Practicing Safe Browsing: Understanding How and Why University Students Use Virtual Private Networks

Agnieszka Dutkowska-Zuk, Austin Hounsel*, Andre Xiong*, Marshini Chetty†
Nick Feamster‡, Molly Roberts‡, Brandon Stewart*
Lancaster University, Princeton University*, University of Chicago†, University of California at San Diego‡

Abstract

Despite their name and stated goal, Virtual Private Networks (VPNs) often introduce users to new security and privacy threats. For example, recent studies have shown that VPNs can leak user traffic to third-party trackers. In light of these developments, we set out to understand how and why a highly educated population, university students, chooses and uses VPNs, whether they are aware of data leakages by VPNs, and how their awareness and attitudes about VPNs affects their decisions to use them. To answer these questions, we conducted 32 in-person interviews, a survey with 350 respondents, and a controlled lab study with 11 users, all university students in the United States. We found that, surprisingly, access, cost, and performance trumped privacy concerns for many users; many users even expected that their VPNs were collecting data about them. Even presenting information to users about the data leaked from VPNs to third-party trackers had little effect on their attitudes, suggesting that more work is needed to improve ways to show users what can be inferred from data collected about them.

1 Introduction

Many Internet users employ Virtual Private Networks (VPNs) [22, 34], a technology that encrypts all network traffic from a client device to an intermediate server on the Internet. Many VPN services are now available; large companies ranging from Cloudflare to Facebook now also provide their own VPNs [6, 21, 25]. Some estimates indicate that the VPN market has grown from being worth $16.5 billion in 2016 to $20.6 billion in 2018 [9]. Unfortunately, many VPNs fail to provide even basic security. For example, some VPNs have leaked user traffic, breaking security and privacy claims made by the providers [15, 23]. Other VPNs may capture user traffic and send the data to third parties for targeted advertising [5, 13]. At one point, Facebook Onavo even collected application traffic without notifying users [4, 30].

Given these recent developments, we aimed to better understand how Internet users select VPNs, how and when they use them, and whether information about the security and privacy vulnerabilities of common VPN providers would have any effect on how users selected a VPN, as well as how they used it (including whether they would use one at all). We directed our study towards university students, a population that is generally technically savvy yet also somewhat cost-sensitive. We focused on the following questions:

• Why do students use VPNs?
• How do students choose which VPNs to use?
• Are students aware of the privacy risks that VPNs pose?
• Do students’ attitudes concerning VPNs change when we present them with information about VPNs privacy practices?

To answer these questions, we performed a qualitative study with three parts: (1) in-depth interviews with 32 university students; (2) a large-scale survey of 350 university students; and (3) a controlled laboratory study with 11 university students, involving the use of VPNAudit, a browser extension we developed that shows data leakage from VPNs to third parties.

First, we discovered that most survey respondents were aware that VPNs collect data about users, with about two-thirds of respondents believing that VPNs collect location information. About half of the survey respondents were aware that many VPNs collect information for commercial purposes. Similarly, about two-thirds of interview participants did not believe that VPNs could provide anonymity, with most of the participants using VPNs to access blocked content. Instead, we found that many students chose a VPN based on the cost, performance, and general reputation of the VPN provider. Students considered privacy and security of the VPN as important but secondary factors. Many students understood the intended purpose of a VPN but were not familiar with how a VPN works, which often led to misconceptions and misunderstandings about the privacy guarantees that a VPN could provide. For example, although many students indicated that they used a VPN to protect their data from “companies”, they seemed unconcerned that the VPN provider itself is a company (and sometimes even an advertiser) that is often gathering user data for profit.

After discovering that many students were unconcerned with the data collection practices of their VPN provider (and in fact in many cases expected that their VPN providers collected data about them), we were interested in determining whether we could affect student attitudes about VPNs after showing them concrete information about the types of data that has often been found to leak from VPNs to third parties, including advertisers. To do so, we first designed and implemented VPNAudit, a browser extension that showed to users the extent of traffic that was being passed directly from their browsers to third parties—not being routed through the VPN.
We provide background on VPNs and survey related work. Interestingly, we found that the information that VPNAudit provided to users did not initially change students’ attitudes about VPN usage. We expect that student attitudes may have not been affected either because they did not understand the significance of the information leaks and thus what could be inferred from the information that was leaking to third parties about their browsing patterns, or because these students were not using VPNs to protect their privacy in the first place. Subsequently, however, users’ attitudes changed more measurably when we explained the significance of the data that VPNs leak to trackers. In particular, nearly all of the participants said they were less likely to use a VPN after we explained the extent of information leakage from the VPN.

Our results suggest the need to better inform and educate the general public about the privacy implications of VPNs—especially commercial VPNs. Another important consideration is that our study participants placed cost as an important factor when selecting VPNs. Designers of tools and regulators should also pay attention to equities to make sure that users are not forced to compromise their privacy when using a VPN merely due to considerations of affordability.

2 Background and Related Work

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

2.1 Background

Originally created for enterprises to communicate securely, VPNs rapidly gained broad commercial appeal as personal Internet usage soared [10]. VPNs are one of the many tools that Internet users can utilize to protect against online privacy and security risks. VPNs work by creating a secure, private connection (i.e., a “tunnel”) through the provider’s server through which the user can safely access a destination server [33]. 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 [33]. 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: the user’s IP address is masked, and traffic appears to come from the VPN server’s IP address instead.

Depending on the provider and the user’s goals, VPNs can be used to access destinations on the Internet or on private networks. Users in areas with censored Internet access can utilize VPNs to access blocked content, such as for using Twitter in China [2]. More generally, users can use a VPN to access location-restricted content, such as watching Hulu, a US-only subscription video on demand service, outside the US [19]. Commercial VPN providers often offer multiple servers located in areas with open Internet access, such as the US or Hong Kong [20]. Other VPN users may use VPNs to access content on a private network. For example, a university’s VPN may allow off-campus users to access the university’s library system. Of course, assuming a strong encryption protocol and a trustworthy provider, VPNs also provide better privacy and security in normal, day-to-day Internet usage. Users may want to protect against Internet Service Provider snooping when browsing at home, or against hackers when using unsecured public Wi-Fi hotspots. Although solely relying VPN is not enough to protect an Internet user from the risks of online data collection, it can be very valuable when utilized in tandem with other privacy-preserving tools and tactics such as tracker blockers.

2.2 Related Work

In this section, we discuss related work on data leakages in VPNs, user attitudes on privacy, and user studies of privacy-enhancing technologies.

2.2.1 VPN Data Leakage

Related studies exist on the effectiveness of VPNs, including research on data leakage and traffic manipulation. Researchers studied 14 of most popular VPN providers and found that most of these providers unintentionally leak traffic to websites hosted on IPv6 addresses [23]. More generally, researchers have found that off-the-shelf VPN software is susceptible to passive and active attacks, limiting their ability to provide anonymity for users [1, 3]. Other researchers studied commercial VPN providers and found five providers that implement transparent proxies, which inspect and modify the traffic that users send [15]. Finally, researchers studied VPN apps in the Android marketplace, finding that many of these apps send data to third-party trackers or contain security misconfigurations [13, 35]. There is a lack of literature on VPNs from the end users’ side, regarding their perceptions and usage of VPNs as well as how they relate to their attitudes and behaviors towards privacy and security. Researchers surveyed Pakistani Internet users and found that 57% of respondents used VPNs to access YouTube after the website was censored in 2012 [16]. However, to our knowledge, there are no studies that explore in depth why Internet users configure VPNs and their attitudes on privacy and security. To this end, we gain insights by studying why college students use VPNs and what their usage habits are. In addition, there have been no published usability studies on VPN services. Further exploration is needed on the end user-side of VPNs to better inform their design and messaging.

2.2.2 User Attitudes on Privacy

Other studies have analyzed users’ knowledge of the Internet in general, as well as privacy and security practices. A number of researchers have analyzed users’ mental models in their perceptions of the Internet [17, 24]. In terms of data collection,
Americans are concerned by the online tracking usage of their data by outside entities, but lack an understanding of how their data is used or transmitted [29, 31]. In particular, they expressed higher concern towards how third parties track and collect their data [26]. In general, however, users are confused as to how this online tracking works and how they can protect themselves [28].

Researchers have also tried to find stronger connections to the usage of privacy and security tools. One study suggested that a combination of awareness of, motivation to use, and knowledge of how to use privacy and security tools impacted their usage [7]. However, 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 [14]. The phenomenon of tech-savvy users neglecting to utilize their knowledge to protect themselves could have interesting implications for VPN-focused studies.

3 General Attitudes About VPNs

We first used surveys and interviews to assess students’ general attitudes about VPNs. We explored how and why students use VPNs, their mental models of VPNs, how they choose which VPN to use (and which ones they choose), and their awareness and attitudes about data collection practices of VPN providers.

3.1 Method

To understand students’ general attitudes about VPNs, we conducted 32 qualitative interviews [27] and a large scale survey with 350 college students from one of our institutions.

3.1.1 Interviews

Before participating in a semi-structured interview, participants were asked to fill out a consent form and a short questionnaire, where we collected demographic information and data about their general online habits and behavior. We collected their academic majors and other basic demographic information such as age, gender, and course of study. The interview guide was structured to first get a better understanding of participants’ knowledge and background and participants’ general privacy and security awareness. First, we 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. We then asked participants to describe how a VPN works. Next, we asked how they learned about VPNs and what their first experience using a VPN was. We then asked how participants choose to use a particular VPN and how and why they use a VPN, how participants felt when using a VPN, and whether they use a paid or free versions of VPNs. Finally, we asked about VPN issues and improvements, students’ knowledge and usage patterns of different VPN types, including specific VPNs they had used, about reasons for selecting and using VPNs, perceptions of data collection by VPNs, and any other issues that they faced.

Recruitment. We recruited 32 interview participants. Table 1 shows demographic data of the interview participants, who were mostly 18–24 years old and undergraduate students (81%). We filtered for students who had used a VPN before, and for students that are currently enrolled in a U.S. university undergraduate or graduate program. We aimed to recruit a variety of international and domestic students living in the United States. We concluded that such diverse group would expand our knowledge and understanding on 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 were conducted on a university campus. Four interview participants did not give consent to recording, so detailed notes were taken during these interviews. All other interviews were audio-taped.

Data Analysis. We first transcribed all recorded interviews and developed an extensive codebook to apply to the interview transcripts and field notes. We used the Dedoose platform [8] for all interview analysis following a standard inductive coding approach [27]. One of the research team coded all of the interview transcripts and a second member of the team reviewed the codes. We had 1906 codes in total, including 45 parent codes such as Guidelines when choosing VPN and Possible improvements; and 1861 child codes such as Good reputation of VPN and More user-friendly. Once the transcripts were all coded, the researcher involved in coding wrote up summaries of the coded transcripts and themes arising from this initial analysis phase. The rest of the research team reviewed the summaries and held regular research meetings to decide on the final themes arising from the interviews.

3.1.2 Survey

Based on the interview data and analysis, we then designed a larger-scale survey to complement our interviews data and expand our knowledge about VPN users’ perspective. 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 academic majors and other basic demographic information such as age, gender, and course of study. We also collected background information about respondents’ perception and concern about online data collection, including the nature of 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.

We asked similar questions as in the interviews, but 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 [18]. We included two attention check ques-
tions 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, in order to avoid response bias.

**Recruitment.** For the survey, we recruited undergraduate and graduate students from a large university to take the survey on Qualtrics. We sent email invitations to a random sample (containing 2,748 people) of the university population via an institutional survey research center. We aimed to reach at least 5% of the university’s VPN-using student population as recommended by Lazar [18]. We launched and conducted the survey between February 2019 and March 2019. Our large sample size allowed us to collect 452 responses, of which 350 were completed, passed our attention checks, and fit our recruiting criteria. Our final sample of 350 valid and completed responses is large compared to university’s overall population (4.3%). Table 2 shows detailed demographic data of the respondents. As expected, the majority of them were age 25 and under (79%). Participants with complete valid responses were entered into a draw for one of two $250 Amazon gift cards.

**Data Analysis.** We used Qualtrics and R to analyze the survey data. We first analyzed the response data using tools built-in with Qualtrics. We limited our analysis to the 350 valid and complete responses. First, we performed descriptive analysis on all the survey questions. The respondents were required to answer each question that was shown to them, but certain questions were only shown when applicable. As such, questions that have fewer than 350 data points contain responses from every applicable respondent; a lack of response does not indicate a respondent’s choice to abstain, unless it was an open-ended question. In presenting our results, we discuss percentages in terms of the number of people who were shown the question. However, the figures presented in this section show percentages in terms of the total number of respondents (350), and include “No Answer” values for those who were not shown the question. We qualitatively coded the open-ended answers in a similar fashion to the interviews using a code book that was developed based on multiple reads through the responses. 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 350 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 $r$.

### 3.1.3 Limitations

We interviewed 32 participants to better understand how the students in our study interact with VPNs. Our sample was not varied in terms of drawing on people who were not based in the United States or from other universities. Our survey also has some inherent drawbacks. Recall bias is difficult to avoid in any survey [18]. Our survey and interviews were not completely anonymous as they required survey participants who wished to enter the raffle and all interview participants to submit an email. Additionally, interview participants were asked to meet with one of the research team in person. This could introduce error in the respondents’ levels of honesty. Future research could build on our results using other methods.

Finally, our survey pool was limited to one U.S. institution’s students, and our interview pool was mostly limited to the same institution’s students. Such data may not be representative of all university students, or even all university students in the U.S. Future research could replicate our study with a more general college student population, or with other populations of interest. (To assist with reproducing this study for other populations, we will release our survey instrument and interview scripts.)

### 3.2 Results

We explore students reasons for using VPNs, whether they understand what VPNs do and how they work, which VPNs students choose to use, and whether they are concerned about the data collection practices of VPN providers.

#### 3.2.1 How and Why Students Use VPNs

We found that although privacy is of some concern for students, it is often secondary consideration. Furthermore, most students do not use VPNs regularly. When students do use VPNs, it is mainly to access blocked content and institutional materials, not to protect privacy.

**Students mostly use VPNs to access blocked content and institutional materials.** Most survey respondents used a VPN to access institutional materials when off campus (66%) (Figure 1). More survey respondents reported using a VPN to bypass Internet censorship (48%) than those wanting to protect privacy or security. However, privacy and security were important factors with 27% of respondents selecting both and 40% selecting at least one of the two as a reason.
For those who specified “Other”, students commonly reported using a VPN to access Advanced Placement (AP) scores, as S108 notes: “To access AP scores early (they were releasing them one time zone at a time to prevent too much web traffic)”. Similarly, most interview participants (21/32) reported that they use a VPN to bypass geographic firewalls, and to watch movies or TV shows online (15/32). For eleven interview participants, accessing blocked content was the priority when using a VPN as P24 describes in a typical example we heard:

I found out that I couldn’t access the application or login to my account through the phone application, because I wasn’t in the United States(…). And I downloaded, I think it’s called Express VPN. And that was able to help me work around the location, geographical issue, and access the account so I could cancel the subscription.

In another typical example, P11 spoke of using a VPN for news websites that were not blocked but had different or limited content depending on IP address of the Internet user. As they were from United Kingdom (UK), they wanted to access the UK BBC website while they were in the US. Also, P26 shared that they used a VPN in order to help their mom:

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.

Many students were not using a VPN for privacy reasons. Only 40% of survey respondents said that they usedVPNs to protect their privacy and/or for their security. We asked these respondents to choose and rank who they were protecting themselves from when using a VPN. Most of these survey respondents ranked companies, hackers, the government, and websites as top concerns. Fewer participants were concerned about other governments or inside threats from friends and family as shown in Figure 2.

Similarly, thirteen interview participants admitted that privacy was not the main reason for using a VPN. Fewer (7/32) used it to protect their personal information and at least four wanted a VPN to be secure and keep them anonymous, such as, P21:

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.

A few interview participants (3/32) used VPNs because they liked the idea that there was a “free” space on the Internet. For these types of participants, using a VPN could be a strong statement that security is important, as P25 explains:

It’s why Private Network Access got so popular. They tried to subpoena the guys to release information about some of the people who used the VPN, and then they actually didn’t have it on their servers. So people knew that they didn’t keep records, so everybody started using that one.

Yet, some interview participants were unconcerned about how trustworthy VPNs were. For instance, five interview participants said they would use a VPN while on public Wi-Fi and four while traveling.

Students VPN usage is irregular and on an as-needed basis. Overall, VPN usage appeared to be more irregular and on an “as needed” basis amongst both survey respondents and interview participants. Most survey respondents (58%) reported they did not currently use a VPN, with only 42% survey respondents reporting that they currently use a VPN. When asked how often survey respondents use a VPN, 86% reported

| Age      | # | %  | Gender    | #  | %  | Origin         | #  | %  | Educational status | #  | %  |
|----------|---|----|-----------|---|----|----------------|---|----|-------------------|---|----|
| 18 to 25 | 275| 79%| Female    | 178| 51%| United States  | 258| 74%| Graduate Students  | 123| 35%|
| 26 to 35 | 74 | 21%| Male      | 172| 49%| International | 92 | 26%| Undergraduate Students | 227| 65%|
| 36+      | 1 | 0% |           |    |    |                |    |    |                   |    |    |

Table 2: The distribution over age, gender, origin and education status for 350 survey participants, at the time of collecting the data. Our 92 international participants came from 32 different countries.
only using a VPN sometimes or rarely. A minority reported using a VPN all the time (3%) or most of the time (11%). Most of these survey respondents who had stopped using a VPN (58%) (Figure 3) reported that they were no longer location restricted (45%), did not have anything to hide (37%), and/or simply did not use it enough (34%). Very few respondents reported a lack of security (1%) to be a contributing factor in their decision to stop using VPNs.

3.2.2 Mental Models Of VPNs

Students generally know what VPNs do but they are less familiar with how VPNs work. We first asked participants about their perceptions of VPNs and discovered that most had a fairly good idea about the purpose of a VPN. However, most participants gave incomplete explanations of how VPNs work. When asked what a VPN is (Figure 4), most survey participants could list features of a VPN such as location spoofing (44%). 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 (38%). For example, S283 reported:

It’s been described to me as an “Internet condom.” It protects your Internet information by setting up a different IP address.

Other survey respondents defined a VPN as an intermediary (24%), for example S78 reported that “It’s a porthole to allow private communication/data transfer between two devices.”. Only 3% of survey respondents said they did not know how to define VPNs.

Similarly, almost half (14/32) of the interview participants 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 explains:

It’s sort of a middle man. So instead of you actually downloading the file from somewhere 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 in participants, P25 described a VPN as:

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’s what VPNs are to me.

3.2.3 How Students Choose VPNs

Students often start using VPNs before entering university, and rank cost, security, and ease of use ahead of privacy. Most students also liked VPNs more for their utility to access content rather than privacy and security.

Many university students learn about VPNs in high school. Many survey respondents reported first using a VPN in university (44%) and high school (35%) (Figure 5). This sentiment was echoed by several interview participants who elaborated on the reasons why VPNs were needed in high school in particular. Typifying what we heard, P20 told us how he used it to get access to sites 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 school, I went to boarding school 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
download a graphics editor, which they could not afford in
high school:

The school 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 school project. I
think I was maybe 16 at the time.

Nevertheless, some interview participants found it hard to
learn about VPNs, as P18 admitted:

I’ve actually never heard VPN’s brought up in conversa-
tions amongst my friends. That’s because I think they’re
pretty obscure at the moment. The usage of this VPN sort
of hinges on two things, the desire to obtain copyrighted
material for free and also the knowledge of the existence
of VPN’s. Those are two I think pretty big bottlenecks
that sort of limit this sort of information to sort of tech
nerds.

The most important considerations are cost, security, and
ease of use. As shown in Figure 6, the most important con-
siderations as ranked by survey respondents for choosing
between VPNs were cost, security, and ease of use. Just under
half of the participants also valued privacy and speed. Inter-
view participants also noted that the reputation of the VPN
provider was also an important consideration. Transparency
was rated fairly low overall. On the other hand, for most in-
terview participants (19/32), the most important factor was
that the VPN provider had a good reputation; three interview
participants added that if their friends had used a VPN before,
then they were more likely to use one. Ten interview partic-
ipants had various security and privacy requirements, such
as making sure that the VPN had a secure network, that the
VPN provider did not store any of user’ records, that the VPN
provider did not sell users’ information, and that the VPN
protects users’ data. For one participant it was important that
a VPN did not require any personal information when setting
up the account and another one wanted an option of secure
payment. When we asked interview participants how they de-
termined whether their VPN provider was trustworthy, 13/32
said they checked that it had good reviews online. Another
10/32 would verify that through word of mouth and 7/32 knew
it was trustworthy because of who provided access to their
VPN, such as the university.

Our interview participants also indicated that ease of use
(8/32), speed (7/32), cost (6/32), and ease of set up (5/32) were
important. Five interview participants said that they looked
at the price before purchasing a subscription; five said that
it was important that VPN was for free; and four said that
would always choose a cheaper option. For example, for P11,
the main factors were word of mouth, experts’ opinion, cost
as well as customer service available:

I look on, Tech Radar and PC Monitor, those kinds of web-
sites, (...) I get some reviews from friends (...) So, when
I came to China I was deciding between Express and
Astro, and I just looked on their websites, went through,
server locations, cost, and their privacy policies, (...) available customer service, which was very important as
well.
Students value access to content over security and privacy. We asked survey respondents to report, in short-answer form, what they liked and disliked about VPNs, as shown in Figure 7 and Figure 8. The ability to access restricted content was by far the most commonly liked feature of students’ VPNs (64%). S131 appreciated that they could have access to a variety of 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 received far fewer mentions. Survey respondents did not like slow (24%) and unstable (24%) VPN connections. S192 shared their frustration:

The connection is very slow and unstable, and it would often turn off while I was accessing the Internet so that I would have to reload everything.

Survey respondents did not like the complexity of interfaces and their features. As S306 explained:

It is annoying to log into all the time, and it automatically logs me out after a designated amount of time.

and S279:

It is difficult to use and the set-up process is confusing. Selecting a new VPN is very confusing because there are so many options.

14% of survey participants also complained about the cost of VPNs. For example, they did not like that free VPNs have limited server locations and they have to pay for unlocking additional locations.

3.2.4 Which VPNs Students Choose

Students feel most comfortable with using VPNs provided by their institutions. They are puzzled as to whether commercial VPNs actually provide privacy and security over Internet. Thus, they believe that a university VPN is a safer choice.

University VPNs are most prevalent. Most survey respondents used the VPN offered by their college (65%). Nearly half also used free commercial VPNs (49%). A smaller fraction of students used paid commercial VPNs (28%). Figure 9 summarizes these results.

Students feel safer using their university VPN. Students were more comfortable with the VPN provided by their school and paid VPN providers than free VPN providers. Figure 12 shows that, more survey respondents felt safe using the university or employer provided VPN than with free VPNs.

When asked whether it was important who their VPN provider was, 11 interview participants reported that it was important, especially for those who used university’s VPN (7/32), which was reassuring for them that this VPN was safe. Interviewees were split on what they were willing to do on-
Students are confused about whether paid VPNs provide more privacy. 22 interview participants reported that they would use free VPNs while ensuring it was safe, and nine said that they would not use them because they did not feel safe. Nevertheless, many were confused about the benefits of using a free versus paid VPN as expressed by P24:

I think the one that you have to pay for is more trustworthy. But, it could easily be the other way around. Just because you have to pay for something doesn’t mean that it is more reliable, or even more efficient. But, I do think that the paid ones generally people might think that they are more safe to use. And that their information may be more secured, just because of that added price tag on it.

### 3.2.5 Expectations About VPN Data Collection

Students were skeptical about VPNs’ data practices. They were aware their data could be collected, but they did not necessarily understand the consequences of the data collection practices.

Students believe that VPN providers collect data about them. 74% of survey participants believed that their VPN provider could collect their data. Figure 13 shows that most of these respondents believed that VPNs collects data for commercial motives (68%), or simply because data collection is a “default consequence of using the Internet” (68%). Around half of these respondents (49%) selected both of those options. Very few survey respondents believed that the motives for data collection were nefarious (such as blackmail, 3%) and a good proportion of survey respondents either gave no answer or selected “I don’t know” (10%). Interestingly, most interview participants (23/32) similarly believed that VPNs collect their data, with some expressing that VPNs keep information for user statistics or to sell the data. For example, P32 believed that it added security, and one 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.

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

Students think that VPNs collect location data and online activity, but they do not know who has access to that data. We asked survey participants who believed that VPNs collected their data what they think VPNs collect. As shown...
in Figure 14, most survey respondents believed that VPNs collect information about location (87%) and online activity (74%). Fewer believed that VPNs collected private messages (17%), recordings (15%), or keystrokes (15%). Some survey respondents did not know what data was collected (10%). There was also little consensus between survey participants on who had access to the data collected by VPNs. The largest proportion of survey respondents, as shown in Figure 15 believed that companies (43%) and the government (34%) had access to the data. A smaller number believed that only the VPN had access (18%) and 19% of survey respondents indicated that they did not know where their data went.

Figure 16 shows that these survey respondents, who believed that their VPN shared their data (61%) generally thought that their location (74%), online activities (70%), interests (58%), and demographic information (57%) were shared. Fewer believed that private messages, recordings, or keystrokes were shared, which is in line with what survey participants believed VPNs were able to collect in the first place. We also asked interview participants about their opinion on VPN data sharing practices. When asked whether they thought their VPN providers could be sharing their information, 17 responded “no” and 11 “yes”, but 12 were uncertain about their response, because they did not feel like they would be able to know anyway. For example, P26 explained:

If they share it with someone, then they’re not sharing it in a way that I would be able to tell, because, for example, I’ve never seen personalized ads from things that I’ve looked at while on the VPN.

From the interview participants who said that VPN providers do not share information with other entities, eight confessed that they hope their information was not being shared, and five admitted that while their VPN providers do not share any information, other VPN providers may do so. Two of these participants believed that even though their VPN providers do not share data with others on regular basis, they would with legal authorities. For instance, P14 shared:

If the Chinese government were to really threaten them. This is a very hypothetical situation. I think information which they could be able to collect and which would be interesting would probably be something like on a service level, the actual content that you’ve been accessing. Like the actual service or addresses which you’ve accessed recently as well as the associated file or data which is generated while somebody is accessing the Internet.

Students do not expect anonymity from VPNs. Students generally did not feel that VPNs provided total anonymity. Three quarters of survey respondents indicated that they thought their VPNs guaranteed access to certain content (75%) and masking of their IP addresses (53%). However, only around one third of survey respondents believed that their VPNs guaranteed privacy (36%), anonymity (30%), and safety from tracking (28%). Similarly, more interview participants did not believe that VPNs guaranteed them anonymity (20/32) than those who felt the VPN did offer privacy and anonymity (8/32). In fact, three quarters of interview participants (24/32) told us that you can be tracked while 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). In a quote that illustrates the sentiment, participant 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...
Some interview participants were convinced that the government could track you even while using a VPN. For example, P30 used a VPN only in different countries to access blocked content. They did not continue to use a VPN in the US as they did not need a VPN to access content anymore and did not see any privacy advantages because all VPNs are “partially, controlled or transparent to the government”. Other interview participants explained one can still be tracked by advertising agencies even if the VPN makes tracking at least harder than normal. To overcome tracking issues, P21 explained that using a VPN is not enough and instead they changed locations frequently when they connected within VPN:

Yes [I can be tracked while using a VPN], especially if I’m using the same IP address. That creates a problem because my Internet footprint… Or Chrome, for example, my web browser could definitely still track me and connect that, see where I’ve been connecting from. Or Gmail could see that. Gmail always tells you, “Oh, you’ve connected from this weird device, or from this location that we don’t recognize.” So I think you can definitely still be tracked.

4 Attitudes About Data Leakage from VPNs

The results from Section 3.2 showed that most students use VPNs to access institutional and geoblocked content; privacy is an important but secondary concern. However, with respect to privacy, we did not ask students about VPN data leakages in the interviews or survey. In particular, beyond collecting data about users, some VPN providers intentionally send data about user behavior to third parties. We wanted to investigate the extent to which students are aware of and concerned about data leakages from VPNs.

For example, Hotspot Shield—a free VPN provider with over 650 million downloads—sends browsing data to select trackers through its Google Chrome extension and mobile application [5, 11]. For example, if a website contains trackers hosted by analytics.google.com (owned by Google), pixel.quantserve.com (owned by Quantcast), or event.shelljacket.us (ownership unknown), then any connections to these trackers are created outside the VPN on Google Chrome. This practice allows Google and Quantcast to see which websites users are visiting, even when the VPN is enabled. Users are not informed that this data is being sent anywhere on the extension’s user interface. Furthermore, the privacy policy for Hotspot Shield states that “Hotspot Shield does not share your browsing history or any other information you choose to provide, with advertisers” but does not explain why Google and Quantcast can track users [12].

4.1 Method

To investigate student attitudes about VPN data leakages, we conducted a controlled laboratory study in which we gave students concrete data about such leakages through a Google Chrome extension.

4.1.1 Background Video and Ratings Survey

Lab sessions lasted about one hour; we recorded audio from these sessions and compensated all participants with a $20 Amazon gift card. We first asked the participants to watch a short video on the website for Hotspot Shield about how VPNs work. We instructed them to watch this video so that each participant would have a general understanding of the claims that popular free VPN providers like Hotspot Shield make with respect to privacy. After the video ended, we asked the participants to browse the Hotspot Shield website as they normally would if they were interested in learning more about the VPN provider. Once each participant finished browsing the website, we instructed them to turn on the Hotspot Shield Chrome extension on a research team member’s computer and configure it to their liking. We used this separate computer to protect the privacy of the participants.

We then gave the participants a set of tasks to complete while Hotspot Shield was enabled. The tasks required the participants to click on links to find information about certain categories of topics. In total, there were three tasks for each of three categories: entertainment, sexual health, and mental health. With each task, we instructed the participants to imagine that they were using their own computer to find information about topics that belonged to these categories. For example, one of the tasks for sexual health reads as follows: “Imagine that you are interested in learning about the symptoms of Chlamydia. Visit the following link to find five signs of Chlamydia, and write them down.” We also asked the participants to think aloud for the duration of the study, noting anything that was of interest to them [32].

Once the participants completed the first set of tasks, we asked them to rate how likely they would be to use Hotspot Shield on a scale of 1 to 5, with 5 being the “most likely” rating. The participants were not informed that Hotspot Shield sends browsing data to certain trackers outside of the VPN. We also asked the participants a series of follow-up questions to gather their baseline thoughts about Hotspot Shield.

4.1.2 Browser Extension: VPNAudit

We developed VPNAudit as a Google Chrome extension to show participants privacy leaks in Hotspot Shield. The extension works by examining webpages that participants visit while using Hotspot Shield, and it looks for the Google Analytics, Quantserve, and Shelljacket trackers listed in Section 5. It then counts the number of unique webpages that these trackers were present on. The data for each tracker is shown to users in a pop-up window when they click on the icon for the extension. When a user clicks on the name of a tracker in the pop-up window, they see a list of each unique webpage under a heading that reads “Browsing history sent to tracker”. It is important to list these webpages because it allows the
participants to visualize what information about themselves that trackers can infer from browsing history.

We showed the participants VPNAudit before giving them another set of tasks. At this point in time, we did not explain what information the extension was showing because we wanted to see if the participants understood the extension without our intervention. We simply pointed to the extension, showed them how to access it on their own for the remainder of the study, and informed them that it was collecting the displayed information while they were completing the first set of tasks.

The second set of tasks we asked them to complete used the same categories as before: entertainment, sexual health, and mental health. However, the tasks themselves were not the same within each category. For example, in the “sexual health” category within the first set of tasks, we asked the participants to look up information related to Chlamydia. In the “sexual health” category within the second set of tasks, we asked the participants to look up information related to HIV. We chose different tasks to ensure that the participants would be attentive throughout the study. We emphasize that the tasks were carried out on a research team member’s computer to protect the participants’ privacy.

Once the participants completed the second set of tasks, we again asked them to rate how likely they would be to use Hotspot Shield on a scale of 1 to 5, with 5 being the “most likely” rating. Finally, we showed participants articles about the HotSpot Shield data leakages and discussed the implications of these leaks and what could be inferred with them. Following these discussions, participants were asked to rate how likely they would be use Hotspot Shield a final time, again on a 1 to 5 scale. Finally, we asked the participants a series of follow-up questions to assess their understanding of VPNAudit and to understand their views on VPN data leakages.

4.1.3 Recruitment and Participants

Table 3 summarizes the demographic information of our participants. We recruited participants from the same university as in the first two parts of the study, again via the institutional survey center. In total, 64 people responded to our recruitment e-mails but some were ineligible as they had completed the interview or survey or were not students. We were able to conduct our study with 14 of the 65 eligible participants. We had to discard three interviews because of audio related issues and because we later discovered that two of the participants had participated in the survey and interview portion of our study, which left us with valid data from 11 participants.

With respect to VPN usage, seven participants indicated that they had used institutional VPNs, and three participants indicated that they had used a paid, commercial VPN. Finally, all of our participants were students at a particular university.

4.1.4 Data Analysis

We used similar analysis procedures to the first parts of our study such as transcribing and qualitatively coding the interview data using a codebook and review by multiple team members to reach consensus on the final results.

4.1.5 Limitations

There are several limitations of our participant demographics. For example, our sample size was limited to 11 participants, which means that our findings cannot generalize to all university students. Our participants were also mostly Computer Science students that may be more technically sophisticated than students of other disciplines. Most of our participants were from the US, which limits our ability to understand how international students think about privacy with respect to VPNs. Finally, all of our participants were students at a particular university.

4.2 Results

The participants gave a median rating of 3.5 and 4 before and after using VPNAudit, respectively. Eight participants did not change their ratings. P8 was more willing to use Hotspot Shield after we showed them VPNAudit because the VPN seemed easy to use and was not “obtrusive”. We marked several of the ratings between two integers when participants gave two ratings in their response. P3 and P5 indicated that they would still use Hotspot Shield after being shown VPNAudit because they believe trackers would somehow track them even if Hotspot Shield did not leak their data. P3 expounded on this:

Even with the tracking turned off, there’s all sorts of techniques they use. So this stuff doesn’t really, or the tracker stuff doesn’t really surprise me or change my opinion. Because you have to do additional stuff to prevent that anyway.

Two participants indicated that they do not care if Google Analytics could track them. P4 said that they “just look up random things all the time”, so they are not concerned about Google knowing what they are looking up. However, if Google knew that they were actually buying a “home medical test”, for instance, then they would be concerned. P1 gave a more detailed answer:

Table 3: Demographics of laboratory study participants.
To be honest, I’m not that worried about it in general. Selling data or privacy of data, because I feel like ... I don’t know, I’ve just never been that worried about privacy of data in general. I would be worried about privacy of personal information that you used when using your credit card and stuff like that. I would be more worried about that, and that would be protected by the website, as opposed to by the VPN.

After completing the second set of tasks with VPNAudit, five participants believed that they did not need Hotspot Shield for the tasks we gave them. For example, P5 was concerned about trackers having information that feels personal to them, but not other kinds of information:

I guess the medical conditions of HIV and Chlamydia probably would be more sensitive... but for a movie I might watch, and even a therapist, I think I wouldn’t really mind as much just because I could be searching for it, someone else, etc.

In general, participants had an incomplete understanding of what VPNAudit was showing them. Seven participants explained that data was being sent to Google and Quantserve while they were completing the tasks. However, five of these participants did not attribute this behavior to Hotspot Shield deliberately leaking their data. Interestingly, two participants thought that VPNAudit itself was a tracker. In summary, these preliminary results suggest that most participants were not concerned about data leakages to trackers, even after using VPNAudit.

After we explained to participants the types of inferences that were possible from leaked data, they gave a median rating of 2.5 and said they were less likely to use Hotspot Shield in the future. The participants generally felt that the VPN provides less privacy than they previously expected. P2—who gave a 1 for their third rating—typifies this sentiment:

Now I don’t believe the VPN helps me achieve the sort of stated purposes. It doesn’t seem that it guarantees anonymity to the extent that I want, like complete anonymity.

However, we gathered data for only 11 participants, which limits our ability to generalize. We also believe VPNAudit could be better designed to improve inference literacy.

5 Discussion

Our research highlights several important findings. First, some student attitudes which initially appear contradictory suggest significant gaps in mental models about the advertising and data collection ecosystems. Specifically, many students said repeatedly that they were unconcerned about whether VPNs collected data about them, while at the same time expressing that they primarily used a VPN to protect their data from “companies”. This logical discontinuity clearly overlooks the fact that commercial VPN providers are themselves companies—and some of these providers even profit from the collection and sharing of user data. Students’ concern with data collection from companies also implies that they should be more concerned about data leaks to third-party trackers than they were, based on the information that we provided them from VPNAudit.

Second, we discovered that users tend to care more about privacy when they discover the types of information that can be inferred from the data that is collected by VPN service providers and leaked to trackers. Yet, even when we presented this information to students via the VPNAudit tool, many did not express concern about the data that was being collected about them until we explained this in depth to them. Ultimately, students need more scaffolding to reason about the information that VPNs collect about them as well as how that information can be used.

This insight points to important future work in improving inference literacy concerning VPNs. Users can benefit from tools that concretely demonstrate what can be inferred from the information that leaks from VPNs. For example, students were aware of the type of information that VPNs collect, such as location, but could not appreciate the concrete implications of these data leaks. Better tools to improve inference literacy could help students make more informed decisions about when and how they use VPNs, as well as which VPNs to use.

Ultimately, the responsibility for informing students about the capabilities, shortcomings, and data collection (and leakage) behaviors of VPNs rests with multiple parties. The VPN providers themselves could be more forthcoming about the data that they collect, as well as the information that is leaked to trackers outside of the VPN; absent cooperation from the VPN providers, of course, a third-party service could surface this information to users. Our initial studies with VPNAudit suggest that it is difficult to entice users to care about VPN data collection and data leakage, however, even when they are presented directly with the information. More work is needed from researchers and third parties about the extent of inference that is possible from the data that VPNs collect and leak to third parties and how best to show this to users.

6 Conclusion

In this paper, we explored how university students choose virtual private networks, how they use them, and their general attitudes about data collection by commercial VPN providers. Through interviews, a large scale survey, and a controlled laboratory study, we discovered that (1) many students choose a VPN primarily to circumvent network controls, to gain access to blocked content; (2) concerns about privacy were important but secondary; (3) students use VPNs to achieve a pragmatic goal and understand what generally what they do but not very much about how they work; (4) students generally expect their VPN provider to be collecting data about them; and (5) students were unable to infer the implications of data collection, even after being shown concrete data about data leakages to third parties in our VPNAudit tool. It became clear through our study that although students valued privacy in the abstract,
the choice of VPN software and provider was ultimately a pragmatic question of network access, performance, and cost. Given the existing practices of VPN providers, from data collection about users to well-documented and studied data leakages from VPNs, students (and users in general) could benefit from better tools and interventions that explain the risks that they assume when choosing and using a VPN—and that many of them, in spite of their name, may not provide much in the way of privacy.

References

[1] N. M. 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] D. Anderson. Splinternet Behind the Great Firewall of China. Queue, 10(11):40, 2012.

[3] J. Appelbaum, M. Ray, K. Koscher, and I. Finder. vpwns: Virtual pwned networks. In 2nd USENIX Workshop on Free and Open Communications on the Internet. USENIX Association, 2012.

[4] 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/2NZW5py.

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

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

[7] S. Das, T. Kim, L. Dabbish, and J. 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.

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

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

[10] S. Hirst. The History of VPN - How It All Began, Jan. 2018. https://thepvpn.guru/history-of-vpn/.

[11] Don’t Drink Hotspot Shield’s Kool-Aid. https://blog.windscribe.com/dont-drink-hotspot-shields-k-cool-aid-a190798dd2c02?gi=71a54d46e48. Accessed: 2019-05-27.

[12] Hotspot Shield Privacy Policy. https://www.hotspotshield.com/privacy/. Accessed: 2019-05-27.

[13] 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 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.

[14] R. 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.

[15] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez. An empirical analysis of the commercial vpn ecosystem. In Proceedings of the Internet Measurement Conference 2018, IMC ’18, pages 443–456, New York, NY, USA, 2018. ACM. http://doi.acm.org/10.1145/3278532.3278570.

[16] 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, pages 271–284. ACM, 2014.

[17] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. 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.

[18] J. Lazar, J. H. Feng, and H. Hochheiser. Research methods in human-computer interaction. Wiley, Chichester, West Sussex, U.K, 2010. OCLC: ocn431936033.

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

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

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

[22] PCMag. What Is a VPN, and Why You Need One, 2019. https://www.pcmag.com/article/352757/you-need-a-vpn-and-heres-why.

[23] V. C. Perta, M. V. Barbera, G. Tyson, H. Haddadi, and A. 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.

[24] E. S. Poole, M. Chetty, R. E. Grinter, and W. K. 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.

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

[26] E. 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.

[27] L. Seidman. Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences. Teachers college press, 2013.
[28] F. Shirazi and M. 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.

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

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

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

[32] M. Van Someren, Y. Barnard, and J. Sandberg. The think aloud method: a practical approach to modelling cognitive. Citeseer, 1994.

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

[34] Wired. If You Want a VPN to Protect Your Privacy, Start Here, 2017. https://www.wired.com/2017/03/want-use-vpn-protect-privacy-start/.

[35] Q. Zhang, J. Li, Y. Zhang, H. Wang, and D. Gu. Oh-Pwn-VPN! Security Analysis of OpenVPN-Based Android Apps. In International Conference on Cryptology and Network Security, pages 373–389. Springer, 2017.