How and Why People Use Virtual Private Networks

Agnieszka Dutkowska-Zuk, Austin Hounsel[*], Amy Morrill[†]
Andre Xiong[*], Marshini Chetty[†], Nick Feamster[†]
Lancaster University *[*]Princeton University* *[†]University of Chicago*

Abstract

Virtual Private Networks (VPNs) are often used to protect online users' privacy, but many VPNs do not guarantee privacy and may even compromise user privacy through leakage of traffic flows, data collection and sharing, and so forth. In this paper, we aim to understand the extent to which people are aware of privacy and security risks when using VPNs, as well as how they use and adopt VPNs in the first place. To do so, we conducted a study of 729 VPN users in the United States about their VPN usage habits and preferences. Our study comprised 32 in-person interviews with university students, a survey of 349 university students and a survey of 348 general VPN users on Prolific. We present three findings. First, although a general population of VPN users primarily use VPNs to improve privacy and security, students are additionally concerned with access to content (e.g., circumvention of geographic restrictions). Second, both groups concluded that VPNs collect data about them, exposing gaps in both mental models about how VPNs work and awareness of the risks of data collection. Finally, most users learned about VPNs in high school or college and use free VPNs but feel safer using VPNs provided by their institutions. These results could form the basis of future research, awareness campaigns, and regulatory activity.

1 Introduction

Virtual Private Networks (VPNs) [13] encrypt all network traffic from a client device to an intermediate server, which subsequently forwards traffic to an ultimate destination. Many users rely on VPNs to improve their privacy, and many VPN services are available, with companies from Cloudflare to Facebook providing VPNs [10, 30, 34]. Some estimates indicate that the VPN market has grown from $16.5 billion in 2016 to over $30 billion in 2020, and it is expected to grow at an annual rate of over 15% between 2021 and 2027 [14, 15]. Yet, despite their relatively widespread use, and in spite of their name, many VPNs fail to provide basic privacy guarantees. For example, some VPNs have accidentally leaked user traffic, breaking security and privacy claims made by the providers [20, 31]. Other VPNs may capture user traffic and send the data to third parties for targeted advertising [9, 17]. At one point, Facebook Onavo collected application traffic without notifying users [7, 42].

Given that many VPNs may introduce their own privacy risks, it is imperative to understand whether users are aware of these risks. A better understanding of user attitudes and awareness concerning VPNs can shed light on possible improvements to VPNs, from technical design improvements to awareness campaigns. Towards this goal, we posed the following research questions:

- Why do people use VPNs?
- Are people aware of the security & privacy risks of VPNs?
- How do people choose which VPNs to use?

To study these questions, we conducted a study of 729 VPN users in the United States (U.S.). First we conducted 32 in-person interviews with university students. We then surveyed 349 university students from one institution as well as a general sample of 348 VPN users on Prolific. We chose to study both university students and a general population of VPN users for several reasons.

First and foremost, there are different types of VPNs, offered by different organizations and institutions, for different purposes; and yet, sometimes users may use VPNs for a variety of priorities and purposes. Specifically, universities typically offer a VPN to their students and employees to access various content and services (e.g., at some universities, various compute clusters and services are only available via VPN). Thus, this population typically has better access to and awareness about at least one VPN, affording at least a basic level of familiarity with VPNs, if not more experience with VPN usage. Second, in the general population, people may have a broader range of goals for using VPNs, and their default behavior may be to seek a commercial VPN of some type, as opposed to using their university or employer's VPN. Exploring our questions with different target populations allows us to understand our questions from a variety of perspectives, given the wide-ranging purposes for VPNs.

Our study yields three important findings, which we discuss in Section 4. First, the general population used VPNs more for security and privacy and tended to use VPNs continuously; in contrast, the student population tended to use VPNs more as a way to access restricted content and would use them more on demand. Both groups used free VPNs predominantly, but the general population tended to be more skeptical of free VPNs. The university students used VPNs to gain access to content and materials at their institutions (e.g., restricted pages, library materials), or to bypass censorship or filtering of content. For these students, privacy and security were secondary considerations. Second, most users were generally not familiar with the technical details of how a VPN works, which often led to misconceptions and misunderstandings about the privacy guarantees that a VPN could provide. Some of these misunderstandings were more fundamental, suggesting that not only did users not understand technically how VPNs work, but also

they did not understand the capabilities and incentives for various VPN providers to collect data about them. For example, although many users in both populations indicated that they used a VPN to protect their data from "companies" in general, they seemed unconcerned that the VPN provider itself is a company (and, in the case of some, such as Facebook's Onavo VPN, even an advertiser) that is often gathering user data for profit. Both groups concluded that data collection practices of VPNs was a general consequence of being online. Finally, both groups started using VPNs in high school or college, and most participants selected VPNs based on cost, security, and speed. The general population prioritizes safety and security when selecting a VPN, but students primarily care about accessing content and the general reputation of the VPN provider. These findings suggest possible avenues for future work for researchers and regulators; to improve mental models of VPNs and to design ways to help users better distinguish between various use cases for VPNs and the broader implications of VPN data collection.

2 Background and Related Work

We provide background on VPNs and survey related work, including work studying privacy and security vulnerabilities from VPNs, past studies of user attitudes about privacy, and studies of user attitudes about VPNs.

Background: Virtual Private Networks Originally created for enterprises to communicate securely, VPNs rapidly gained broad commercial appeal as personal Internet usage soared [16]. VPNs create a secure connection ("tunnel") to a server, from which a user can safely access a destination [44]. VPN providers can encrypt and authenticate this connection using a number of methods with varying degrees of effectiveness, including OpenVPN, Layer 2 Tunneling Protocol, Internet Protocol Security, and several others [13]. From the perspective of a network eavesdropper, the VPN user's traffic appears to be coming from the VPN server, as opposed to from the user's device. VPNs can be used to access destinations on the Internet or on private networks, such as on a private enterprise or campus network. Contrasting these institutional VPNs, commercial VPNs connect users to a server that is not associated with a specific institution. Users may use commercial VPNs to access blocked content, such as Twitter in China [2] or to access location-restricted content [28]. Commercial VPN providers often offer multiple servers [29].

VPN Data Leakage Recent studies have illustrated the privacy pitfalls of VPNs. For instance, researchers studied 14 of the most popular VPN providers and found that most of these providers unintentionally leak traffic to websites hosted on IPv6 addresses [31]. Researchers have also found that off-the-shelf VPN software is susceptible to passive and active attacks, limiting their ability to provide anonymity [1, 3]. For instance, a study of VPN apps in the Android marketplace discovered that many VPNs send data to third-party trackers or have security misconfigurations [17, 45]. Some of the data collection that VPNs do may also be intentional. For example, a study of commercial VPN providers found five providers that implement transparent proxies, which inspect and modify traffic that users send [20]. Our study adds to previous work on VPN data leakage by investigating users' awareness of the privacy and security issues associated with VPNs, as well as whether these issues impact user behavior and decisions about which VPNs to use.

User Attitudes on Privacy There have been many studies of user attitudes on privacy and the Internet, which have found that users are aware of privacy threats on the Internet but often are either unable or unmotivated to protect themselves from those threats. Researchers have analyzed users' mental models in their perceptions of the Internet more generally [19, 22, 23, 33]. For instance, users in the U.S. are concerned about online tracking and want to control it in certain situations [26, 35, 39, 43], yet they are often confused as to how tracking works and how they can protect themselves [38]. One study suggested that a combination of awareness of, motivation to use, and knowledge of how to use privacy and security tools affected people's usage of these tools [11]. Another study focused on online privacy and security attitudes and behaviors found that while Internet users with stronger technical backgrounds were more aware of privacy and security threats, they did not engage in more secure practices than their less knowledgeable peers [19], with the exception of "expert users" [8]. Previous research showed that 18-to-22 year olds are likely to rely on strategies to make themselves less visible online [32]. These phenomenon of tech-savvy and younger users neglecting to use their knowledge to protect themselves could have implications for VPN-focused studies. Similarly to these studies, our work will also investigate user attitudes about privacy and the impact of those attitudes on user behavior. We expand on past work by focusing specifically on VPN users, who may differ significantly from previous populations that have been studied.

User Attitudes on VPNs Several studies have investigated how and why people use VPNs. Researchers surveyed Pakistani Internet users and found that 57% of respondents used VPNs to access YouTube while the website was censored in 2012 [21]. Past work explored how smartphone people used VPNs when Facebook was banned in Sri Lanka [18]. Contrasting these two studies, our research concerns a different demographic and is more extensive. Additionally, a study conducted in the United Kingdom and Japan found that users prioritize review ratings and price over interface and security considerations when comparing VPN apps [40]. This study also found differing priorities between UK and Japanese participants, indicating that cultural background may affect user perceptions of VPNs, necessitating our study of users living in the U.S. [40]. In another European focused masters thesis, a researcher described the perceptions of VPNs held by 11

laypeople and 8 experts working at a professional service firm in the Netherlands. This study found that, while experts' concepts about VPNs tended to be more accurate than those of laypeople, there was confusion among both groups about how VPNs work and what threats are mitigated by using a VPN [5]. In our paper, we similarly investigate user perceptions of VPNs, but we use a larger sample from more diverse backgrounds in a different country, the U.S.

The most closely related study to our own specifically focused on users who adopt VPNs as a privacy-enhancing technology (PET) through a survey of 90 technologically savvy Reddit users and students [27]. Similarly to our study, this paper investigated why people adopt VPNs, and a common finding across both papers is that many participants used VPNs for reasons other than simply to achieve privacy (e.g., to circumvent geographic restrictions, for access control). However, our study still fills a gap in the literature because it had a much larger sample of participants, used more robust methods, and investigated areas of VPN usage not covered in previous papers. The VPN-as-PET study had a much smaller sample of VPN users—only 37 users in the survey had ever used a VPN, an order of magnitude less than the size of our survey. Moreover, that study surveyed one group of participants, while our methods include in-depth interviews and comparing surveys from two distinct populations to determine the extent to which our themes hold among students as well as in the general population. Thus, our study can be used to complement and corroborate overlapping results from the previous study, which is important given its limited sample size and methods. Additionally, our research questions actually differ substantially from those of the VPN-as-PET study apart from the overlap in asking about VPN adoption. The other study investigated why users abandon VPNs and the differences in users with practical and emotional considerations for using VPNs; our study did not focus on either of those questions, instead investigating users' choices of VPN technology and mental models about how VPNs work and the guarantees that they do and do not provide. Therefore, we believe that our paper is an important contribution to the literature on VPNs because it corroborates and expands on previous work, as well as investigates novel questions about VPN usage.

3 Method

We conducted a two-part study of 729 U.S. users to answer our research questions about how and why people use VPNs, their mental models of VPNs, how they choose which VPN to use, and their awareness and attitudes about data collection practices of VPNs. In one part of the study, we interviewed 32 student VPN users from one university in the U.S. [37]. We also conducted a survey of 349 students from the same university, and a survey of 348 VPN users from a general population on Prolific. All aspects of this study were approved by our institutions' Institutional Review Boards (IRB).

3.1 Interviews

To explore user attitudes towards and behaviors with VPNs and to help identify themes to explore more broadly in a larger survey, we conducted semi-structured interviews of a substantial number of student participants.

Interview Guide We designed our interview guide to get a better understanding of participants' knowledge and background and participants' general privacy and security awareness about VPNs. We first asked participants who they believed could collect data about them online and who they would want to prevent seeing certain information about their online habits. To understand users' mental models of VPNs, we then asked participants to describe how a VPN works in their own words. Next, we asked how users' learned about VPNs and what their first experience using a VPN was. Next, to understand how users select VPNs, we asked how participants choose to use a particular VPN, how and why they use a VPN, how participants felt when using a VPN, and whether they used a paid or free version of their VPN(s). Finally, we asked about likes, dislikes, and improvements concerning current VPNs; to do so, we asked questions on students' knowledge of and usage patterns of different VPN types, including specific VPNs they had used, their reasons for selecting and using VPNs, and perceptions of data collection by VPNs. Before participating in the semi-structured interview, participants were asked to fill out a consent form and a short questionnaire that asked about user's academic majors and other basic demographic information such as age, gender, course of study, and general online habits.

3.1.1 Recruitment

We recruited 32 interview participants via our university's institutional survey research center (the "gold standard" for constructing participant panels), as well as through social media platforms such as Twitter. Table 1 shows demographic information about the interview participants, who were mostly 18–24 years old and undergraduate students (81%). We selected only students who had used a VPN before and were currently enrolled in our university's undergraduate or graduate program. We aimed to recruit a variety of international and domestic students living in the U.S. so that this diverse group could expand our knowledge and understanding of how and why participants use VPNs. Interviews were conducted in Summer and Fall 2018. Participants were compensated with a $20 Amazon gift card. We conducted 23 interviews via Skype, and another nine in-person on our university campus. Each interview lasted for about one hour. Four interview participants did not give consent to recording, so we collected detailed notes in lieu of a recording. All other interviews were audio recorded.

3.1.2 Data Analysis

We first transcribed all recorded interviews and developed an extensive codebook to apply to the interview transcripts and

Age	#	%	Gender	#	%	Origin	#	%	Education/Current Enrollment	#	%
18 to 24	26	81%	Female	17	53%	United States	12	37.5%	Postdoctoral Researchers	4	13%
25 to 34	5	16%	Male	14	44%	International	20	62.5%	Graduate	2	6%
35 to 44	1	3%	Other	1	3%				Undergraduate	26	81 %

Table 1: *The distribution over age, gender, origin and education status for 32 interview participants, at the time of collecting the data; 20 international participants came from 17 different countries.*

Main Code	Definitions
Reasons for VPN usage	Motivations and goals behind VPN usage
What is a VPN?	Mental model of a VPN
Guidelines when choosing VPN	Personal preferences of VPN's qualities and strategy in choosing a VPN
Trust in VPN provider	Attitudes towards their VPN provider
Using institution related VPN	Usage habits regarding institutional VPNs
Use or trust free VPN	Attitudes towards commercial free VPNs
VPN practices	Thoughts on VPNs' data practices
What a VPN guarantees	Assumptions about VPNs' assertions
Tracking while using VPN	Assumptions about protection that VPNs provide against tracking

Table 2: *Summary of main codes reported in the interviews.*

field notes. We used the Dedoose platform [12] for qualitatively coding the transcripts for a thematic analysis [36]. One member of the research team first coded all of the interview transcripts and a second member of the team performed a second round of coding for consistency. When there were any points of disagreement, this was discussed and resolved as a team. We had 45 parent codes and including child codes, we had a total of 1906 codes. Once the transcripts were all coded, the whole research team met and discussed the codes to identify nine parent codes of interest, shown in Table 2, with 31 child codes as reflecting the main themes in the data. For example, our main code *Reasons for VPN usage* had four child-codes, which represented participants' motivation behind using VPNs: *Bypass geographic firewalls, Work, Privacy, Not Privacy/Security*. To illustrate, an example quote linked to *Bypass geographic firewalls* child-code was participant's 26 testimony: *'I have my mom reroute the U.S. IP (Internet Protocol) address to a Mexican IP address with a VPN, so then she could watch her Venezuelan TV (Television) shows.'*

The primary coder then wrote summaries of these codes. The research team reviewed the summaries and held regular research meetings to decide on the final themes arising from the interview data. Calculating inter-rater reliability (IRR) is not necessary for the type of analysis that we performed, because shared consensus can still be reached without this measure in thematic analysis [4]. McDonald et al. also state that calculating IRR is not necessary when coded data is not the end product but instead part of the process to derive concepts and themes, or in our case, as input for thematic analysis [25].

3.2 Surveys

Based on the interview data and analysis, we then designed a larger-scale survey to complement our interview data and expand our knowledge about VPN users' perspectives, which we deployed to two different populations: university students and general VPN users. These surveys were conducted to determine what themes from the interviews held with a larger sample of users of differing technological knowledge and access to VPNs. For our surveys, we first pre-screened and filtered out respondents who did not consent to the survey, were under 18, or had never used a VPN. As in the interviews, we collected demographic information such as age, gender, and course of study. In accordance with best practices, for the student population, we collected demographic information at the beginning of the survey because this information was used for screening; for the general population, we moved these questions to the end of the survey to minimize threat [6]. Notably, our demographic questions were slightly different for university students and for general VPN users, as we replaced university-specific questions, such as academic major, with questions about vocation. Our survey asked for background information about respondents' perceptions and concerns about online data collection, including the nature of the data collected, who is collecting data, and why they are collecting data. We also asked about respondents' usage patterns of different tools and tactics to combat online risks, as well as how they sourced them.

The remainder of the survey asked similar questions as in the interviews around users mental models of VPNs, their expectations of VPNs for privacy and security, their usage habits with VPNs and how they select VPNs. In our survey, we generally avoided open-ended questions to prevent user fatigue and reduce the complexity of data analysis; as a result, we asked only three open-ended questions. We also avoided double-barreled questions, negative questions, and biased wording [24]. We included two attention check questions that required a certain response to ensure respondents were answering mindfully. Participants that had been interviewed in the first part of our study were not allowed to take

the survey, to avoid response bias. We piloted our survey with our research team members as well as larger research groups focused on usable privacy and security and human-computer interaction. Based on our pilots, we altered the survey flow and wording to ensure questions were clear.

3.2.1 Recruitment

Students We recruited university students from a large university in the U.S. to take the survey which we created using Qualtrics. We sent email invitations to a random sample (containing 2,748 users) of the university population via the university's institutional survey research center. We aimed to reach at least 5% of the university's VPN-using student population as recommended by Lazar [24]. We launched and conducted the university student iteration of our survey between February 2019 and March 2019. Our large sample size allowed us to collect 452 responses, of which 349 were completed, passed our attention checks, and fit our recruiting criteria. The average survey completion time was 15 minutes, excluding 35 surveys which took more than 2 hours complete, which we assume occurred because people forgot to submit the survey upon completion or completed it over several sittings. Our final sample of 349 valid and completed responses is large compared to the university's overall population (4.3%). Table 3 shows detailed demographic data of the respondents. As with the interviews, the majority of the university respondents were age 25 and under (79%). Participants with complete valid responses were entered into a draw for one of two $250 Amazon gift cards.

General Population We recruited general VPN users on Prolific, an online recruiting platform. We pre-screened for participants who were currently living in the U.S. and who had used a VPN before using a screener survey. We then directed users to our main survey. We launched and conducted the general VPN user iteration of our survey between August 2021 and September 2021, and collected 530 responses, of which 348 were completed, passed attention checks, and fit our recruiting criteria. Notably, several responses had answers copied from the Internet (e.g. to define how a VPN works) or shared answers with other respondents, and we filtered out these responses from our data set. The average survey completion time was 15 minutes. Participants were paid approximately 15 dollars per hour for completing a survey response in accordance with the minimum wage guidelines.

3.2.2 Data Analysis

We used Qualtrics and R to analyze the data from both iterations of the survey. We first analyzed the response data using tools built-in with Qualtrics. We limited our analysis to the valid and complete responses. First, we performed descriptive analysis on all the survey questions.

Certain questions were only shown if respondents selected certain answers in both surveys. As such, questions that have fewer data points than the sample size contain responses from every applicable respondent. For Table 4, all respondents in the university population were shown the questions but not required to answer them. This issue was fixed before we deployed the survey to a general population of VPN users. In presenting our results, we show counts in terms of how many participants were shown a question. Where applicable, we also include counts for those who were not shown the question or chose not to answer.

Similarly to the interviews, we qualitatively coded the open-ended answers using a code book that was developed based on multiple reads through the responses. The graphs show all survey codes used for each question. One team member coded all the responses for both surveys. A second team member reviewed all the coded responses to ensure consistency and to discuss any points of disagreement. Since the initial coding pass was primarily done by the first researcher, we did not calculate IRR. In the graphs, we report on the most prevalent codes occurring in the survey data. In the graphs presented, response count reflects the total number of participants who chose an option. Oftentimes this was in answer to a "Check all that apply" question, so the total of all the responses may be greater than the number of participants if any participant selected multiple options. In questions where participants were asked to choose and rank options, we compute a weighted score on the inverse ranking, where weights correspond to $1/r$ for a ranking of r [41].

When reporting our qualitative data, we refer to our interview participants as "P", our student survey participants as "S", and our general population survey participants as "G".

3.3 Limitations

Our study has several limitations. First, we only recruited students from one university in the U.S.. Although the university makes a concerted attempt to recruit a diverse cross-section of students, any single university may not be representative of all university students. Second, our interviews and surveys may be subject to recall bias which is difficult to avoid [24]. Third, our student interviews and survey were not completely anonymous as they required survey participants who wished to enter the raffle and all interview participants to submit an email address. Interview participants were asked to meet with a member of the research team in person which could affect the respondents' honesty. Fourth, our survey did not distinguish between precise notions of security and privacy, thus participants could interpret these concepts differently. Finally, we ran our survey of general VPN users almost two years after running our survey of university students, which could have affected responses based on changes in user perceptions of VPNs or in VPNs themselves during this time.

4 Findings

We present findings on how and why people[1] use VPNs, their mental models of VPNs, and how they choose VPNs.

[1] We use "people" to refer to respondents in our study, not all people.

Survey	Age	#	%	Gender	#	%	Origin	#	%	Education/Current Enrollment	#	%
University	18 to 25	274	79%	Female	178	51%	United States	257	74%	Graduate	123	35%
	26 to 35	74	21%	Male	171	49%	International	92	26%	Undergraduate	226	65%
	36+	1	0%									
General Population	18 to 24	157	45%	Woman	205	59%	United States	342	98%	Graduate	82	24%
	25 to 34	121	35%	Man	134	39%	International	6	2%	Undergraduate	196	56%
	35 to 44	52	15%	Non-binary	7	2%				High School	68	20%
	45 to 54	18	5%	Prefer not to disclose	1	0%				< High School	2	0%
				Prefer not to self describe	1	0%						

Table 3: *The distribution over age, gender, origin, and education status for the survey participants at the time of collecting the data. Our 92 international participants from the first survey came from 32 different countries. Our 6 international participants from the second survey came from 5 different countries.*

4.1 VPN Usage

The general population used VPNs more for security and privacy (Figure 2), and thus tended to use VPNs continually. Although the student population also valued these goals, students tended to view VPNs more as a way to access restricted content (Figure 2), and would use VPNs more on-demand. All participants used free VPNs predominantly (Table 4), but the general population was more skeptical about the safety of free VPNs. Both groups felt safest using institutional VPNs. (Table 5)

4.1.1 Which VPNs Do Users Use?

General Population Figure 1 shows which types of VPNs our respondents used. Most general population VPN respondents used free commercial VPNs (186/348), while paid commercial VPNs (122/348) were less popular.

School VPNs (111/348) and employer-provided VPNs (109/348) were used by about one-third of our respondents. Table 4 shows that Hotspot Shield (58/186) was a first choice of free VPN among the general population. Other common choices were Proton VPN (38/186), Betternet (32/186), TunnelBear (28/186), and Hola (23/186).

The general population respondents also chose paid commercial VPNs; they primarily used NordVPN (49/122), ExpressVPN (39/122), Private Internet Access (16/122), IPVanish (15/122) and TunnelBear (12/122). Overall, there was a larger number of VPNs that were used by the general population than the student population. This applies not only to paid commercial VPNs, but also to free commercial VPNs.

The general population felt most safe using university or employer-provided VPNs (Table 5). On the other hand, the general population felt more vulnerable using free VPNs than the student population and also placed more trust in paid VPNs than the student population.

Students Most student respondents used the VPN offered by their university (228/349) and nearly half also used free commercial VPNs (172/349) (Figure 1). A smaller fraction of students used paid commercial VPNs (97/349). Fewer respondents used VPNs through their employer (60/349) or a

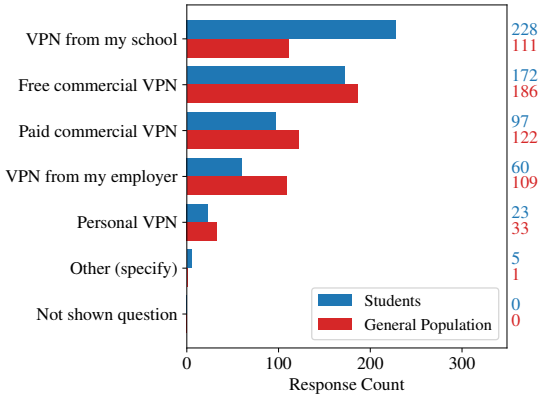

Figure 1: *Types of VPNs used (responses selected by participants)*

personal VPN that they set up themselves (23/349); 49/349 students used only VPNs provided by their university, and 91/349 used only commercial VPNs.

Table 4 also shows the most common VPNs that student respondents used; these choices are similar to the general population sample. The students used a variety of paid VPNs, including ExpressVPN (40/97), NordVPN (18/97), and PrivateInternetAccess (10/97). There is also a long tail of less popular choices, with 50/97 students using paid commercial VPNs that five or fewer other students used. Eight survey participants that reportedly used paid commercial VPNs did not specify particular VPNs.

The most common free commercial VPNs respondents used were Hotspot Shield (40/172), TunnelBear (33/172), Hola (27/172), and Betternet (25/172). Notably, some respondents indicated they used SonicWall or ConnectTunnel which is the VPN offered by the university, indicating some confusion on what is an institutional versus commercial VPN provider. Furthermore, 35 student respondents that reportedly used free commercial VPNs did not specify which VPNs they used.

Table 5 shows that students felt safest using university or employer-provided VPNs. They also felt safer using paid commercial VPNs than free commercial VPNs.

When asked whether it was important who their VPN provider was, 11/32 interview participants said it was, particularly for these who used their university's VPN (7/11).

Survey	Free VPN	#	%	Paid VPN	#	%
General Population	Hotspot Shield	58	18.1%	NordVPN	49	16.3%
	ProtonVPN	38	11.9%	ExpressVPN	39	13%
	Betternet	32	10%	Private Internet Access	16	5.3%
	TunnelBear	28	8.8%	IPVanish	15	5%
	Hola	23	7.2%	TunnelBear	12	4%
	Less popular choices	136	42.5%	Less popular choices	167	55.7%
	Total responses	315	100%	**Total responses**	298	100%
University Students	Hotspot Shield	40	20%	ExpressVPN	40	30%
	TunnelBear	33	16.5%	NordVPN	18	13.5%
	Hola	27	13.5%	PrivateInternetAccess	10	7.5%
	Betternet	25	12.5%	TunnelBear	8	6%
	HIDE.ME	11	5.5%	AstrillVPN	5	3.8%
	Less popular choices	58	29%	Less popular choices	50	37.6%
	Total responses	194	100%	**Total responses**	131	100%

Table 4: *Breakdown of the most commonly used free and paid VPNs from each survey.*

Survey	Response	VPN through school/employer	#	%	Paid VPN	#	%	Free VPN	#	%
General Population	Safe		41	22.3%		36	29.5%		8	4.3%
	Somewhat safe		69	37.5%		59	48.4%		47	25.3%
	Neutral		49	26.6%		25	20.5%		60	32.3%
	Somewhat vulnerable		18	9.8%		1	0.8%		65	34.9%
	Vulnerable		7	3.8%		1	0.8%		6	3.2%
University Students	Safe		54	23.5%		21	22.3%		4	2.8%
	Somewhat safe		73	31.7%		31	33%		46	31.9%
	Neutral		71	30.9%		27	28.7%		36	25%
	Somewhat vulnerable		32	13.9%		11	11.7%		46	31.9%
	Vulnerable		8	3.5%		4	4.3%		12	8.3%

Table 5: *How "safe" participants feel using different types of VPNs. (responses selected by participants)*

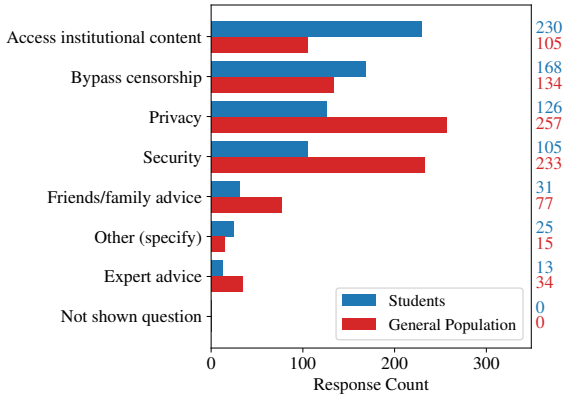

Figure 2: *Why do/did you use a VPN? (responses selected by participants)*

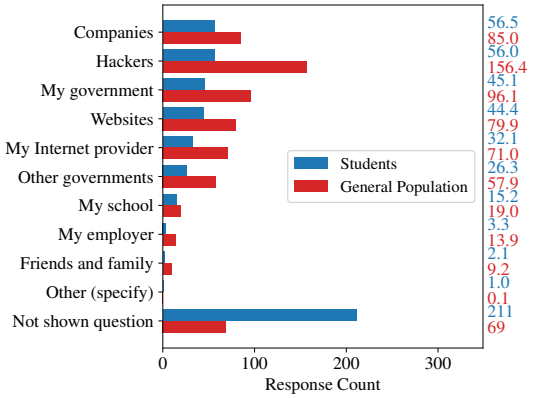

Figure 3: *Who are you trying to protect yourself from? Choose and rank your choices based on level of concern.*

University VPNs were reassuring for them because they believed they were safe to use. However, interviewees were less consistent concerning what they were willing to do online using their university or employer-provided VPN. For example, 5/16 interview participants who used their university VPN reported that they would use it only for completing university work, because they simply did not feel private, they felt that university could track them, or that using their university network made them more vulnerable. On the other hand, 5/16 interview participants told us they used their university VPN for private activities, such as browsing. For example, P32 would simply forget to switch it off and did not mind having it on:

> It really doesn't bother me if someone is looking at what I'm doing while I'm on the VPN, just because my philosophy is like, at this point it's probably all there anyway.

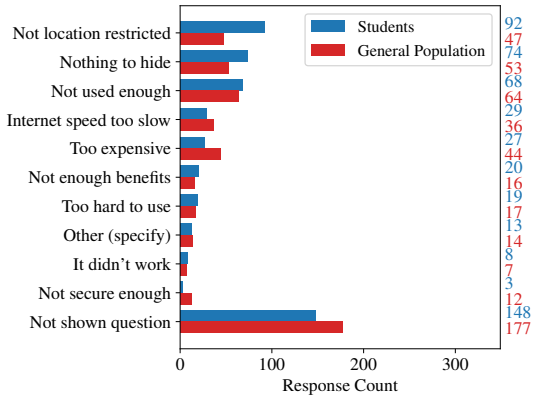

Figure 4: *Why did you stop using a VPN? (responses selected by participants)*

4.1.2 Why Do Users Use VPNs?

General Population Figure 2 shows why respondents used VPNs. General population respondents reported using VPNs because of the privacy (257/348) and security (233/348) they provide, with 279/348 participants selecting at least one of these options. We asked these respondents to choose and rank who they were protecting themselves from when using a VPN. Figure 3 shows that these respondents were primarily concerned about hackers, companies, government, and websites. Interestingly, not many saw a threat in their closer circles, including their school, employer, friends, and family.

In contrast to the student respondents, bypassing censorship (134/348) and accessing institutional content (105/348) were somewhat less prevalent reasons for using VPNs in the general population sample. Fewer respondents from the general population specified other reasons through free response for using VPNs (15/348).

Students Most student respondents used a VPN to access content—specifically institutional materials—when off-campus (230/349) (Figure 2). Additionally, 168/349 survey respondents reported using a VPN to bypass Internet censorship, and 138/349 survey participants said that they used VPNs to protect privacy or security. Similarly to the general population, most of these survey respondents ranked companies, hackers, the government, and websites as top concerns. As shown in Figure 3, fewer participants were concerned about other governments or friends and family.

For those who specified "Other" in the survey, students commonly reported using a VPN to access Advanced Placement (AP) scores, as S108 noted: "To access AP scores early (they were releasing them one time zone at a time to prevent too much web traffic)".

Our student interview participants (21/32) reported using a VPN to bypass geographic firewalls and watch movies or TV shows online (15/21). For eleven student interview participants, accessing blocked content was a priority when using a VPN. In a typical example, P11 spoke of using a VPN for news websites that were not blocked but had different or limited content depending on the Internet Protocol (IP) address of the Internet user. As this participant was from the United Kingdom (UK), they wanted to access the UK British Broadcasting Corporation (BBC) website while they were living in the US. Also, P26 used a VPN to help his or her mother:

> Venezuela has blocked everything coming from their YouTube channels, and I have my mom reroute the US IP address to a Mexican IP address with a VPN, so then she could watch her Venezuelan TV shows.

Thirteen interview participants said that privacy was not the main reason for using a VPN. Fewer (7/32) used it to protect their personal information, and four wanted a VPN to be secure and keep them anonymous. For example, P21 said:

> I guess I don't like the idea of [the university] or an ISP being able to see all of my traffic. I don't think that I trust anyone with all of my traffic or consumer habits.

4.1.3 How Often Do Users Use VPNs?

General Population The general population respondents used VPNs more often than students. Around half of our respondents did not currently use VPNs (171/348). Most reported using VPNs sometimes (164/348), followed by 91/348 respondents who reported using them most of the time. The minority of respondents who reported having completed or being currently enrolled in higher education in the general sample reportedly used VPNs on the ends of the spectrum: 31/348 used VPNs always, and 62/348 rarely. About half of the general population respondents (171/348) stopped using VPNs at the time of data collection, as they did not use it enough (64/171), had nothing to hide (53/171), were not location restricted (47/171), or found VPNs too expensive (44/171) (Figure 4).

Students VPN usage appeared to be more irregular and on an "as needed" basis among student respondents. Most students (201/349) reported that they did not currently use a VPN, with only 148/349 survey respondents reporting that they currently use a VPN. When asked how often student respondents used a VPN, 302/349 reported only using a VPN sometimes or rarely. A minority reported using a VPN all the time (10/349) or most of the time (37/349). Figure 4 shows that of the 201 respondents that stopped using VPNs, some reported that they were no longer location restricted (92/201), did not have anything to hide (74/201), or simply did not use it enough (68/201). Very few of these respondents reported a lack of security (3/201) to be a contributing factor in their decision to stop using VPNs.

Seven interview participants reported using VPNs only when they needed to, while 4/32 participants would always have it on. One interviewee from this group explained that VPNs would take up storage on their computer, and consume battery life. Another example of on-demand usage was from P26, who was restricted by the bandwidth limitations of Windscribe, a free VPN:

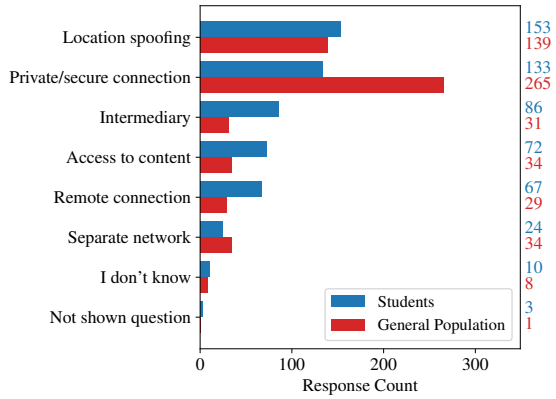

Figure 5: *What do you think a VPN is? (response coded by researchers)*

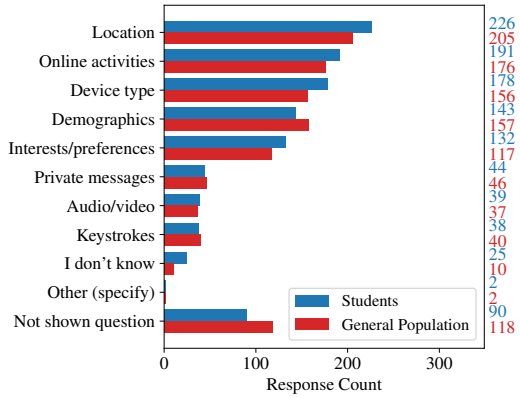

Figure 6: *What kind of data do you think your VPN provider collects about you? (responses selected by participants)*

> Like the Windscribe, I get 10 GB every month, and I certainly go through more than 10 GB of Internet.

4.2 Mental Models of VPNs

> Most participants did not know how VPNs worked technically (Figure 5) but knew the purpose of a VPN. Both groups believed VPNs collect data about them as a default consequence of using these tools and primarily for advertising reasons (Figure 7). Regardless, the general population expected privacy and safety from tracking from VPNs (Figure 10).

4.2.1 What Do Users Think VPNs Are?

General Population More general population respondents described VPNs as a private or secure connection (265/348) than the student population (Figure 5). This is typified by the response from G39, who described VPNs in terms of the security features they supposedly provide:

> A blocker. Blocking out information such as location, passwords, any personal information on my device.

Fewer respondents described VPNs as software that enables location spoofing (139/348). Even fewer described VPNs as intermediaries (31/348), or as software that enables them to access certain content (34/348). They also more often described VPNs as separate networks (34/348) than as remote connections (29/348).

Students Most survey participants had a fairly good idea about the purpose of a VPN, such as location spoofing (153/349) (Figure 5). As S255 described, for them a VPN was "Tricking my Internet to think I'm somewhere else in the world." Survey respondents also described a VPN as a private or secure connection (133/349). As S283 reported:

> It's been described to me as an "Internet condom". It protects your Internet information by setting up a different IP address.

Others defined a VPN as an intermediary (86/349), for example S78 reported that "It's a porthole to allow private communication/data transfer between two devices." Ten survey respondents reported they did not know what VPNs are or how to define them. Overall, our participants seemed to have a good functional model of VPNs ("what a VPN does for me"), as opposed to a technical model.

Similarly, when asked what a VPN is, most interview participants could list features that a VPN provided. On the other hand, most participants were less familiar with technical explanations. Almost half (14/32) described a VPN as routing your Internet activity through third party machines or as a service for changing your IP address, masking your identity (10/32), or reducing others ability to track you (10/32). P18 explained:

> It's sort of a middle man. So instead of you actually downloading the file from someplace where somebody might be looking at you downloading it, they download it for you and then they send it to your computer. So it figures that they downloaded it and not you.

Some participants believed that VPNs allow you to access blocked content (13/32), allow access into another network (7/32) and others described a VPN as secure, private, or adding an extra level of safety (13/32). In a quote typical of what we heard from participants, P25 described benefits of using a VPN:

> Its usefulness is pragmatism, it's like, "I need to see this YouTube video, but they don't let me see it in Brazil so I'm just going to do it in Belgium." I think that that's what VPNs are to me.

4.2.2 Do Users Consider VPNs Private?

General Population 230/348 of the general population respondents reported that VPNs collect data about them, such as their location (205/230), online activities (176/230), information on the device they used (156/230), demographics (157/230), or interests (117/230) (Figure 6). However, 76/230 respondents believed that only their VPN had access to their

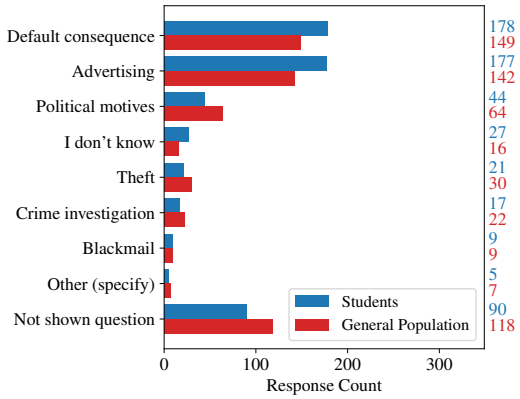

Figure 7: *Why do you think your VPN provider collects your data? (responses selected by participants)*

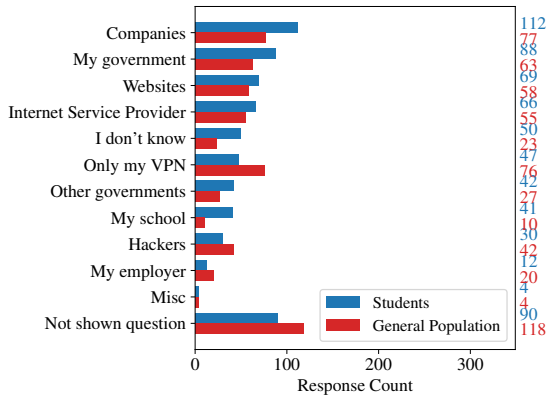

Figure 8: *Who do you think has access to the data collected by your VPN? (responses selected by participants)*

data (Figure 8). Few general population respondents believed that the motives for collecting data were nefarious. The general population respondents also more commonly believed that their data was collected by for political motives (Figure 7).

154/230 respondents thought their information was being shared with other parties. As shown on Figure 8, the general population believed that other companies (77/154), government (63/154), websites (58/154), and their Internet Service Provider had access to their data. They also believed that other entities have access to users' online activities (122/154), location (119/154), demographic information (110/154), interests/preferences (97/154) and type of user's device (88/154) (Figure 9).

Students 259/349 of student survey respondents believed that their VPN provider could collect data about them. Figure 6 shows that most student respondents believed that VPNs collect location data (226/259) and online activities (191/259). Fewer believed that VPNs collected pri-

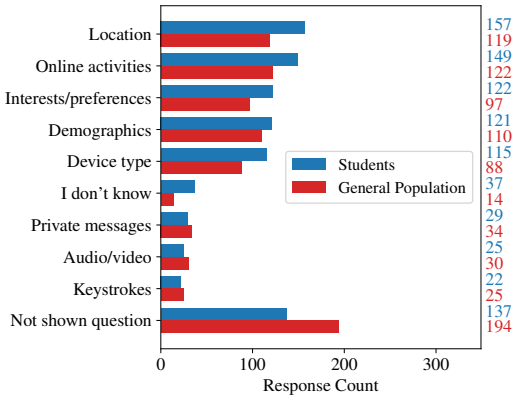

Figure 9: *What information do you think is being shared with these entities? (responses selected by participants)*

vate messages (44/259), recordings (39/259), or keystrokes (38/259). Some student respondents did not know what was collected (25/259).

Figure 7 shows that most of these respondents believed that VPNs collect data for commercial motives (177/259), or simply because data collection is a "default consequence of using the Internet" (178/259); 126/259 of respondents selected both options. Like the general population, few respondents believed that the motives for data collection were nefarious—such as blackmail (9/259)—and some survey respondents selected "I don't know" (27/259).

There was also little consensus between participants on who had access to the collected data. The largest proportion of student respondents, as shown in Figure 8, believed that companies (112/259) and the government (88/259) had access to the data collected by VPNs. A smaller proportion believed that only VPNs had access (47/259), and 50/259 of respondents did not know where their data went.

Figure 9 shows that the 212/259 respondents that believed other entities had access to the data collected by their VPN thought that their location (157/212), online activities (149/212), interests (122/212), and demographic information (121/212). Fewer believed that private messages (29/212), recordings (25/212), or keystrokes (22/212) were shared, which coincides with what survey participants believed VPNs could collect.

Most interview participants (23/32) also believed that VPNs collect their data, with some expressing that VPNs keep data for statistics or to sell the data. For example, P11 believed that VPNs could keep logs for many different reasons:

> If you're using VPNs for a bit more nefarious means, for example, like buying drugs or trading child pornography and things like that. (. . .) I think some of them do keep logs, and they're able to give them over to police, and the governments, and things like that. (. . .) And then, other ones are a bit more simple, like tracking users' web habits to sell to advertisers and things like that.

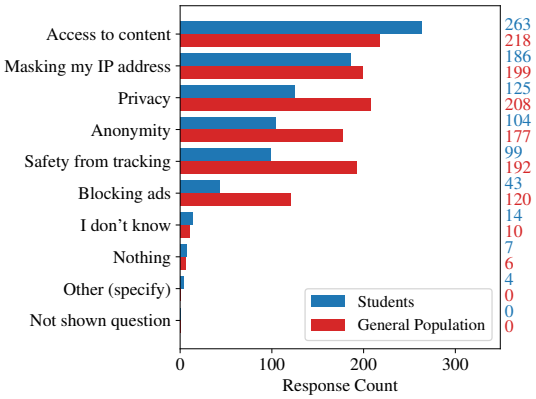

Figure 10: *What do you think your VPN guarantees? (responses selected by participants)*

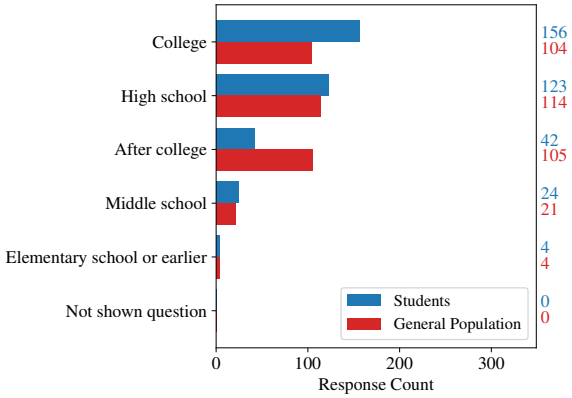

Figure 11: *When did you first use a VPN? (response selected by participants)*

Interestingly, several interviewees (7/32) also believed that the university has a VPN to access all information about students and to monitor if someone is cheating during exams.

4.2.3 Do Users Feel Anonymous When Using VPNs?

General Population Figure 10 shows that the general population survey respondents believed that VPNs guarantee not only access to content (218/348), but also privacy, (208/348), safety from tracking (192/348), and anonymity (177/348). 199/348 of the respondents also believed that VPNs mask their IP addresses.

Students Interestingly, student respondents generally did not feel that VPNs provided total anonymity. Three quarters of all student respondents believed their VPNs guaranteed access to certain content (263/349) and masking of their IP addresses (186/349). However, only about one-third of student respondents believed that their VPNs guaranteed privacy (125/349), anonymity (104/349), and safety from tracking (99/349) (Figure 10).

Similarly, most interview participants did not believe that VPNs guaranteed them anonymity (20/32). In fact, three-fourths of interview participants (24/32) believed that it is possible to be tracked when using VPNs, and some believed that there is always a way to do so (8/32) and that you can be tracked by VPN provider itself (9/32). P1 explained:

> If it is SSL encryption, the VPN provider would still know that you are communicating with a certain web service but the VPN provider would not or probably not know the contents of the communication if it's SSL encrypted. They would only know who you want to communicate with. And if it's not encrypted, then they can see. They can be doing packet sniffing or even more malicious things like deep packet injection and deep packet inspection to actually look at the contents of that communication and do potential malicious things with that.

4.3 VPN Selection

> Many respondents learned about VPNs as early as high school or college (Figure 11). All respondents choose VPNs based on cost, security, and speed (Figure 12). The general population prioritizes better security and safety but students primarily care about accessing content and the good reputation of VPNs when choosing one.

4.3.1 When Do Users Start Using VPNs?

General Population The general population showed considerable variability concerning when they first started using VPNs, as shown in Figure 11. A plurality of these respondents first used a VPN as early as high school (114/348). A similar number of participants first used a VPN either in college (104/348) or after college (105/348).

Students Most student respondents reported using VPNs first at their university (156/349) (Figure 11). Many also reported using VPNs as early as high school (123/349). Not many participants first used a VPN "after college" (42/349), likely because a large fraction of the sample was undergraduate students.

Two interview participants reported that they first started using VPNs when they were in high school. P20 told us how he used VPNs to access websites that were blocked by his high school:

> I've used them for a few reasons, but privacy was never really one of them. It was just when my content was restricted when I was in boarding university, I went to boarding university for high school. Our Wi-Fi was very tightly patrolled. So any number of things were blocked, like from adult content, to a lot of sports websites for instance were blocked, because they "encouraged gambling" and I like to watch a lot of sports online illegally, because that was the only way I could watch them.

Another participant, P26, shared how they used a VPN to

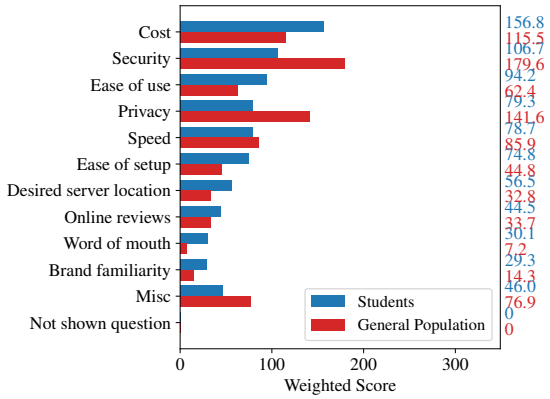

Figure 12: *Rank the five most important factors when choosing a VPN.*

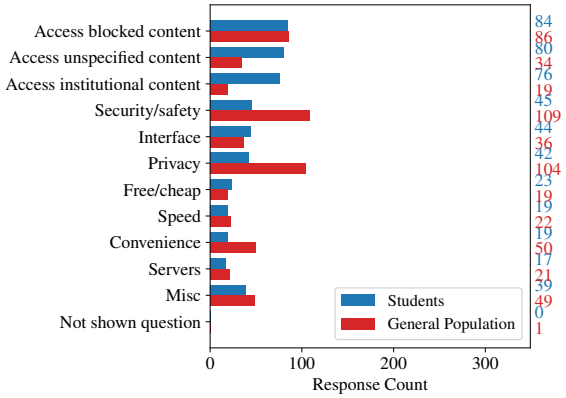

Figure 13: *What do you like about your VPN(s)? (response coded by researchers)*

download a graphics editor, which they could not afford in high school:

> The university computers came with a standard photo editor that was pretty bad. So we wanted to use Photoshop, and Photoshop is very expensive. So one of my friends recommended that we torrent it from The Pirate Bay, so we went on there, and I remember it has a warning that says, make sure your IP is masked(. . .) I did that, and then we downloaded Photoshop for a university project. I think I was maybe 16 at the time.

4.3.2 How Do Users Select a VPN?

General Population Figure 12 breaks down what considerations were important to the general population when choosing between VPNs. The general population respondents considered security and cost to be important considerations when choosing which VPN to use. Privacy was a more important consideration than ease of use for the general population, which is consistent with our other finding that the general population often describes VPN functionality in terms of privacy and security (Figure 5).

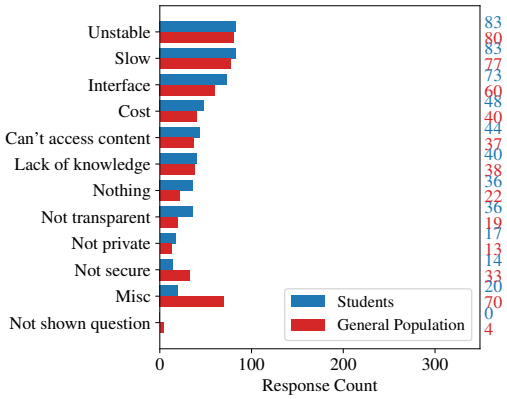

Figure 14: *What do you dislike about your VPN(s)? (response coded by researchers)*

We asked respondents to report in short-answer form what they liked and disliked about VPNs; Figures 13 and 14 show the coded results. The general population appreciated different things about their VPNs than the student population. They tended to value security/safety (109/348) and privacy (104/348) highly. As G327 said:

> Instead of feeling like lots of different users and companies are hoarding and selling data about me, now I only feel like one company is doing it! Hooray!

Slightly more general population respondents liked that their VPN enabled them to access blocked content (86/348), but fewer mentioned access to unspecified forms of content (34/348). Other qualities like convenience and speed were less important.

The general population disliked their VPNs for many of the same reasons that the student population did. They primarily expressed frustration with unstable (80/348) or slow (77/348) VPNs. They also did not like VPNs with poor interfaces (60/348), and some said that VPNs that were too costly (40/348).

Students The most important considerations that student respondents had when choosing between VPNs were cost, security, and ease of use (Figure 12). Student respondents valued privacy relatively less than the general population, and speed and transparency were rated as relatively low priorities, as well.

Figures 13 and 14 show what students liked and disliked about their VPNs. The ability to access blocked content (e.g., geo-restricted video streaming websites), institutional content, or other kinds of content was by far the most commonly liked feature of students' VPNs (223/349). S131 appreciated the ability to have access to many things:

> It allows me to view content that is restricted by a time zone limit like test scores, acceptance letters etc. Also if you're in another country that doesn't allow certain media platforms (e.g., Netflix, Hulu), VPNs allow you to access them.

Other qualities, including security, privacy, and interface design, were less prevalent concerns.

Student respondents did not like slow (83/349) and unstable (83/349) VPN connections. Forty-eight student participants also complained about cost, either in general or for specific features. For example, some students did not like that free VPNs have limited server locations and that they have to pay for additional options.

Interviewees and student respondents differed slightly in terms of how they chose a VPN to use. For most interview participants (19/32), the most important factor was that the VPN provider had a good reputation; three participants added that if their friends had used a VPN before, then they were more likely to use one. When we asked interviewees how they determined whether their VPN provider was trustworthy, 13/32 said they checked to see whether it had good reviews online. Another 10/32 would verify the reputation of the VPN provider through word of mouth, and 7/32 determined trustworthiness based on who provided access to their VPN, such as the university.

We asked interviewees about their general experience and feelings related to VPN usage. We wanted to know whether they saw any differences in their Internet experience when using VPNs. Ten interviewees found the biggest difference was their ability to access blocked content; 8/32 felt more secure. Nevertheless, 10/32 interviewees did not see any difference in the way they used the Internet and did not observe changes in their online habits. P20 noted:

> I sort of have the assumption that any time I use the Internet, any privacy I have is super limited. But you would think that using a VPN would help with that in some way. I don't think it would actually change my behavior online at all, but I think it would definitely make you feel a bit more secure in that.

5 Implications of Findings

Most participants considered data collection by the VPN provider to be a default consequence of using the service. Participants typically had limited understanding of how VPNs work and of data collection on the Internet in general. We view this as cause for concern and perhaps a direct consequence of some of our other findings about users' lack of understanding about the guarantees on data protection VPNs provide. Some of this defeatism and confusion may arise from the conflated nature of the term "VPN", which not only refers to many different functional deployments (e.g., institutional, commercial) but also a variety of use cases from improving privacy to gaining access to restricted content. The term "private" in VPN can be misleading; previous research and studies have shown that users may be surrendering *more* privacy depending on their choice of VPN provider than if they had not used a VPN in the first place [20]. Some users seem to deem this tradeoff as acceptable, in spite of the fact that they also choose their VPN provider on the basis of the privacy guarantees it provides.

Our study's main takeaway is that users ultimately need a better understanding of how VPNs work, as well as the broader implications of VPN data collection. Users could also benefit from better resources to help them to choose a VPN. Future studies could investigate how VPN interfaces could be enhanced to improve mental models of VPN functionality and provide information about the actions and data flows associated with the VPN. For instance, intuitive graphics and tutorials could show how a VPN manipulates and re-routes a user's traffic. Such material could make it clear both how VPNs operate and the parties that still have access to private data. Users may also benefit from concrete demonstrations and examples of what can be inferred from data that VPNs intentionally leak to third parties. Potential tools (e.g., a browser extension) could help users understand (1) what data VPNs may collect about them; (2) what data leaks *outside* of the VPN (e.g., to ISPs, content providers).

Moreover, many users selected VPNs based on cost, and yet at the same time were concerned about whether free VPNs collected and shared data about them. This finding suggests that users not only may have fundamental misunderstandings about how data is collected about them on the Internet, but also that some users may be constrained by cost, ultimately making privacy a luxury good. Although more work is needed to confirm this hypothesis, we expect that both conceptual misunderstanding and cost constraints may be putting certain populations at higher risk of data collection, and future work could also more deeply explore strategies for "privacy equity" among demographics who may need both the education and the financial means to select a safer VPN. The results from this work could also be extended to understand whether user attitudes and awareness about VPN practices translate to other privacy-enhancing technologies, including private-browsing mode on common browsers or with Tor.

6 Conclusion

This paper has explored how different groups of users use VPNs, their mental models and attitudes about data collection by VPN providers, and how and why they choose certain VPNs. This study has revealed several new and interesting themes: (1) The general population uses VPNs more for security and privacy and tends to use VPNs continually. Students also valued these goals but tended to use VPNs more as a means to circumvent access controls; (2) Most participants believed VPNs collect data about them as a default consequence of using these tools, primarily as a means for targeted advertising; and (3) Participants from both groups learned about VPNs around high school and college or, in the case of the general population, later. Future work could attempt to repeat this study with other populations and design interventions to help users understand these risks.

Acknowledgments. This work was supported in part by NSF Award CNS-1953513.

References

[1] Nasser Mohammed Al-Fannah. One leak will sink a ship: Webrtc ip address leaks. In *2017 International Carnahan Conference on Security Technology (ICCST)*, pages 1–5. IEEE, 2017.

[2] Daniel Anderson. Splinternet Behind the Great Firewall of China. *Queue*, 10(11):40, 2012.

[3] Jacob Appelbaum, Marsh Ray, Karl Koscher, and Ian Finder. vpwns: Virtual pwned networks. In *2nd USENIX Workshop on Free and Open Communications on the Internet. USENIX Association*, 2012.

[4] David Armstrong, Ann Gosling, John Weinman, and Theresa Marteau. The place of inter-rater reliability in qualitative research: an empirical study. *Sociology*, 31(3):597–606, 1997.

[5] Veroniek Binkhorst. Improving cyber risk communication: Mental models of vpn in a professional services firm in the netherlands. Technical report, Delft University of Technology, 2020.

[6] Norman M Bradburn, Seymour Sudman, and Brian Wansink. *Asking Questions: The Definitive Guide to Questionnaire Design—For Market Research, Political polls, and Social and Health Questionnaires*. John Wiley & Sons, 2004.

[7] Business Insider. People are furious about Onavo, a Facebook-owned VPN app that sends your app usage habits back to Facebook, 2018. https://bit.ly/2NQW5py.

[8] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[9] CDT Complaint to the FTC on Hotspot Shield VPN, 2017. https://cdt.org/insight/cdts-complaint-to-the-ftc-on-hotspot-shield-vpn/.

[10] Cloudflare. Introducing Warp: Fixing Mobile Internet Performance and Security, 2019. https://blog.cloudflare.com/1111-warp-better-vpn/.

[11] Sauvik Das, Tiffany Kim, Laura Dabbish, and Jason Hong. The Effect of Social Influence on Security Sensitivity. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, pages 143–157, 2014.

[12] Dedoose, 2019. https://dedoose.com/.

[13] Jason A Donenfeld. Wireguard: Next generation kernel network tunnel. In *NDSS*, 2017.

[14] GeoSurf. VPN Usage Statistics, 2019. https://www.geosurf.com/blog/vpn-usage-statistics/.

[15] Global Market Insights. Virtual Private Network (VPN) Market, 2020. https://www.gminsights.com/industry-analysis/virtual-private-network-vpn-market.

[16] Summer Hirst. The History of VPN - How It All Began, January 2018. https://thevpn.guru/history-of-vpn/.

[17] Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. In *Proceedings of the 2016 ACM on Internet Measurement Conference - IMC '16*, pages 349–364, Santa Monica, California, USA, 2016. ACM Press. http://dl.acm.org/citation.cfm?doid=2987443.2987471.

[18] Asela Jayatilleke and Parakum Pathirana. Smartphone vpn app usage and user awareness among facebook users. In *2018 National Information Technology Conference (NITC)*, pages 1–6. IEEE, 2018.

[19] Ruogu Kang. "My data just goes everywhere": user mental models of the internet and implications for privacy and security. In *SOUPS'15 Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, pages 39–52, Ottawa, Canada, July 2015. USENIX.

[20] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. An empirical analysis of the commercial vpn ecosystem. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, pages 443–456, New York, NY, USA, 2018. ACM. http://doi.acm.org/10.1145/3278532.3278570.

[21] Sheharbano Khattak, Mobin Javed, Syed Ali Khayam, Zartash Afzal Uzmi, and Vern Paxson. A look at the consequences of internet censorship through an isp lens. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 271–284. ACM, 2014.

[22] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. "When I am on Wi-Fi, I am fearless": privacy concerns & practices in everyday Wi-Fi use. In *Proceedings of the 27th International Conference on Human Factors in Computing Systems - CHI 09*, page 1993, Boston, MA, USA, 2009. ACM Press. http://dl.acm.org/citation.cfm?doid=1518701.1519004.

[23] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263. IEEE, 2019.

[24] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. Wiley, Chichester, West Sussex, U.K, 2010. OCLC: ocn431936033.

[25] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[26] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. (do not) track me sometimes: Users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies*, 2016(2):135–154, 2016.

[27] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. *Proceedings on Privacy Enhancing Technologies*, 1:83–102, 2020.

[28] NordVPN. Advantages & Benefits of VPN, 2019. https://nordvpn.com/features.

[29] NordVPN. List of NordVPN server locations, 2019. https://nordvpn.com/servers.

[30] PCMag. The Best VPN Services of 2019, 2019. https://www.pcmag.com/roundup/296955/the-best-vpn-services.

[31] Vasile C Perta, Marco V Barbera, Gareth Tyson, Hamed Haddadi, and Alessandro Mei. A glance through the vpn looking glass: Ipv6 leakage and dns hijacking in commercial vpn clients. *Proceedings on Privacy Enhancing Technologies*, 2015(1):77–91, 2015.

[32] Pew Research Center. The state of privacy in post-Snowden America, 2016. https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[33] Erika Shehan Poole, Marshini Chetty, Rebecca E. Grinter, and W. Keith Edwards. More than meets the eye: Transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems - DIS '08*, pages 455–464, Cape Town, South Africa, 2008. ACM Press. http://portal.acm.org/citation.cfm?doid=1394445.1394494.

[34] Quantcast. Quantcast Measure - Free Audience Insights & Analytics Tool, 2019. https://www.quantcast.com/products/measure-audience-insights/.

[35] Emilee Rader. Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google. In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, pages 51–67, 2014.

[36] Johnny Saldañna. *The Coding Manual for Qualitative Researchers*. SAGE, Los Angeles, 2nd ed edition, 2013.

[37] Irving Seidman. *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Teachers college press, 2013.

[38] Fatemeh Shirazi and Melanie Volkamer. What Deters Jane from Preventing Identification and Tracking on the Web? In *Proceedings of the 13th Workshop on Privacy in the Electronic Society - WPES '14*, pages 107–116, Scottsdale, Arizona, USA, 2014. ACM Press. http://dl.acm.org/citation.cfm?doid=2665943.2665963.

[39] Jeff H Smith, Tamara Dinev, and Heng Xu. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4):989, 2011. https://www.jstor.org/stable/10.2307/41409970.

[40] Nissy Sombatruang, Tan Omiya, Daisuke Miyamoto, M Angela Sasse, Youki Kadobayashi, and Michelle Baddeley. Attributes affecting user decision to adopt a virtual private network (vpn) app. In *International Conference on Information and Communications Security*, pages 223–242. Springer, 2020.

[41] William G Stillwell, David A Seaver, and Ward Edwards. A comparison of weight approximation techniques in multiattribute utility decision making. *Organizational behavior and human performance*, 28(1):62–77, 1981.

[42] TechCrunch. Apple removed Facebook's Onavo from the App Store for gathering app data, 2018. https://techcrunch.com/2018/08/22/apple-facebook-onavo/.

[43] Joseph Turow. Americans & Online Privacy: The System Is Broken. Technical report, University of Pennsylvania, 2003.

[44] Steven J. Vaughan-Nichols. How Does a VPN Work?, August 2017. https://www.ign.com/articles/2017/08/11/how-does-a-vpn-work.

[45] Qi Zhang, Juanru Li, Yuanyuan Zhang, Hui Wang, and Dawu Gu. Oh-Pwn-VPN! Security Analysis of OpenVPN-Based Android Apps. In *International Conference on Cryptology and Network Security*, pages 373–389. Springer, 2017.