VPN Awareness and Misconceptions: A Comparative Study in Canadian and Japanese Contexts

Lachlan Moore
Waseda University, NICT
lachlan.moore@nsl.cs.waseda.ac.jp

Tatsuya Mori
Waseda University, NICT
mori@nsl.cs.waseda.ac.jp

***Abstract*—This study delves into the utilization patterns, perceptions, and misconceptions surrounding Virtual Private Networks (VPNs) among users in Canada and Japan. We administered a comprehensive survey to 234 VPN users in these two countries, aiming to elucidate the motivations behind VPN usage, users' comprehension of VPN functionality, and prevalent misconceptions. A distinctive feature of our research lies in its cross-cultural comparison, a departure from previous studies predominantly centered on users within a Western context. Our findings underscore noteworthy distinctions among participant groups. Specifically, Japanese users predominantly employ VPNs for security purposes, whereas Canadian users leverage VPNs for a more diverse array of services, encompassing privacy and access to region-specific content. Furthermore, disparities in VPN understanding emerged, with Canadians demonstrating a superior grasp of VPN applications despite limited technical knowledge, while Japanese participants exhibited a more profound understanding of VPNs, particularly in relation to encrypting transmitted traffic. Notably, both groups exhibited a constrained awareness regarding the data logging practices associated with VPNs. This research significantly contributes to the broader comprehension of VPN usage and sheds light on the cultural intricacies that shape VPN adoption and perceptions, offering valuable insights into the diverse motivations and behaviors of users in Canada and Japan.**

I. Introduction

Virtual Private Networks (VPNs) have become an essential tool for protecting online privacy. By encrypting communications between users and intermediate servers, VPNs play a crucial role in protecting sensitive data [42], [13]. Initially used in professional environments [9], VPN technology has been widely adopted and commercialised, with a market value estimated at over 44 billion USD by 2022 [36]. However, despite their apparent benefits, VPNs are not without their limitations. Previous studies of commercial VPN ecosystems have shown that many providers unintentionally leak data, undermining their promise of user anonymity [23], [27], [34]. In addition, some VPNs deliberately collect user data for commercial purposes [4], while others are required to do so by law [20]. Nevertheless, VPNs offer significant benefits, such as circumventing Internet censorship [43], accessing geographically restricted content [22], and mitigating the vulnerabilities inherent in unsecured Internet connections [37]. The reasons why individuals use VPNs vary; people in countries with limited internet freedom may use VPNs primarily to circumvent censorship [17], while expatriates may use them to access content from their home countries.

Numerous studies have delved into the technical limitations of VPNs [44], [18], [23], [34], yet research on users' perceptions and understanding of VPNs remains limited. Much of the existing research has focused on specific subsets of Internet users [38], [30], [3], [11], [35] or has broadened its scope beyond VPNs [39], [16]. To bridge this gap, it is imperative to incorporate insights from a globally diverse user base, recognizing the impact of cultural differences on aspects such as password memorability [8]. A comprehensive understanding of VPN users' viewpoints across varied geographical and cultural backgrounds is essential, particularly in light of previous research highlighting the influence of cultural factors on the adoption of security tools [1]. This inclusive approach is pivotal for shaping future research endeavors and aiding developers in comprehending the diverse requirements, preferences, and application contexts of these heterogeneous user groups.

To better understand VPN usage and perceptions, we conducted an extensive user study with 234 participants, primarily from Canada and Japan. These two countries offer contrasting cultural and technological landscapes, providing a unique perspective that our team, with direct experience in these regions, can fully appreciate. Our methodology included an extensive online survey targeting both current and former VPN users. The survey was carefully designed to provide detailed insights into participants' understanding, practical applications, and emotional attitudes toward VPN technology. The study is structured to address three key research questions, each designed to uncover different facets of VPN usage:

RQ1: Why are people using VPNs?
RQ2: What do people believe about VPNs?
RQ3: What are the common misconceptions around VPNs?

Symposium on Usable Security and Privacy (USEC) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-5-2
https://dx.doi.org/10.14722/usec.2024.23045
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

The findings from our survey, elaborated in Section 4, reveal significant variations in the perceptions and usage of VPNs across distinct cultural landscapes. The insights gleaned from participants in Japan and Canada, in particular, display starkly differing viewpoints.

Japanese participants predominantly associate VPNs with the enhanced security provided by encrypted connections. Their emphasis lies squarely on the protective benefits these services offer, highlighting an acute awareness and concern for security within the digital environment. This perspective underscores a focused approach towards VPNs, primarily as a tool for safeguarding online interactions. In contrast, Canadian participants exhibit a more expansive understanding and application of VPNs. Beyond acknowledging the security benefits, they also appreciate additional features such as enhanced privacy, the ability to access region-specific content, and circumventing geo-restrictions. This broader view reflects a more comprehensive understanding of VPNs, encompassing various aspects beyond mere security. Canadian respondents appear to leverage VPNs for a wider array of purposes, indicating a richer, more multifaceted grasp of the technology.

This divergence in perspectives between the two groups not only highlights cultural differences in the approach to digital privacy and security but also suggests varying levels of familiarity and sophistication in VPN usage. The contrast between the Japanese focus on security and the Canadian holistic view of VPNs underscores the importance of considering cultural context in the development and marketing of these technologies.

Despite the cultural disparities identified, a notable commonality emerged from our study: participants from both Japan and Canada harbor similar misconceptions about online data collection practices and the policies of VPN services. This confusion predominantly revolves around how VPNs process and manage user data, leading to misconceptions about the actual degree of privacy and anonymity that these services provide.

This finding is particularly significant as it directly influences users' realistic expectations and trust in VPN services. Many users may overestimate the privacy capabilities of VPNs, potentially leading to a false sense of security and anonymity. This gap in understanding highlights the need for enhanced public education and awareness regarding the functionalities and limitations of VPNs, especially in relation to their data management practices and privacy policies.

Enhancing comprehension in this domain empowers users to make more informed decisions regarding their privacy and data security. Educating users about the nuances of VPN technology, addressing specific misconceptions within various cultural contexts, is crucial for fostering a safer and more privacy-conscious online environment.

The paper is organized as follows: Section 2 provides background information and explores related works on VPNs. Section 3 presents an overview of the methods employed in constructing our study. The results of the study are detailed in Section 4, while Section 5 delves into a discussion of the findings, limitations, and outlines potential avenues for future research. Section 6 serves as the conclusion of our study. Furthermore, the design of our survey is detailed in the Appendices accompanying this work.

II. Background and Related Work

In this section we describe the background of VPNs and related studies, including work on the adoption of privacy tools, studies of the VPN ecosystem, cross-cultural studies of misconceptions, and surveys of sub-populations of VPN users.

Since their inception in 1996 by Microsoft as a secure communications protocol primarily for enterprise networks [28], VPNs have undergone significant evolution. Crawshaw et al. provide a comprehensive analysis of this evolution and explore the reasons for these significant changes [9]. Originally designed to connect separate enterprise networks, VPNs have been commercialised and are now widely available to the average user. Modern VPNs offer a range of functions beyond their original scope, including privacy, censorship bypass and remote access capabilities [37].

The popularity of VPNs has skyrocketed due to a number of factors. One influential factor is the increasing prevalence of Internet censorship. This is exemplified by Pakistan's move to block pornographic content in 2011 [24] and the recent implementation of Bill C-11 in Canada [31]. Coupled with the general trend towards monitoring Internet traffic [41] and the shift to remote working catalysed by the COVID-19 pandemic [13], the demand for VPNs has never been greater.

In the face of this burgeoning popularity, commercial VPNs have provoked a range of responses. Different countries have responded differently to the public's increasing use of VPNs. In four countries, the use of VPNs is completely illegal. A further six have imposed severe restrictions on their use; China and Russia, for example, only allow government-approved VPNs [29]. Unfortunately, these approved VPNs often come with strings attached, such as agreements for backdoors and data logging, effectively undermining their role in protecting privacy. It's also worth noting that India recently introduced a mandate requiring VPN providers to log user data [20]. As VPNs continue to grow in use and popularity, understanding the additional users of VPNs, the issues and restrictions they face on a ever increasing restricted Internet remains a dynamic and contentious issue.

A. Related Work

Analysis of VPN Ecosystems With the growth and popularity of the commercial market for VPNs, so have the studies of the commercial VPN ecosystem. VPN traffic was found to even take up to 2.6% of all traffic within an Internet Service Provider (ISP) [27]. These works have found that many VPN providers leak user data through a variety of means [23], [27], [34]. There are even cases of commercial VPNs leaking traffic during tunnel failure and even some VPNs leaking DNS traffic [34]. Although these studies are able to measure the overall ecosystem of VPNs, they are unable to show why on a user level people are adopting VPNs.

Adoption of Privacy Tools Prior research has explored reasons behind adopting privacy tools, including VPNs. For instance, a demographically-stratified survey in the United States with 500 participants highlighted misconceptions about VPNs, with users often mistaking them for security solutions [39]. Interestingly, despite having experience with VPNs as a tool, misconceptions still remained common. Similarly, Namara et al. [30] conducted a survey of 90 tech savvy users, to identify common attributes that users had when adopting a VPN. They find that users of VPNs fall into two categories, those motivated by emotional considerations and those motivated by practical considerations. They noticed that people motivated primarily by emotions were more likely to continue using a VPN than those who were using a VPN for practical needs, especially once those needs are met. Moreover, Sombatruang et al. [38] interviewed 32 users from the UK and Japan, finding price and reviews as significant factors impacting VPN adoption.

User Studies on VPNs There are various works regarding users' thoughts and perspectives on VPNs. Dutkowska-Zuk et al. [11] conducted a study of 729 VPN users, of both students and general users in the US, to explore why they use a VPN, how they use a VPN, and if they understood the privacy risks introduced by VPNs. They found various differences in use cases between students and the general population, with the students being more concerned with content access than privacy, as well as students using VPNs less frequently. Despite the differences in use cases they also found that both groups had a low understanding of data collections risks associated with VPNs. Binkhorst et al.[3] interviewed 18 expert and non-experts users of VPNs in a corporate context, they found that despite being experts in a field experts and non-experts have similar mental models of VPNs. Also, finding that experts tend to have false perspectives on security aspects of VPNs. Ramseh et al. [35] conducted a survey of 1,252 VPN users in the US and nine VPN providers on motivations, needs, threat model, and mental model of users, and the key challenges and insights from VPN providers. Discovering that users rely on VPN review sites that VPN providers admit are mostly motivated by money. They also similarly find that users have a flawed mental model about data collected by VPNs, as well as how much protection VPNs provide.

While preceding research has provided valuable insights, it exhibits limitations in comprehensively understanding the diverse user base of VPNs. This study addresses this gap by conducting an in-depth examination of the perspectives and understandings of VPN users originating from two culturally distinct societies, as delineated by Hofstede's cultural dimensions [15]. In our approach, we fostered creativity among users in articulating their thoughts and perceptions, thereby enhancing the depth of our inquiry. To the best of our knowledge, our work represents the first attempt to systematically consider and compare the cultural variations among VPN users.

Given the rapid expansion of the VPN ecosystem, our research is poised to contribute significantly by elucidating the needs and considerations of the diverse global VPN user population. Furthermore, it offers valuable insights into the challenges faced by users worldwide in comprehending and navigating security and privacy tools. This study, therefore, not only fills a critical void in existing literature but also lays the groundwork for a more nuanced understanding of the evolving landscape of VPN usage on a global scale.

III. Methodology

In this section, we provide a thorough overview of our survey, covering aspects such as the development process, content, and structural arrangement. We delve into the specific focus of each segment and explain our approach to coding open-ended questions. In conjunction, we present an understanding of our participant demographics and detail the recruitment process. Finally, we outline the ethical considerations that were consistently followed throughout the course of the study.

A. Survey Design

We believe that an effective survey requires the incorporation of the multiple perspectives inherent in the cohort under study. To achieve this goal, the genesis of our survey involved several small-scale investigations that incorporated a diverse participant base prior to the final large-scale iteration. In our nascent iteration, we drew inspiration from previous surveys focused on VPN users and used them as a baseline [34], [38], [11]. Our team then engaged in dialogue to refine the survey's overall structure, question wording, and question types, making essential changes to align with our research objectives. Once we were satisfied with the initial version, we conducted a pilot survey with five participants drawn from our personal networks of friends and family. The review of the quality of the results and the aggregated feedback from the participants spurred the generation of suggested changes and additions. These suggestions were vetted within our team before being incorporated into the survey.

Our methodology employed an iterative framework comprising cycles involving pre-survey preparation, results analysis, feedback incorporation, and subsequent discussion. Significantly, each cycle featured an expanding participant cohort, beginning with an initial five participants, progressing to nine, and ultimately reaching twenty in the concluding survey iteration. This deliberate increase in participant numbers was accompanied by a strategic effort to enhance heterogeneity, considering factors such as age, background knowledge, and cultural influences.

The final iteration of our survey consists of 26 questions spread across five different sections. Embedded within the survey are four unique questions designed to be posed only to a specific subset of participants; these questions can only be accessed through specific participant responses. The range of question types within the survey includes primarily multiple choice questions, supplemented by three open-ended questions and a single open-ended question that asks respondents to visually illustrate their thoughts. To avoid the onset of respondent fatigue, we deliberately limited the inclusion of open-ended questions in our survey. In addition, we carefully avoided

Gender	Canada	Japan	Age	Canada	Japan	Education Level	Canada	Japan
Male	47	65	18 - 25	27	8	High School	13	28
Female	42	33	26 - 35	35	28	Technical certificate	2	4
Non-binary/Other	4	0	36 - 45	21	37	Undergraduate degree	48	33
Prefer not to say	2	2	46 - 55	6	22	Post-graduate degree	12	3
			56 - 65	3	4	College diploma	14	25
			Over 65	0	0	Other	2	2
			Prefer not to say	3	1	Prefer not to say	4	5

TABLE I: Demographics of all 195 analyzed participants.

Location of Residence	#	Nationality	#		#		#
Japan	100	Japan	99	Pakistan	1	Syrian Arab Republic	1
Canada	95	Canada	81	Philippines	1	United Kingdom of Great Britain and Northern Ireland	1
		Russian Federation	3	Republic of Moldova	1	Benin	1
		Italy	1	India	1	China	1
		Nigeria	1	South Korea	1	Prefer not to say	1

TABLE II: Residence and identified Nationalities of all 195 participants.

Background in IT or related field	Canada	Japan	Consider themselves knowledge in IT or related field	Canada	Japan
Yes	27	25	Strongly disagree	4	20
No	68	75	Somewhat disagree	10	26
			Neither agree nor disagree	12	22
			Somewhat agree	59	30
			Strongly agree	10	3

TABLE III: Background and knowledge levels of all 195 analyzed participants.

double-barreled questions, negatively worded questions, and questions with any semblance of bias, in accordance with established HCI research methodologies [25].

Our first section was tasked with collecting demographic data, including variables such as age, gender, location, and identified nationality. Then we proceeded with a quality check, validating that the respondent's had previous or current exposure to VPNs. This was followed by a section that elicited information about the participant's VPN usage, exploring the motivations behind usage, the type of VPN used, and the frequency of VPN usage. The following section measured participants' understanding of VPNs. We solicited responses to two open-ended questions, one in written format and another encouraging a graphical representation of their understanding of a VPN. In addition, we presented multiple choice questions probing common aspects of VPN usage. In the final section of the survey, we explored participants' trust in VPN vendors, ISPs, and network administrators. To capture levels of trust without ambiguity, we used a five-point Likert scale [26].

We note that our survey was designed to be accessible in both English and Japanese, with the original version created in English. The translation process was facilitated by team members who were fluent in both languages. To ensure the accuracy of the translation, it was carefully reviewed several times by multiple members of our team.

B. Participant Recruitment and Demographic Overview

Leveraging Prolific, a widely used global online participant recruitment tool, and Lancers, a Japanese crowdsourcing platform, we strategically engaged 100 participants from Canada through Prolific and an additional 103 participants from Japan via Lancers. The selection of Prolific was driven by its capacity to ensure a gender-balanced recruitment process. Recognizing that Prolific had fewer than 100 active Japanese users, we opted for Lancers to augment our Japanese participant pool. Additionally, 31 participants were recruited from our team's acquaintances, friends, and family members. However, it is crucial to note that these 31 responses were excluded from the final study analysis and solely employed for testing purposes. Additionally, five participants from Canada and three participants from Japan did not pass the quality check and were thus excluded, resulting in 95 valid participant responses from Canada and 100 from Japan.

The decision to focus on participants from Canada and Japan is underpinned by the lived experiences of key team members in these respective countries. The nuanced cultural insights and contextual understanding drawn from their personal experiences uniquely position our team to navigate and interpret the intricacies of the cultural disparities observed in the study. This strategic approach enhances the depth and authenticity of our research, allowing us to not only collect data but also to glean meaningful insights grounded in the cultural fabric of Canada and Japan. By incorporating team members with direct ties to these countries, our study gains a richer dimension that adds depth and credibility to the interpretation of the findings.

Table I provides a summary of the demographics of the 195 participants analyzed. On average, Japanese participants were slightly older than their Canadian counterparts. In addition, the gender distribution of the Japanese participants was skewed toward males. The study also included a small number of

participants who lived outside of Canada and Japan. In addition, not all participants identified their nationality as Canadian or Japanese. Table II shows these nationality distributions. Table III provides an overview of participants' background knowledge in information technology (IT) and related fields. The majority of participants from both countries reported no background in these areas. However, it is noteworthy that Canadian participants rated their IT knowledge significantly higher than their Japanese counterparts.

C. Analyzing Open-Ended Responses and Multilingual Considerations

To analyse open-ended questions, including those pertaining to participants' drawings, we employed a codebook approach as outlined by Thematic Analysis [6]. Our team systematically reviewed all responses, establishing categories to encompass diverse response types. Definitions and themes corresponding to these categories were then formulated to serve as the foundation for response categorization. Any responses defying straightforward categorization underwent collaborative discussions, leading to refinements in preliminary definitions and themes. This iterative process continued until the number of responses that resisted categorization was significantly reduced. Refer to Table IV for an overview of definitions and major themes associated with each code.

Because our survey was distributed in both English and Japanese, the open-ended responses in Japanese required translation into English to facilitate coding analysis. Translation of written responses from Japanese to English was accomplished by utilizing DeepL [10]. In addition, longer responses were reviewed by bilingual team members to confirm meaning fidelity. Due to inherent language differences, the majority of Japanese responses were reviewed. For the question regarding participants' drawings, analysis was conducted by team members who were proficient in both English and Japanese. Since most of the drawings contained no textual content, categorization was relatively straightforward. However, where Japanese text was present in participants' responses, native speakers reviewed the meaning to ensure consistency.

D. Ethical considerations

In accordance with our Institutional Review Board (IRB) guidelines, we conducted a thorough evaluation of our user study, which was determined to fall into an exempt category, eliminating the need for further IRB procedures. We also prioritised privacy by not collecting any unnecessary personal information. In addition, our survey on the Qualtrics platform begins with an informed consent page, ensuring that each participant explicitly agrees to participate in the study. We also included demographic questions with an option for respondents to select 'Prefer not to say'. No identifying information was collected from participants, and all response data is managed solely by our team members.

Participants' compensation varied depending on their location. To ensure a consistent quality of responses, we devised compensation criteria that considered both the time and effort needed to finish the survey and the minimum wages of participants' respective locations. Our survey is estimated to take between 8–10 minutes to complete. Based on the wages per country [33], [19], Canadian participants were compensated 2.5 CAD, while Japanese participants were compensated 100 JPY.

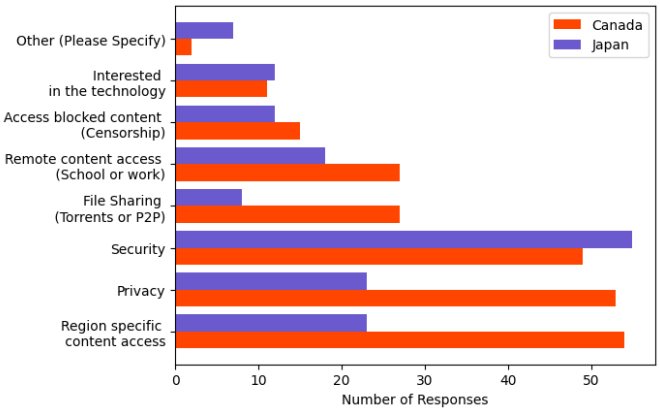


Fig. 1: Why do/did you use a VPN? Responses collected from participants.

IV. Results

In this section, we present and analyze the findings of our survey, with a primary focus on the reasons behind VPN usage, participants' understanding of VPNs, and the prevailing misconceptions surrounding VPNs.

A. Usage of VPNs

We explore the reasons behind participants' use of VPNs. We allowed participants to choose multiple reasons for their VPN use, which categories are laid out in Figure 1. In total the most popular reason to use a VPN was security (53% n=195), followed by region specific access to content (39% n=195) and privacy (39% n=195). Although, the popularity of region specific access to content and privacy was mostly prioritized by respondents based in Canada. With those participants located in Canada ranking region specific content access (57% n=95), privacy (56% n=95), then security (52% n=95) as the most prevalent reasons for VPN use. In comparison participants located in Japan were much more concerned with security (55% n=100) reasons for VPN use. Additionally, privacy (23% n=100), region specific content access (23% n=100), and file sharing (8% n=100) were considerably less popular among respondents based in Japan than ones based in Canada. Unsurprisingly, both groups of participants ranked their use case of a VPNs for access to blocked content (14% n=195) rather low. This can be attributed to the high level of Internet freedom enjoyed in both Canada and Japan [17].

It is noteworthy that among participants whose location of residence and nationality differed, the most prevalent reason for using VPNs was to access region-specific content (24% n=46). One possible explanation for this correlation is the unique circumstances faced by these users, such as living

Q16 - What do you think a VPN is? Please describe it the best you can.		
Code	Key Themes	Definition
Content Access	accessing data, remote connection	A way to access content that is not available or is secured without a specific connection.
Privacy tool	tracking, traffic, encryption, monitoring, anonymize, hiding activity	Keeps one's personal activity or data private.
IP masking	IP address, location, region, spoofing	Obscuring IP being used to another IP that is not the original being used.
Secure connection	security, encryption, tunneling	Protection of users system or network from harm, theft, and unauthorized use.
Separate Network	network, buffer, sever	A completely different network connection separate from the local network and internet.
Other	other, acronyms, not sure, non answer	Other responses that are not categorized in above, includes simple definitions or responses that are 'not sure.'
Q17 - Use the following to provide a drawing to explain how you think a VPN works.		
Code	Definition	
Intermediate Connection	Depiction of an intermediate server between the connection and VPN or user.	
Shield	Depiction of a VPN as a wall or shield that is separating the host computer from the outside network.	
Addition of VPN	Depiction of a VPN being added to the connection. This may involve a new IP address, location or general security being added to the connection.	
Tunnel	Depiction of the VPN as a tunnel, which surrounds the data being sent and received in a connection.	
Location access	Depiction of a VPN as a way to access a different location from where the user is located.	
Other	Other responses that are not categorized in above, includes simple definitions or responses that are 'not sure.'	

TABLE IV: Codes created by our team for the data categorization of questions 16 and 17.

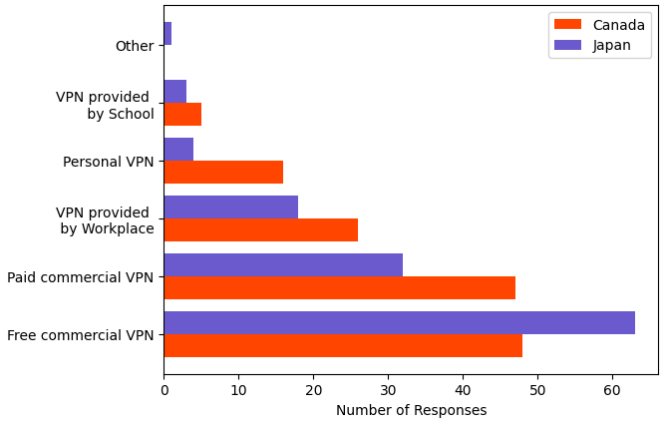


Fig. 2: What type(s) of VPNs do you use? Responses collected from participants.

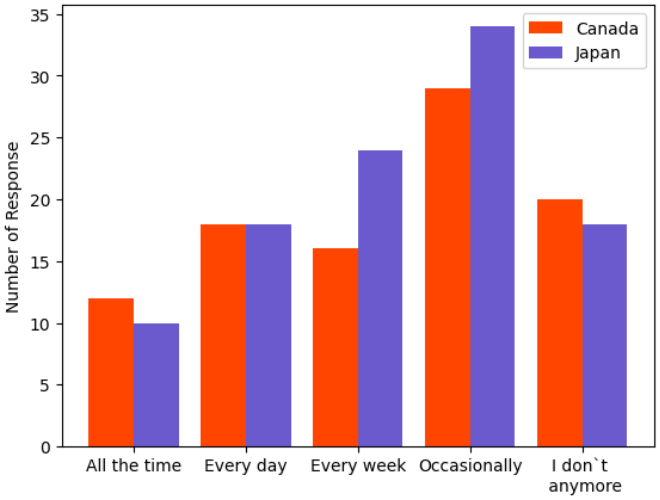


Fig. 3: How often do you use a VPN? Responses collected from participants.

abroad and desiring access to content that is specific to their home country.

Moving forward, we investigate the types of VPNs that participants use. Similarly to the previous section, participants were able to choose multiple responses regarding the type(s) of VPNs they use. Shown in Figure 2 Commercial VPNs, both free (57% n=195) and paid (41% n=195), were the most popular VPN types among participants. Participants in Canada preferred to use free commercial VPNs (51% n=95) by a close margin to paid commercial VPNs (49% n=95). Of these VPNs, two paid VPN services were the most popular choices NordVPN (28% n=95), followed by ExpressVPN (20% n=95). In contrast to participants located in Canada, participants in Japan prioritized the use of free commercial VPNs (63% n=100). Of these NordVPN (22% n=100) remained the most popular choice, followed by Tunnelbear (9% n=100), which does offer a free service. Additionally, younger respondents between the ages of 18-35, located in both countries, responded mostly NordVPN (27% n=116) and ExpressVPN (16% n=116) as their choice of VPN. This finding could correlate to the younger demographic's tendency to consume media such as YouTube, where VPNs, such as NordVPN and ExpressVPN are aggressively advertised [2].

Figure 3 illustrates the frequency of VPN usage reported by participants. The majority of participants indicated that they only used a VPN occasionally (32% n=195). Interestingly, the overall patterns of VPN usage were similar for participants from both Japan and Canada. With only slight variations in stopping VPN usage (19% n=195), usage every week (21% n=195), and usage all the time (11% n=195). Approximately 20% of the participants stated that they no longer use a VPN. In Canada, the reasons cited for discontinuing VPN usage were no longer having a need (60% n=20) or not using it frequently enough (25% n=20). On the other hand, participants in Japan stopped using VPNs due to insufficient usage (50% n=18) or no longer having a need for it (100% n=8).

Table V depicts the distribution participants' age at the time of their initial VPN usage. It reveals that Canadian participants tended to start using VPNs at younger ages compared to their Japanese counterparts. The majority of participants in Canada first used a VPN between the ages 18-25 (39% n=95) and ages 26-35 (25% n=95). In comparison participants located in Japan primarily first used a VPN at slightly older ages, between 36-45 (39% n=100) and 26-35 (34% n=100). We see this trend of a younger experience of VPN usage continue with almost 20% of Canadian participants having used a VPN before the age of 18 (19% n=95). In fact only a couple participants in Japan first used a VPN before the age of 18 (2% n=100).

Slightly more than half of the total 195 participants, 49

	Under 18	18-25	26-35	36-45	46-55	56-65	Over 65	Prefer not to say
Canada	18	37	24	12	2	0	0	2
Japan	2	15	34	39	6	4	0	0
Total	20	52	58	51	8	4	0	2

TABLE V: When did you first start using a VPN? responses collected from participants.

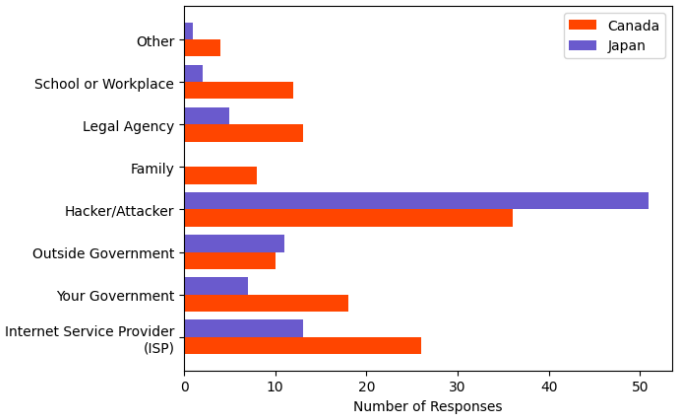


Fig. 4: Who are you trying to protect your browsing data from? Responses collected from participants who answered 'Yes' to using a VPN to secure their browsing activity (59% n=195).

from Canada and 67 from Japan, indicated that they utilized VPNs to enhance the security of their browsing activities. The distribution of participant responses regarding the entities they aimed to safeguard their data from is presented in Figure 4. Notably, participants from both Canada (75% n=49) and Japan (76% n=67) expressed a strong desire to protect their data from hackers, emerging as the primary concern for both groups. The next commonly selected entity for data protection, as identified by participants from both countries, was their ISP, with Canadian participants (53% n=49) and Japanese participants (19% n=67) showing particular apprehension about safeguarding their data from ISPs. Interestingly, only participants from Canada (16% n=49) expressed concerns about securing their data from family members. Indicating a potential cultural difference between the two groups in which groups they are more willing to share information with. About the same number of participants in both groups wished to keep their data from an outside government, the participants from Canada (37% n=49) were more concerned about their own government accessing their data than participants in Japan (10% n=67).

In summary, participants from Japan exhibited a heightened level of apprehension regarding unauthorized data access by malicious actors, leading them to employ VPNs as a proactive safeguard against such threats. In contrast, participants from Canada expressed a wider array of concerns and demonstrated diverse preferences in terms of the entities they sought protection against through VPN utilization. Moreover, both groups primarily reported to use VPNs for security purposes, while Canadian participants also utilized VPNs for additional purposes such as accessing restricted content and preserving privacy.

B. Beliefs of VPNs

We look into participants' beliefs of VPNs by asking them about their individual understanding of what they think a VPN is. Figure 5 shows the distribution of these responses, which were coded by our team. Participants in Canada primarily understood VPNs a tool for IP masking (31% n=95), a privacy tool (25% n=95), followed by a secure connection (19% n=95). A few participants believed that a VPN was for content access (8% n=95), or a separate network (8% n=95). Fewer respondents in Canada were categorized as others (8% n=95) and of these two participants were unable to describe what a VPN is. Participants in Canada demonstrated a solid belief of VPNs' purposes, often responses contained information about what the VPN was being used for. For example, a participant in Canada describes a VPN as a tool for disguising their IP and changing their perceived location:

> **P73**: 'It's a tool that disguises your IP address allowing you to anonymously browse online, it also doesn't save any of your information. The only people who can still see your activity is your internet provider. It can make you appear to be somewhere else.'

In comparison, over a third (37% n=100) of the participants in Japan overwhelmingly described a VPN as being used for a private or secure connection. Often including references to increased security or the encryption of traffic between destinations. This is a typical translated response by a participant in Japan describing a VPNs use as a encrypted connection:

> **P183**: 'VPNs are used to encrypt communications over the Internet to enhance security and protect user privacy.'

Although, the next most common response, just under a fifth (18% n=100) of participants in Japan, were in the other section which included mostly responses that were unable to answer the question or just expanded the VPN acronym. The subsequent prominent responses from participants in Japan included the utilization of VPNs for privacy (15% n=100), establishing a separate network (14% n=100), accessing restricted content (10% n=100), and masking their IP addresses (6% n=100).

Figure 6 displays the distribution of coded responses to our open-ended question where users are prompted to answer by drawing out their thoughts to explain how they think a VPN works. Over 40% of participants (46% n=95) in Canada responded by creating a depiction of a connection with the VPN as an intermediate between the client and server. This was followed by other (23% n=95) and then location access (15% n=95) being the next common coded response. Fewer

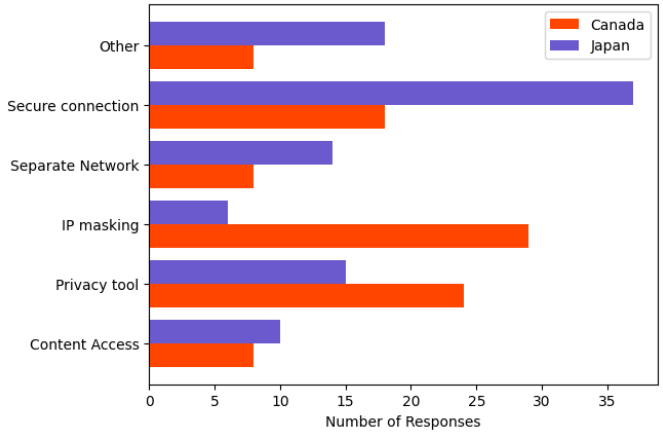


Fig. 5: What do you think a VPN is? Please describe it the best you can. Response coded.

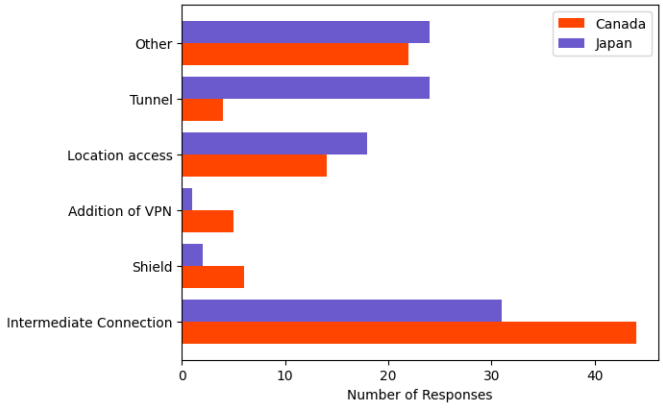
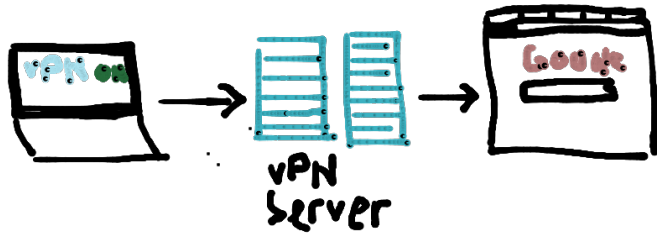
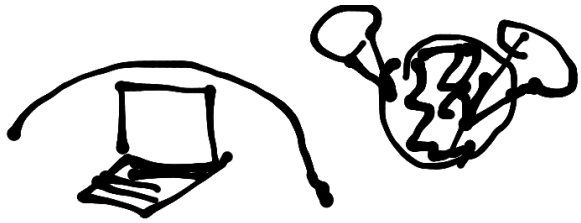


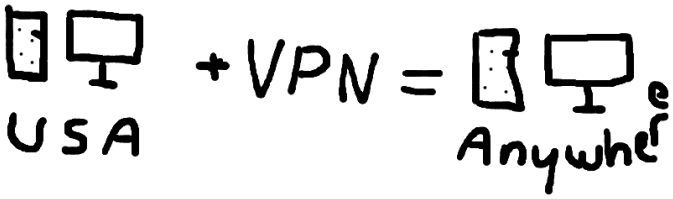
Fig. 6: Use the following to provide a drawing to explain how you think a VPN works. Can be any format. Responses coded.



(a) Example of a 'Intermediate Connection' coded drawing. Response from P82.



(b) Example of a 'Shield' metaphor coded drawing. Response from P95.



(c) Example of a 'Addition of VPN' coded drawing. Response from P8.

Fig. 7: Three examples of participants located in Canada drawings of how a VPN works. (a) Intermediate Connection, (b) Shield, and (c) Addition of a VPN.

participants responded with depictions of VPNs as shields (6% n=95), an addition to a connection (5% n=95), and then a tunnel (4% n=95). Figure 7 depicts two examples of participants from Canada's drawings of how they think a VPN works. A good representation, shown in Figure 7a, displays the common approach taken by Canadian participants, portraying a VPN as an intermediary connection. Typically, one side of the drawing displays the user's device, connected to the Internet, and further linked to the VPN, which is symbolized as a server or node positioned centrally within the connection. The connection then proceeds to its ultimate destination, depicted as a web page. Occasionally, participants included their ISP within the connection or even depicted the final connection taking place in a different location or with a distinct IP address. The depictions made by users of an intermediate connection often display a strong understanding of the connection structure of the VPN. Although, these representations often fall short of the encryption and decryption process carried out between the host machine and the VPN server. Another example is displayed in Figure 7b where the VPN is depicted as a 'shield' or 'barrier'. In this depiction, the participant's device is shown on the left side of the drawing, and is being covered by a barrier. On the right side, a globe is depicted with two distinct locations marked. It can be inferred that these two locations represent the VPN's capability to enable location spoofing for the user, allowing them to appear as if they are accessing the internet from different geographical locations while their device is protected by this shield. In contrast to the intermediate connection representations, the shield examples fail to portray the connection process of a VPN, indicating a lack of understanding among these participants regarding how the connection actually works. Figure 7c illustrates the inclusion of VPN code as an example. The depicted device is labeled as being located in the United States initially. After the VPN is added, the device's location becomes unrestricted. While this example showcases the functionality of a VPN, it does not provide insight into how the VPN accomplishes this task. Consequently, it indicates that similar coded representations of VPN reflect limited understanding of the underlying mechanisms of a VPN.

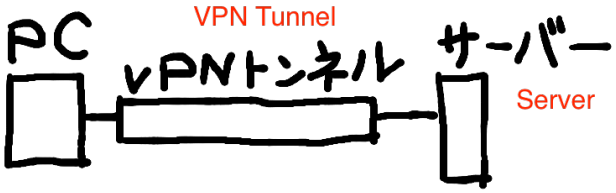
Similar to participants in Canada, participants in Japan

mostly understood the workings of VPNs as an intermediary connection (31% n=100). However, the subsequent prevalent comprehension among users in Japan was with tunneling (24% n=100) and other (24% n=100). The least common coded responses for participants in Japan were location access (18% n=100), shield (2% n=100), and the addition of a VPN (1% n=100). We see three notable examples of participants located in Japan's responses depicted in Figure 8. The first example shown in Figure 8a displays a comprehensive drawing of the representation of location access. On the left side of the drawing the user, represented by the annotation of me, is shown in a foreign country, denoted by the annotation above of outside the country. On the right side of the image, Japan is depicted, identified by the annotation of Japan, featuring a server located there, marked by the annotation of server. Between these two sides, two different connections are displayed. The lower connection signifies that a direct connection to Japan is not possible, shown by the annotation of cannot enter directly, while the upper connection indicates that a connection can be established using a VPN, shown by the annotation. Overall, this example highlights the capability of VPNs to facilitate a connection from a different geographical location. Figure 8b presents the second example, illustrating a VPN metaphorically as a tunnel. This representation, similar to the location access example depicted in Figure 7a, showcases the user's device (PC) on the left side and the ultimate connection destination (annotated as a server) on the right. Instead of a central connection, a broader rectangle is depicted as a representation of a tunnel, which is described by the annotated label. This simple yet impactful illustration visually communicates the concept of a VPN encrypting data for a secure passage for data transmission. Lastly, Figure 8c depicts a response categorized under the 'other' category. In this instance, the participant wrote in Japanese expressing their lack of comprehension of the question and their inability to provide a representation of how a VPN operates. This observation is intriguing, highlighting that certain VPN users have no understanding of the underlying mechanisms of a VPN.

Notably of the overall twelve responses (five from Japan and seven from Canada) in the other section were drawings that either did not depict a representation of a VPN's function or had a general lack of effort such as seemingly random scribbles.

To summarize, participants from Canada displayed a strong belief for the various use cases of VPNs, while participants from Japan focused more on the technical aspects of VPN functionality rather than its applications. Canadian participants demonstrated a solid grasp of VPN server configurations as intermediaries in connections, but often did not relate VPNs to data encryption. In contrast, participants from Japan exhibited a higher level of association regarding data encryption and VPNs, though overall comprehension was still lacking in both groups.

(a) Example of a 'Location Access' coded drawing with translated annotations. Response from P132.



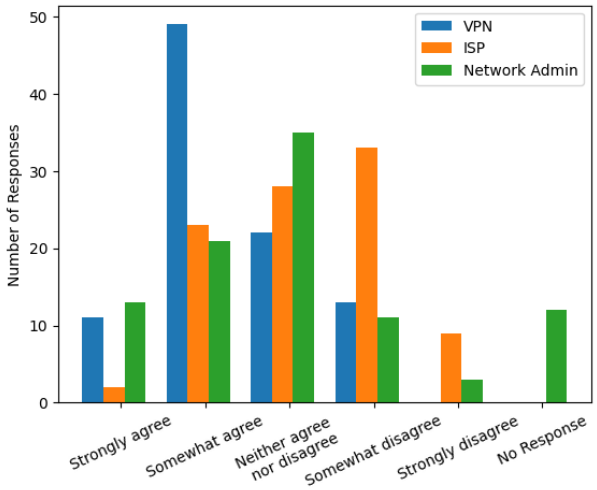
(b) Example of a 'Tunnel' metaphor coded drawing with translated annotations. Response from P154.

(c) Example of a 'Other' coded drawing with translated annotations. Response from P121.

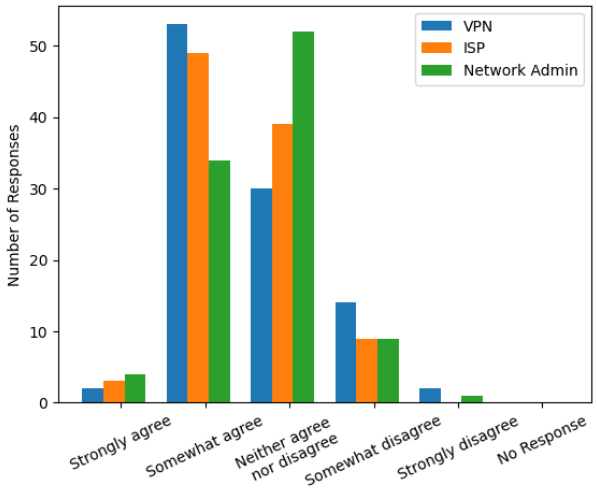
Fig. 8: Three examples of participants located in Japan drawings of how a VPN works. (a) Location Access, (b) Tunnel, and (c) Other.

C. Trust Analysis of VPN Stakeholders

We shift our focus to users' trust in stakeholders involved in the provision of VPN services. We asked participants three questions, asking them to rate their trust in VPNs, ISPs, and network administrators using a five-point Likert scale. Figure 9 presents the results. Participants in Canada generally trusted VPNs more than ISPs and network administrators, with the latter distribution just below neutral. Interestingly, few Canadian participants expressed complete trust in VPNs (12% n=95), ISPs (2% n=95), or network administrators (14% n=95). No Canadian participants expressed complete distrust of VPNs, although a small number expressed complete distrust of ISPs (9% n=95) and network administrators (3% n=95). A similar distribution of trust was observed among participants in Japan, although they expressed more trust in both ISPs and network administrators than participants in Canada. Few Japanese participants completely trusted their VPN (2% n=100), ISP (3% n=100), or network administrator (4% n=100). No one completely distrusted their ISP, with only a few showing complete distrust in their VPN (2% n=100) and



(a) Canada.



(b) Japan.

Fig. 9: The level of trust ranked by participants between VPN, ISP, and Network Administrator. (a) Canada, (b) Japan.

network administrator (1% n=100).

When asked who they trusted more with their data, Canadian respondents overwhelmingly said their VPN provider (62% n=95), followed by network administrators (22% n=95), and then ISPs (15% n=95). A t-test confirmed a statistically significant difference in the level of distrust between VPNs and ISPs ($p = 1.50 \times 10^{-9}$). Meanwhile, Japanese participants expressed the most trust in their VPN provider (44% n=100), followed by their ISP (36% n=100), and finally their network administrator (20% n=100). Here, the level of trust in ISPs was closer to that of VPN providers, as shown by a non-significant t-test result ($p = 0.65$). When comparing the overall trust levels of VPNs ($p = 0.06$) and ISPs ($p = 7.83 \times 10^{-8}$) between the two groups, statistical tests indicate significant differences. These results underscore the differences in trust levels towards VPNs and ISPs in different national contexts.

To summarize, participants from both countries exhibited a higher level of trust in VPN providers compared to ISPs, with Canadian participants expressing a greater distrust towards ISPs.

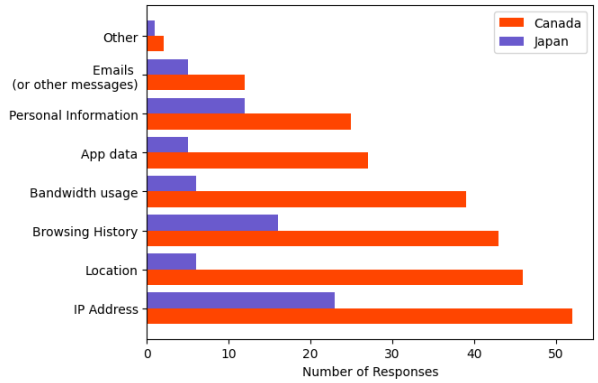


Fig. 10: What type of information do you think is collected by your VPN provider? Responses collected from participants who answered 'Yes' to believing their VPN provider collects data from them (49% n=195).

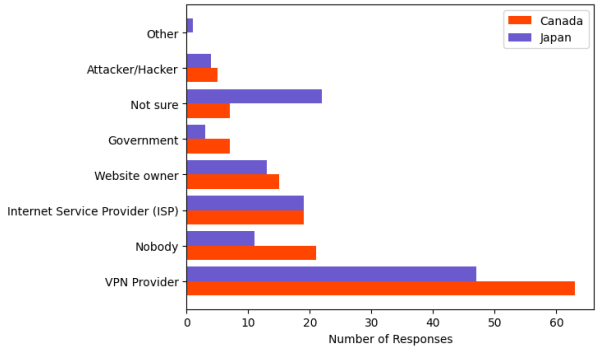


Fig. 11: While using a VPN and visiting a website, who do you believe knows that you have visited that website? Responses collected from participants.

D. Misconceptions

The initial misconception is evident from the findings presented in Figure 1. A significant majority of VPN users (53% n=195), located both in Canada (52% n=95) and Japan (55% n=100), state they are using a VPN for security reasons despite the primary purpose of a VPN being privacy protection. This is worrisome as misunderstanding the proper use case and breadth of security and privacy may cause users to introduce unnecessary vulnerabilities. It is worth noting that certain VPNs may be bundled with security software, such as antivirus programs [32], and conversely, some antivirus software may include VPN functionality [5]. The bundling of VPNs with security software could potentially confuse VPN users, leading them to believe that these additional functionalities are inherent features of VPNs themselves.

The majority of participants (49% n=195) believe that their VPN provider collects data about them, with the remaining believing that their VPN did not collect data (26% n=195) or were not sure (24% n=195). Interestingly, a total of 22

participants who reported to use VPNs that have a zero logging policy still believed that their VPN was logging their information. Of the participants that believed their VPN provider was collecting their information we asked them to select the types of information they thought was being collected, which is represented in Figure 10. Most participants believed that their IP address (96% n=96), browsing history (80% n=96), and location (69% n=96) were being collected. Participants located in Canada selected more choices of the types of information they thought their VPN provider collected about them. In comparison participants located in Japan selected fewer options about the type of data they believed was being collected. Despite the conceptions participants had on VPNs collecting their data, the majority of participants admitted to reading none (59% n=195) or only some (43% n=195) of the privacy policy of their VPN(s).

Another prevalent misconception we investigated pertained to participants' understanding of who they believed could observe their internet traffic when using a VPN while visiting a website. The distribution of responses made by participants is shown in Figure 11. Consistent with the previous results the majority of participants from Canada (66% n=95) and from Japan (47% n=100) believe that their VPN provider would be able to see what website they visited. VPN providers may log data, for example most free VPNs do and commercial VPNs often only save required information, these participants are correct with their assumption. Although, a large portion of participants have a flawed perception, believing their ISP (19% n=195) and the website owner (14% n=195) can see the website they visit over a VPN. One participant from Canada did recognize that VPN providers do not often log personal information and only handle the necessary information for account creation and payments, if applicable. This participant stated that:

> **P81**: 'Whatever data I gave when signing up (CC #, name, email)'

On the other hand another participant did also recognize this fact as well. However, they also displayed concern that traffic was still being monitored by their VPN and provided to their local government and law enforcement for surveillance.

> **P83**: 'Anything used to pay to sign up plus that can be connected to a username that connects to the app through the paid acct so an IP address is tagged to it and I assume they keep logs of all traffic in and out to give to LEO and Govt for 'surveillance' and security.'

The differences between both of these participants' statements show that there is still a lack of understanding of VPNs data policies.

In general, participants from both groups share similar misconceptions. They demonstrate a common lack of understanding regarding the primary purposes of VPNs and the data collection policies employed by VPN providers. Furthermore, there is a shared deficiency in comprehending how information is collected on the Internet.

E. Exploring Cultural Context

In our research, we conducted a comparative investigation involving two distinct cultural contexts: Canada and Japan. An understanding of the cultural divergences and convergences between these groups is paramount for a nuanced interpretation of our findings. Canada, recognized statistically as a multicultural country [7], embraces a culture that strongly emphasizes individualism, yet it is also characterized by values of tolerance, respect, and a community-oriented mindset [12]. In contrast, Japan, often characterized as more homogeneous [21], places a high value on harmony and tends to prioritize the needs of the group over individual desires [14]. These cultural disparities provide a crucial backdrop for the interpretation of our research outcomes.

With this cultural framework in mind, we investigated how participants from both Canada and Japan understood and interacted with VPNs. Notably, many participants encountered difficulties in articulating and illustrating the functionality of a VPN. These misconceptions were pervasive in both groups, with subtle variations in their understanding of VPN functionality and the services it offers. Canadian participants exhibited a more comprehensive understanding of the various use cases for VPNs, while Japanese participants demonstrated a heightened awareness of how VPNs anonymize data in transit, as evidenced by their frequent use of the 'tunnel' metaphor, illustrated in Figure 8b. The Canadian group's understanding aligns with prior research [11] conducted in culturally similar contexts, underscoring the importance of incorporating populations with diverse cultural backgrounds, such as Japan, in our study. Furthermore, our findings revealed a general lack of understanding among participants regarding various VPN use cases, with privacy, rather than security, being the primary perceived benefit.

The variance in perception and usage of VPNs between Japan and Canada can be attributed, in part, to the distinct cultural and societal backgrounds of each country. The emphasis on security in VPN usage among Japanese users may reflect broader societal values emphasizing order and community stability over individual privacy. Conversely, the focus of Canadian users on privacy and content accessibility aligns with the values of individualism prevalent in a multicultural society. Additionally, the common misconception held by both groups regarding VPNs' data collection practices underscores a widespread misunderstanding of digital privacy and security globally. It is evident that the cultural differences in VPN usage and understanding are deeply rooted in each country's culture, values, and societal background. However, it is essential to acknowledge that this perspective is only one facet, and other factors, such as digital literacy, access to technology, and government regulations, should also be considered.

V. Discussion

In this section, based on the findings from our study, we discuss recommended actions for VPN providers, limitations of our research, and potential future work.

A. Recommended Action

In light of these findings, a strategic course of action can be formulated to address the identified gaps in understanding the inner workings of VPNs. Firstly, there is a compelling need for the standardization of regulations governing VPN providers, with a particular emphasis on the realm of VPN advertising. The pervasive use of deceptive and unethical strategies in VPN advertisements, as documented in previous research [2], underscores the urgency for clear delineation of acceptable practices. By establishing transparent guidelines for advertising privacy and security tools, users can be better equipped to discern the genuine protective capabilities of these tools.

Furthermore, recognizing the cultural disparities among countries, it is imperative to tailor education and awareness initiatives to align with the distinct understanding and attitudes of VPN users. Customizing education programs in this manner holds the potential for more effective utilization of VPNs and heightened security awareness globally. Specifically, initiatives may be devised to enhance user comprehension of VPN functionalities, fostering informed decision-making.

Addressing the broader implications of VPN adoption, as they become increasingly integral to internet traffic, warrants consideration. Anticipating a potential shift towards VPN-like protocols for handling escalated data volumes, the prospect of wider adoption as a default protocol for sensitive data is envisioned. This ambitious proposition seeks to streamline user experience by automating the intricacies of VPN functionalities within operating systems, eliminating the need for users to grapple with complex technicalities.

In examining the comparative trust levels in VPNs and ISPs in Canada and Japan, the existing disparities evoke concerns, especially given the less comprehensive regulatory framework for VPNs. Despite the analogous data access capabilities of VPN providers and ISPs, the former operates with considerably less regulatory oversight. This disjunction raises pivotal inquiries about the associated risks and safeguards pertinent to VPN utilization. Contrary to the assumption of inherent superiority in data protection and privacy offered by VPNs over ISPs, the need for a meticulous examination of the regulatory environment surrounding VPN services becomes evident. An in-depth analysis of the existing regulatory landscape is indispensable for discerning the nuanced implications and formulating informed policies to safeguard user interests.

B. Limitations

There are several limitations to our study. First, we only recruited participants located in Canada and Japan. These participants are not a representative sample of all VPN users. Our findings may not accurately reflect the behaviors, attitudes, and motivations of VPN users from other regions or cultural backgrounds. In addition, we recruited participants through the Prolific platform, which may introduce selection bias. Although it is a widely used platform recommended for crowdsourcing in research, it is crucial to recognize that the user base of Prolific may have a higher level of technological literacy compared to the general population [40]. In contrast, Lancers does not have a feature for collecting representative samples and operates on a first-come, first-served basis, potentially introducing additional issues of representativeness into our study. Finally, our survey design is susceptible to recall bias, a common challenge in self-report studies [25]. Participants may not accurately recall or report their past experiences, behaviors, or attitudes regarding VPN use.

C. Future Work

Given the findings and limitations of the present study, several promising avenues for future research emerge. First, expanding the scope of the survey population would provide valuable insights into underrepresented groups. In addition, interesting subpopulations remain unexplored. For example, an analysis of VPN use in countries with pervasive censorship and restricted Internet freedoms could provide unique perspectives. Given the inherent limitations of a survey, a qualitative study, such as interviews, could provide a deeper understanding of users' thoughts and perceptions. This approach would provide a more nuanced understanding of the underlying factors influencing VPN adoption and use, allowing for a more sophisticated analysis of the issue. In addition, supplementing quantitative data from surveys with qualitative findings could help researchers triangulate results and provide a more complete understanding of the topic at hand.

VI. Conclusion

In conclusion, our research investigated cultural disparities in VPN use, comprehension, and perception among users in Japan and Canada. The study unveiled notable distinctions in usage priorities, with Japanese participants prioritizing security and Canadian participants valuing privacy and content accessibility. Additionally, a variance in the VPN beliefs around was observed, with Canadians demonstrating a more comprehensive awareness of VPN benefits compared to the Japanese, who primarily associated VPNs with encrypted connections. Furthermore, misconceptions regarding VPN data collection practices and policies were identified in both groups.

This study contributes to a broader understanding of user experiences with security and privacy tools, emphasizing the importance of tailored public education. The findings underscore the significance of addressing cultural nuances in VPN education to promote more informed decision-making. This research aims to facilitate greater awareness and effective utilization of VPN resources within diverse cultural contexts.

Acknowledgment

The authors would like to thank Ayako A. Hasegawa for her valuable advice on the progress of this research and the National Institute of Information and Communications Technology (NICT) for its support of our research activities.

REFERENCES

[1] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 137–153.

[2] O. Akgul, R. Roberts, M. Namara, D. Levin, and M. L. Mazurek, "Investigating influencer vpn ads on youtube," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 876–892.

[3] V. Binkhorst, T. Fiebig, K. Krombholz, W. Pieters, and K. Labunets, "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)*. Boston, MA: USENIX Association, Aug. 2022, pp. 3433–3450. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/binkhorst

[4] P. Bischoff. (2023, may) Study: How the most popular free vpns use your data. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/free-vpn/

[5] Bitdefender, "Bitdefender - global leader in cybersecurity software," 2023. [Online]. Available: https://www.bitdefender.com/

[6] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development*. Sage Publications, Inc, 1998.

[7] S. Canada. (2022, oct) The canadian census: A rich portrait of the country's religious and ethnocultural diversity. Statistics Canada. [Online]. Available: https://www150.statcan.gc.ca/n1/daily-quotidien/221026/dq221026b-eng.htm

[8] A. Constantinides, M. Belk, C. Fidas, and G. Samaras, "On cultural-centered graphical passwords: Leveraging on users' cultural experiences for improving password memorability," in *Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization*, ser. UMAP '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 245–249. [Online]. Available: https://doi.org/10.1145/3209219.3209254

[9] D. Crawshaw, "Everything vpn is new again: The 24-year-old security model has found a second wind." vol. 18, no. 5, p. 54–66, nov 2020. [Online]. Available: https://doi.org/10.1145/3434571.3439745

[10] DeepL, "Deepl translate: The world's most accurate translator," 2023. [Online]. Available: https://www.deepl.com/translator

[11] A. Dutkowska-Żuk, A. Hounsel, A. Morrill, A. Xiong, M. Chetty, and N. Feamster, "How and why people use virtual private networks," in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 3451–3465. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/dutkowska-zuk

[12] N. Evason. (2016, jun) Canadian culture. Cultural Atlas. [Online]. Available: https://culturalatlas.sbs.com.au/canadian-culture/canadian-culture-core-concepts

[13] A. Feldmann, O. Gasser, F. Lichtblau, E. Pujol, I. Poese, C. Dietzel, D. Wagner, M. Wichtlhuber, J. Tapiador, N. Vallina-Rodriguez, O. Hohlfeld, and G. Smaragdakis, "The lockdown effect: Implications of the COVID-19 pandemic on internet traffic," *CoRR*, vol. abs/2008.10959, 2020. [Online]. Available: https://arxiv.org/abs/2008.10959

[14] M. Fukushima, S. F. Sharp, and E. Kobayashi, "Bond to society, collectivism, and conformity: A comparative study of japanese and american college students," *Deviant Behavior*, vol. 30, no. 5, pp. 434–466, 2009. [Online]. Available: https://doi.org/10.1080/01639620802296212

[15] T. C. F. Group. (2023, nov) Country comparison tool. The Culture Factor Group. [Online]. Available: https://www.hofstede-insights.com/country-comparison-tool

[16] F. Herbert, S. Becker, L. Schaewitz, J. Hielscher, M. Kowalewski, A. Sasse, Y. Acar, and M. Dürmuth, "A world full of privacy and security (mis)conceptions? findings of a representative survey in 12 countries," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, apr 2023. [Online]. Available: https://doi.org/10.1145%2F3544548.3581410

[17] F. House, 2023. [Online]. Available: https://freedomhouse.org/countries/freedom-net/scores?sort=descorder=Total%20Score%20and%20Status

[18] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An analysis of the privacy and security risks of android vpn permission-enabled apps," in *Proceedings of the 2016 Internet Measurement Conference*, ser. IMC '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 349–364. [Online]. Available: https://doi.org/10.1145/2987443.2987471

[19] T. Kajimoto and L. Kihara. (2022, aug) Japan's planned record minimum wage hike opens path to sustained gdp growth. Reuters. [Online]. Available: https://www.reuters.com/world/asia-pacific/japans-average-minimum-wage-set-rise-record-pace-this-year-nikkei-2022-08-01/

[20] M. Kan. (2022) India orders vpn providers to log and hand over customer data. PC Mag. [Online]. Available: https://www.pcmag.com/news/india-orders-vpn-providers-to-log-and-hand-over-customer-data

[21] D. Kenley, "The myth of homogeneity: Immigration and ethnicity in 20th century japan," https://www.japanpitt.pitt.edu/, 2014.

[22] E. Khan, A. Sperotto, J. van der Ham, and R. van Rijswijk-Deij, "Stranger vpns: Investigating the geo-unblocking capabilities of commercial vpn providers," in *Passive and Active Measurement*, A. Brunstrom, M. Flores, and M. Fiore, Eds. Cham: Springer Nature Switzerland, 2023, pp. 46–68.

[23] 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*, ser. IMC '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 443–456. [Online]. Available: https://doi.org/10.1145/3278532.3278570

[24] S. Khattak, M. Javed, S. A. Khayam, Z. A. Uzmi, and V. Paxson, "A look at the consequences of internet censorship through an isp lens," in *Proceedings of the 2014 Conference on Internet Measurement Conference*, ser. IMC '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 271–284. [Online]. Available: https://doi.org/10.1145/2663716.2663750

[25] J. Lazar, J. H. Feng, and H. Hochheiser, *Research Methods in Human-Computer Interaction*. Wiley Publishing, 2010.

[26] R. Likert, *A technique for the measurement of attitudes*, 1932.

[27] A. Maghsoudlou, L. Vermeulen, I. Poese, and O. Gasser, "Characterizing the vpn ecosystem in the wild," in *Passive and Active Measurement*, A. Brunstrom, M. Flores, and M. Fiore, Eds. Cham: Springer Nature Switzerland, 2023, pp. 18–45.

[28] Microsoft. (1996, may) Microsoft leads initiative for virtual private networks across the internet. [Online]. Available: https://news.microsoft.com/1996/03/04/microsoft-leads-initiative-for-virtual-private-networks-across-the-internet/

[29] S. Migliano. (2023) Are vpns legal? Top10VPN. [Online]. Available: https://www.top10vpn.com/what-is-a-vpn/are-vpns-legal/

[30] M. Namara, D. Wilkinson, K. Caine, and B. Knijnenburg, "Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, pp. 83–102, 01 2020.

[31] Nolita. (2023, may) Canada's online streaming act (bill c-11) explained. Express VPN. [Online]. Available: https://www.expressvpn.com/blog/canadas-online-streaming-act-bill-c-11-explained/

[32] NordVPN, "The best online vpn service for speed and security — nordvpn," 2023. [Online]. Available: https://nordvpn.com/

[33] G. of Canada, "Current and forthcoming general minimum wage rates in canada," September 2022. [Online]. Available: https://srv116.services.gc.ca/dimt-wid/sm-mw/rpt1.aspx

[34] R. Ramesh, L. Evdokimov, D. Xue, and R. Ensafi, "VPNalyzer: Systematic Investigation of the VPN Ecosystem," in *Network and Distributed System Security*. The Internet Society, 2022. [Online]. Available: https://dx.doi.org/10.14722/ndss.2022.24285

[35] R. Ramesh, A. Vyas, and R. 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)*. Anaheim, CA: USENIX Association, 2023.

[36] J. A. Sava. (2023, May) Size of the virtual private network (vpn) market worldwide from 2019 to 2027. Statista. [Online]. Available: https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/

[37] M. Smirniotis. (2021, mar) What is a vpn and what can (and can't) it do? The New York Times. [Online]. Available: https://www.nytimes.com/wirecutter/guides/what-is-a-vpn/

[38] N. Sombatruang, T. Omiya, D. Miyamoto, M. A. Sasse, Y. Kadobayashi, and M. Baddeley, "Attributes affecting user decision to adopt a virtual private network (VPN) app," *CoRR*, vol. abs/2008.06813, 2020. [Online]. Available: https://arxiv.org/abs/2008.06813

[39] P. Story, D. Smullen, Y. Yao, A. Acquisti, L. Cranor, N. Sadeh, and F. Schaub, "Awareness, adoption, and misconceptions of web privacy tools," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, pp. 308–333, 07 2021.

[40] J. Tang, E. Birrell, and A. Lerner, "Replication: How well do my results generalize now? the external validity of online privacy and security surveys," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Boston, MA: USENIX Association, Aug. 2022, pp. 367–385. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/tang

[41] K. Townsend. (2023, may) Uk introduces mass surveillance with online safety bill. [Online]. Available: https://www.securityweek.com/uk-introduces-mass-surveillance-with-online-safety-bill/

[42] A. Vigderman and G. Turner. (2023, may) 2023 vpn usage statistics. Security.org. [Online]. Available: https://www.security.org/vpn/statistics/

[43] Z. Wang, Y. Cao, Z. Qian, C. Song, and S. V. Krishnamurthy, "Your state is not mine: A closer look at evading stateful internet censorship," in *Proceedings of the 2017 Internet Measurement Conference*, ser. IMC '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 114–127. [Online]. Available: https://doi.org/10.1145/3131365.3131374

[44] D. Xue, R. Ramesh, A. Jain, M. Kallitsis, J. A. Halderman, J. R. Crandall, and R. Ensafi, "OpenVPN is Open to VPN Fingerprinting," in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/xue-diwen

APPENDIX

We are interested in the better understanding of the following from a global perspective; Why Virtual Private Networks (VPNs) are being adopted and used, What users understand and do not understand about VPNs, and What misconceptions are common around VPNs. For this study, you will be presented with questions relevant to VPNs, there usage, your personal thoughts about VPNs, and trust regarding VPN providers. Your responses will be kept completely confidential. Questions contained with in this study are of the following format:

- Multiple choice
- Form fields
- Text entry
- Drawing

The study should take approximately 10-15 minutes to complete. Your participation in this research is voluntary. You have the right to withdraw at any point during the study.
If you have any questions, concerns or feedback regarding the study, the lead researcher (name) can be contacted at (email)
By clicking the button below, you acknowledge:
Your participation in the study is voluntary.

- You are 18 years of age.
- You have used a VPN before
- You are aware that you may choose to terminate your participation at any time for any reason.

1) Gender
   - Male
   - Female
   - Non-binary / other
   - Prefer not to say
2) How old are you?
   - 18 - 25
   - 26 - 35
   - 36 - 45
   - 46 - 55
   - 56 - 65
   - Over 65
   - Prefer not to say
3) Education Level (current or highest completed)
   - Post-graduate education (Masters, Doctorate, Medical/Law School)
   - Undergraduate degree
   - College diploma
   - Technical certificate
   - High School or Equivalent
   - Prefer not to say
   - Other (Please Specify)
4) Is your job/education/background/interest in Information Technologies or a related field?
   - Yes
   - No
   - Other (Please Specify)
5) Do you consider yourself knowledgeable in Information Technologies or related fields?
   - Strongly disagree
   - Somewhat disagree
   - Neither agree nor disagree
   - Somewhat agree
   - Strongly agree
6) In which country do you currently reside?
7) In which country is your identified nationality?
8) Have you used a VPN before?
   - Yes
   - No
9) What type of VPN(s) do you use?
   - Paid commercial VPN
   - Free commercial VPN
   - VPN provided by School
   - VPN provided by Workplace
   - Personal VPN
   - Other (Please Specify)

9.1) *Asked for each participant that selected 'Paid commercial VPN' in **8)***
How much do you spend monthly to use your VPN service(s)? Please provide your local currency in your answer. (CAD, USD, JPY)

10) What is the name of the VPN(s) you use?
   - 1.1.1 + Warp Cloudflare
   - AirVPN
   - Algo
   - Anonine
   - Astrill VPN
   - Atlas VPN
   - Avast Secureline
   - Avira Phantom
   - Azire VPN

- BestVPN
- Betternet
- BolehVPN
- Bullguard
- Cactus VPN
- Cryptostorm
- CyberGhost
- Encrypt.me
- ExpressVPN
- F-Secure Freedome
- FastestVPN
- Free VPN by Free VPN.org
- Goose VPN
- Hide My Ass!
- Hide.me
- HideIPVPN
- Hotspot Shield
- IP Vanish
- IVPN (in custom)
- Ivacy VPN
- K2VPN
- Kaspersky
- KeepSolid VPN Unlimited
- LeVPN
- Mozilla VPN
- Mullvad VPN
- Namecheap
- NordVPN
- Norton Secure VPN
- OVPN
- OpenVPN Access Server
- Outline
- Panda VPN
- Perfect Privacy
- Private Internet Access
- Private Tunnel
- Private VPN
- Proton VPN
- Psiphon
- Pure VPN
- Riseup
- Speedify
- Star VPN
- Steganos
- Streisand
- Strong VPN
- SurfEasy
- SurfShark
- TorGuard
- Touch VPN
- Trust.Zone
- TunnelBear
- Turbo VPN
- University VPN
- Unspyable
- Urban VPN Desktop
- VPN Hotspot - Unlimited Proxy
- VPN Owl
- VPN Plus
- VPN Pro
- VPN Proxy Master
- VPN Super: Best VPN Proxy
- VPN.ac
- VPNBook
- VPNLite
- VPNUK
- VeePN
- Vypr
- Windscribe
- ZenMate
- ZoogVPN
- Other (Please Specify, if more then one separate by commas)

11) Why do/did use a VPN?
- Security
- Remote content access (School or work)
- Region specific content access
- File Sharing (Torrents or P2P)
- Privacy
- Access blocked content (Censorship)
- Interested in the technology
- Other (Please Specify)

12) How often do you use a VPN?
- All the time
- Every day
- Every week
- Occasionally
- I don't anymore

12.1) *Asked for each participant that selected 'I don't anymore' in **12)***
Why did you stop using a VPN?
- No longer needed it
- Too expensive
- Too hard to use
- Too slow
- Not secure
- Not used enough
- Other (Please Specify)

13) When did you first start using a VPN?
- Under 18
- 18-25
- 26-35
- 36-45
- 46-55
- 56-65
- Over 65
- Prefer not to say

14) What devices do you use a VPN with?
- Laptop
- Desktop

- Phone or tablet
- Other (Please Specify)

15) What do you think a VPN is? Please describe it the best you can.
16) Use the following to provide a drawing to explain how you think a VPN works. Can be any format.
17) While using a VPN and visiting a website, who do you believe knows that you have visited that website?
    - Website owner
    - VPN Provider
    - Nobody
    - Internet Service Provider (ISP)
    - Attacker/Hacker
    - Government
    - Not sure
    - Other (Please Specify)
18) *Asked for each participant that selected 'Yes' in **18)*** Do you use your VPN to secure browsing activity?
    - No
    - Yes

(18.1) Who are you trying to protect your browsing data from?
- Internet Service Provider (ISP)
- Your Government
- Outside Government
- Hacker/Attacker
- Family
- Legal Agency
- School or Workplace
- Other (Please Specify)

19) Do you believe that your VPN provider collects data about you?
    - No
    - Yes
    - Not sure

(19.1) *Asked for each participant that selected 'Yes' in **19)*** What type of information do you think is collected by your VPN provider?
- Location
- IP Address
- Browsing History
- Personal Information
- Emails (or other messages)
- Bandwidth usage
- App data
- Other (Please Specify)

20) Have you read the privacy policy of the VPN(s) you use?
    - Yes - all of it
    - Read most
    - Read some
    - No - none of it
    - Other (Please Specify)
21) Do you trust your VPN provider?
    - Strongly disagree
    - Somewhat disagree
    - Neither agree nor disagree
    - Somewhat agree
    - Strongly agree
22) Do you trust your ISP?
    - Strongly disagree
    - Somewhat disagree
    - Neither agree nor disagree
    - Somewhat agree
    - Strongly agree
23) Do you trust your Network Administrator(s)?
    - Strongly disagree
    - Somewhat disagree
    - Neither agree nor disagree
    - Somewhat agree
    - Strongly agree
    - Not applicable
24) Which of the following do you trust more with your data?
    - VPN provider
    - ISP
    - Network Administrator
    - Other network entity
25) Do you think your VPN is easy to use?
    - Strongly disagree
    - Somewhat disagree
    - Neither agree nor disagree
    - Somewhat agree
    - Strongly agree
26) Thank you for participating in this survey. The survey is now completed! If you have any feedback or suggestions please leave it below.