they don't log, track, or sell user data, a reputation and track record for privacy above all else, and a clear idea of how the provider makes their money without selling user data." to build trust.

Security-aware users exhibited lower trust, with 37.5% (6) rating trust at 1/5, 37.5% (6) at 2/5, and 25% (4) at 3/5, none exceeding neutral [4]. They assumed data collection, citing specific data types like "browsing history, connection logs" ("ecstatic-cori") and "traffic, fingerprints" ("infallible-lalande"). Their scrutiny of terms revealed dissatisfaction with vague policies, with "trusting-mahavira" questioning whether VPNs "truly keep no logs."

Figure 2 illustrates the trust gap, amplified by security-aware users awareness of data risks [8, 9].

4.4 Motivations for Choosing Free VPNs

Cost was the primary motivator for general users (73.5%, 61 responses), followed by ease of access (33.7%, 28), lack of awareness of paid options (14.5%, 12), trialing before purchase (14.5%, 12), and trust in providers (6%, 5). Among free VPN users, 87.2% (34 of 39) cited cost, reflecting economic constraints, particularly among younger users (e.g., P15: "Cost (free service)").

Survey responses highlighted economic drivers, with P13 noting free VPNs as a way to avoid "spending a lot of money on subscriptions." Lack of awareness was evident in P11s choice through their statement "lack of awareness about paid options."

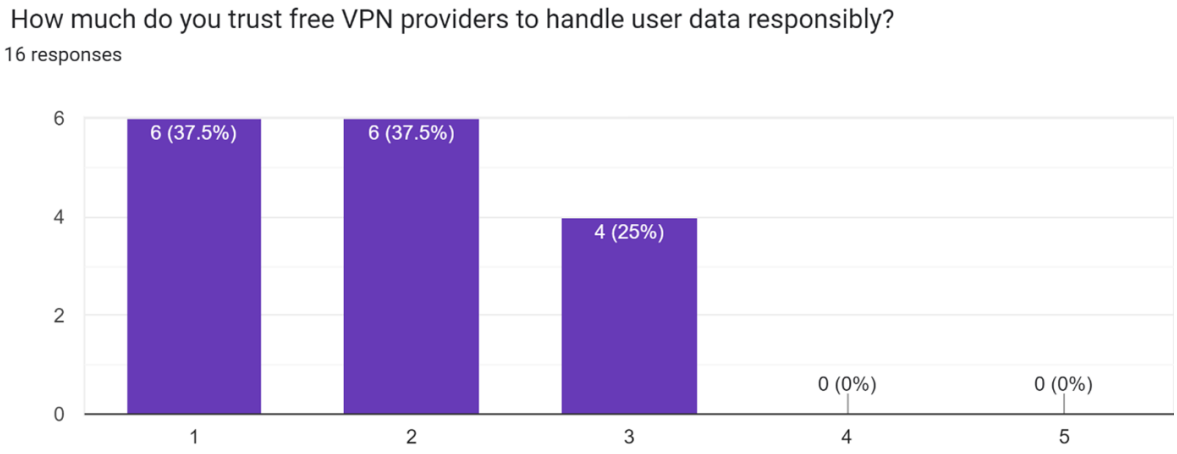
Security-aware users using free VPNs (3 respondents) cited convenience for non-critical tasks, with "goofy-liskov" emphasizing their use as a "quick solution" despite risks [4].

Table 1: Motivations for Choosing Free VPNs Among General Users

Motivation	**Frequency (%)**
Cost	61 (73.5%)
Ease of Access	28 (33.7%)
Lack of Awareness	12 (14.5%)
Trialing	12 (14.5%)
Trust in Provider	5 (6%)

Frequency of motivations for selecting free VPNs among general users, with cost dominating at 73.5%.

(a) General Users



(b) Security-Aware Users

Figure 2: Trust levels in free VPN providers: general users (30.9% minimal trust) versus security-aware users (37.5% at 1/5, none above 3/5), highlighting greater skepticism among technical users.

Table 1 underscores economic incentives, consistent with prior findings [13, 18].

4.5 Common Issues

General users reported frequent issues with free VPNs: slow speeds (51.2%, 44 responses), disconnections (40.7%, 35), invasive advertisements (23.3%, 20), privacy concerns (9.3%, 8), and malware or viruses (7%, 6). Among free VPN users, 58.9% (23 of 39) experienced slow speeds, and 46.2% (18) reported disconnections, impacting usability (e.g., P5: "Data speed gets reduced").

Survey responses emphasized performance issues, with P3 noting "frequent disconnections" and P9 citing "invasive advertisements" as deterrents.

Security-aware users echoed performance concerns but emphasized technical vulnerabilities: weak encryption (68.8%, 11 responses), malware risks (62.5%, 10), and data logging (93.8%, 15) and surprisingly all the participants were concerned with VPNs selling user data to third parties

(100 %, 16)[4]. Table 2 summarizes general users issues.

Table 2: Common Issues with Free VPNs

Issue	General Users (%)
Slow Speeds	44 (51.2%)
Disconnections	35 (40.7%)
Advertisements	20 (23.3%)
Weak Encryption	3 (3.2%)
Malware Risks	6 (7%)
Privacy Concerns	8 (9.3%)

The overlap in performance complaints suggests universal usability challenges, while security-aware users focus on encryption and malware reflects deeper risk awareness [20, 15].

4.6 Perceived Risks and Trust Factors

Data privacy was the primary concern for general users (35.9%, 33 responses), with P17 stating: "Everything you do through an untrustworthy free VPN should be expected to be monitored, tracked, and sold." Other risks included security vulnerabilities (15.2%, 14; P13: "Lack of security"), performance issues (10.9%, 10; P15: "Slow data"), scams (8.7%, 8; P11: "Scam"), and data breaches (6.5%, 6; P12: "Data hack").

Transparency was critical, with 37.2% (35) rating it "absolutely essential" and 30.9% (29) "very important." Open-ended responses emphasized clear policies (P17: "A transparent privacy policy"), better security (13%, 12; P11: "Better security"), and user-accessible data logs (8.7%, 8; P19: 'Making the data available to the user").

Security-aware users focused on data logging (93.8%, 15; "cranky-wilbur": "data collection, hidden tracking, selling user data"), weak encryption (68.8%, 11; "trusting-mahavira": "how strong and up-to-date the VPN encryption is"), and malware (62.5%, 10; "ecstatic-cori": "VPNs dont protect against malware") [4]. They demanded technical assurances: public audits (75%, 12), open-source code (68.8%, 11), and no-ads policies (50%, 8).

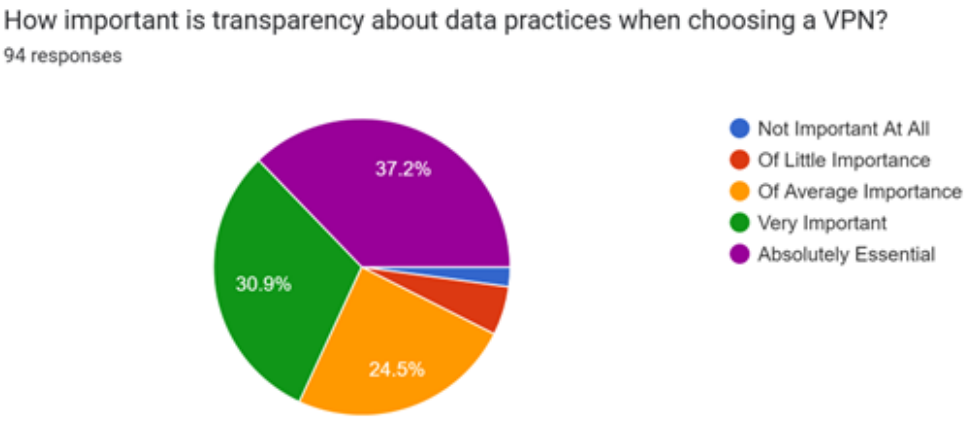
Figure 3 highlights the importance of transparency and privacy.

4.7 Additional Insights: Recommendations and Knowledge Gaps

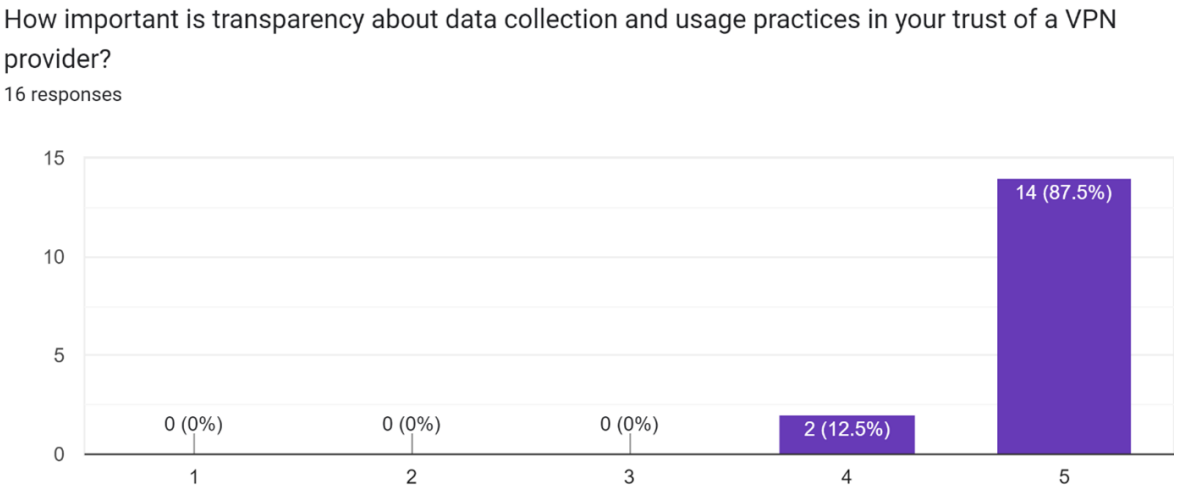
Security-aware users were reluctant to recommend free VPNs to non-technical peers, with 43.8% (7) rating it "very unlikely" and 25% (4) "unlikely," citing risks like "a false sense of security" ("interesting-buck") [4]. They emphasized security protocols and logging policies over ease of use ("cranky-wilbur").

General users showed limited awareness, with 13% (12) citing unfamiliarity with paid options and 48.9% (46) unsure of data practices. Responses like P18s ("not really sure what it is") and P23s ("no idea what a VPN is") highlight an education gap.

Security-aware users high VPN knowledge (75% at 4/5 or higher) shaped their concerns about data monetization ("funny-golick": "Free VPNs likely use your traffic and device information to sell to others") [4].



(a) General Users



(b) Security-Aware Users

Figure 3: Transparency in free VPNs (Rated "Absolutely Essential"): general users (37.2%) versus security-aware users (87.5%).

5 Discussion

The findings confirm a privacy paradox among general users: cost (73.5%) drives free VPN adoption despite low trust (45.8% "No tust and minimal trust") and poor understanding (35%, 1–2/5) [19, 13]. Security-aware users, aware of technical flaws like data logging (93.8%) and weak encryption (68.8%) [9, 15, 4], prefer paid VPNs (43.8%), illustrating knowledge-driven behavior.

The universal demand for transparency (37.2% general users, 100% security-aware users rating it 4/5 or higher) suggests providers could build trust through clear policies, audits, and open-source code [3, 1]. Limited engagement with terms (71%) and widespread uncertainty underscore an education gap [14, 19].

General users reliance on free VPNs for entertainment (52.6% browsing, 34.6% streaming) and avoidance of sensitive tasks (63.8%) reflect pragmatic but risky choices. Security-aware

users technical critiques and preference for paid VPNs suggest education could shift general users toward safer options [18, 17].

5.1 Limitations

The general user surveys skew toward younger participants (61.7% aged 18–24) may underrepresent older demographics VPN trust and usage patterns, limiting applicability to broader populations. The security-aware surveys small sample (16 participants) restricts statistical robustness, potentially missing nuanced technical perspectives. Self-reported data, particularly from general users, may reflect recall inaccuracies or social desirability bias, especially on sensitive topics like privacy concerns. Future studies should target balanced age distributions, expand the security-aware cohort, and incorporate objective measures, such as VPN log analyses or penetration testing, to validate user-reported issues [15, 20].

6 Conclusion

This study rigorously examines trust in free VPN services by comparing 94 general users and 16 security-aware users. General users, predominantly aged 18–24 (61.7%) and motivated by cost (73.8%), use free VPNs primarily for anonymous browsing (52.6%) and streaming geo-restricted content (34.6%), yet exhibit low trust (45.8% minimal) and limited understanding of data practices (47.8% unsure). Security-aware users, with advanced (50%) or expert (25%) cybersecurity skills, favor paid VPNs (43.8%) and critique free VPNs for specific vulnerabilities, including data logging and outdated encryption protocols [4]. The findings directly address the research questions:

- **Demographics and Usage**: Free VPN users are young and entertainment-driven, while security-aware users focus on secure communications for professional tasks.
- **Trust**: General users uncertainty contrasts with security-aware users informed skepticism about data handling and encryption weaknesses.
- **Motivations**: Cost drives general users, whereas security-aware users restrict free VPN use to low-stakes activities like casual browsing.
- **Issues**: Slow speeds (51.2%) and disconnections plague general users, while security-aware users highlight risks like unencrypted traffic.
- **Risks**: Both groups prioritize data privacy, with security-aware users pinpointing threats like third-party data sharing.
- **Recommendations**: Both groups steadily support transparency about the data practices.

Future research should develop targeted educational campaigns to improve general users understanding of VPN data practices, assess the viability of ad-supported VPN models that prioritize privacy, and evaluate the impact of mandatory third-party security audits on user trust [13, 21, 5].

References

[1] Hafiz Abbas, Nouman Emmanuel, Muhammad Faizan Amjad, Tayyaba Yaqoob, Mohammed Atiquzzaman, Zahid Iqbal, and Usman Ashfaq. Security assessment and evaluation of vpns: A comprehensive survey. *ACM Computing Surveys*, 55(13s):273:1–273:37, dec 2023.

[2] Abdulaziz Alshalan, Suman Pisharody, and Dong Huang. A survey of mobile vpn technologies. *IEEE Communications Surveys & Tutorials*, 18(2):1177–1196, 2016.

[3] E. Blancaflor, J. Armado, C. Cabral, E. Laurenio, and J. Salanguste. A comparative analysis of vpn applications and their security capabilities, 2024.

[4] Shetty Kurudunje Deekshith and Shetty Shitil. Free vpns and privacy: A survey of security-aware users. *GitHub Repository : KDShetty11/Free-VPNs-and-Privacy-A-survey-of-security-aware-users*, 2025.

[5] Anna Dutkowska-Żuk, Alison Hounsel, Angela Morrill, Amy Xiong, Marshini Chetty, and Nick Feamster. How and why people use virtual private networks. In *31st USENIX Security Symposium*, 2022.

[6] A. Erdoğan and D. Yızb. Virtual private networks (vpns): A survey, 2008.

[7] Matthias Fassl, Annalisa Ponticello, Andrzej Dabrowski, and Katharina Krombholz. Investigating security folklore: A case study on the tor over vpn phenomenon. In *Proceedings of the ACM Human-Computer Interaction*, 2023.

[8] Muhammad Ikram, Narseo Vallina-Rodriguez, Save Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. An analysis of the privacy and security risks of android vpn permission-enabled apps. In *Internet Measurement Conference*, 2016.

[9] Mobin Tahir Khan, Joseph DeBlasio, Geoffrey M Voelker, Alex C Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. An empirical analysis of the commercial vpn ecosystem. In *Internet Measurement Conference*, 2018.

[10] Sachin Khanvilkar and Ashfaq Khokhar. Virtual private networks: An overview with performance evaluation. *IEEE Communications Magazine*, 42(10):146–154, 2004.

[11] Maryam Mehrnezhad, Kevin Coopamootoo, and Elham Toreini. How can and would people protect from online tracking? *Proceedings on Privacy Enhancing Technologies*, 2022(1):105–125, 2022.

[12] L. Moore and T. Mori. Vpn awareness and misconceptions: A comparative study in canadian and japanese contexts, 2024.

[13] Maria Namara, David Wilkinson, and Kelly Caine. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. *Proceedings on Privacy Enhancing Technologies*, 2020(1):83–102, 2020.

[14] B. H. Priyanka and Ravi Prakash. A critical survey of privacy infrastructures. *CoRR*, abs/1512.07207, 2015.

[15] Rishab Ramesh, Leonid Evdokimov, Daniel Xue, and Roya Ensafi. Vpnalyzer: Systematic investigation of the vpn ecosystem. In *n/a*, 2022.

[16] Rishab Ramesh, Aashish 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*, 2023.

[17] Kamalnath Kishor V Singh and Harshita Gupta. A new approach for the security of vpn. In *Second International Conference on Information and Communication Technology for Competitive Strategies*, 2016.

[18] Natthaphon Sombatruang, Takuya Omiya, Daisuke Miyamoto, M Angela Sasse, Yoshinari Kadobayashi, and Marie Baddeley. Attributes affecting user decision to adopt a virtual private network (vpn) app. In *n/a*, 2020.

[19] Peter Story, Daniel Smullen, Yixin Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021(4):308–333, 2021.

[20] Jack Wilson, David McLuskie, and Ewan Bayne. Investigation into the security and privacy of ios vpn applications. In *15th International Conference on Availability, Reliability and Security*, 2020.

[21] Zhipeng Xu and Jin Ni. Research on network security of vpn technology. In *International Conference on Information Science and Education*, 2020.