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

Abstract: Virtual Private Networks (VPNs) can help people protect their privacy. Despite this, VPNs are not widely used among the public. In this survey study about the adoption and usage of VPNs, we investigate people's motivation to use VPNs and the barriers they encounter in adopting them. Using data from 90 technologically savvy participants, we find that while nearly all (98%; 88) of the participants have knowledge about what VPNs are, less than half (42%; 37) have ever used VPNs primarily as a privacy-enhancing technology. Of these, 18% (7) abandoned using VPNs while 81% (30) continue to use them to protect their privacy online. In a qualitative analysis of survey responses, we find that people who adopt and continue to use VPNs for privacy purposes are primarily motivated by *emotional* considerations, including the strong desire to protect their privacy online, wide fear of surveillance and data tracking not only from Internet service providers (ISPs) but also governments and Internet corporations such as Facebook and Google. In contrast, people who are mainly motivated by *practical* considerations are more likely to abandon VPNs, especially once their practical need no longer exists. These people cite their access to alternative technologies and the effort required to use a VPN as reasons for abandonment. We discuss implications of these findings and provide suggestions on how to maximize adoption of privacy-enhancing technologies such as VPNs, focusing on how to align them with people's interests and privacy risk evaluation.

Keywords: privacy, Virtual Private Networks (VPNs), judgment and decision making, psychology, privacy-enhancing technologies

DOI 10.2478/popets-2020-0006
Received 2019-05-31; revised 2019-09-15; accepted 2019-09-16.

***Corresponding Author: Moses Namara:** Clemson University, mosesn@clemson.edu
Daricia Wilkinson: Clemson University, dariciaw@clemson.edu
Kelly Caine: Clemson University, caine@clemson.edu
Bart P. Knijnenburg: Clemson University, bartk@clemson.edu

1 Introduction

In recent years, increased levels of mass surveillance and data collection have contributed to significant privacy concerns from end-users worldwide [1]. In the United States, Congress enacted a Congressional Review Act to repeal existing privacy rules that required Internet Service Providers (ISPs) to seek permission from its customers to collect and share personal information such as their browsing history [2, 3]. This has driven privacy advocates to motivate internet users to explore privacy-enhancing technologies such as Virtual Private Networks (VPNs) as a technology that can provide an additional layer of privacy protection and anonymity when using the Internet [4]. VPNs are secure communication technologies that were originally developed to connect remote sites or users together over a public network [5]. They have evolved into a consumer tool that is used to provide users with an Internet Protocol (IP) address that is not subject to the censorship rules of their geographical location, as well as to hide users' browsing behavior from surveillance [6]. As a result, they are now widely marketed as privacy-enhancing technologies (PETs) [1] that allow internet users obscure and protect their personal identifiable information, including their online traffic, not only from their ISP, but also from their governments, and other online entities [7].

Around the world, adoption and usage of VPNs is much higher in Asia-Pacific (i.e., 30% of internet users) and Latin America (i.e., 23% of internet users) primarily as a technology to access restricted and censored content [8]. However, VPN adoption and usage remains low (i.e., 18% of internet users) in Europe and North America regions where the main reasons for usage are to remotely connect to the network of one's school institution or employer and as a privacy-enhancing technology [8, 9]. According to a PEW research study [10],

1 e.g., https://mullvad.net/en/ and https://nordvpn.com/

only 13% of online adults in the United States are aware that issues that defeat the concept of online privacy can be minimized by use of a VPN, while 70% of users are not even sure what purpose a VPN serves.

Within the privacy research community, there is a lack of an empirical understanding of the external factors that motivate or hinder users from adopting VPNs primarily as PETs. Likewise, there is no clarity on people's personal considerations or perceptions that underlie this adoption decision. As a step towards addressing this, we conducted a survey targeting VPN users and abandoners to investigate these external factors and personal considerations that motivated or hindered their adoption and usage of VPNs as PETs. We find that while both practical and emotional considerations motivate the *adoption* of VPNs as PETs, only *emotional considerations* are a primary driver behind their sustained usage.

In the following sections, we discuss related work regarding the adoption and use of PETs, as well as important aspects of users' judgment and decision-making practices surrounding adoption. In Section 3, we discuss our survey methodology. Section 4 presents our results, and implications are discussed in Section 5. Section 6 covers our limitations and future work, followed by our conclusion.

2 Related Work

In this section we first cover related work on the adoption and acceptance of privacy-enhancing technologies. We then discuss VPNs as PETs, and usability as a factor in the adoption of PETs, notably VPNs. We then draw from the Technology Adoption Model (TAM) as a useful adoption model that encompasses usability but can also be used as a guideline to discuss other factors that may relate to VPN adoption. Finally, we look at decision-making psychology literature that highlights the existence of both *practical* and *emotional* decision processes. We subsequently use this distinction to formulate our guiding research questions.

2.1 Adoption and Acceptance of PETs

Previous studies on privacy-enhancing technology adoption found that PET adoption was impacted by factors such as usability and usefulness [11–13]. In the context of PETs, usefulness refers to the belief and extent to which people find PET tools effective at improving and safeguarding their online privacy. In interviews with Chief Information Security Officers in the medical field, Johnson and Willey noted that "physicians working at home could use a virtual private network (VPN) to gain access to hospital systems, but sometimes found it slow or cumbersome and chose to download the data to their remote laptops instead"[11]. Likewise, adoption could be thwarted by the lack of obvious tangible benefits. Within corporations, for example, there is often a positive business-related outcome and an economic justification for their investments in PETs before a positive decision to adopt PETs is taken [12]. Note that in contrast to these works, our current work focuses on VPN adoption by private individuals rather than corporations.

Similarly, Caulfield et al. [13] used privacy attributes i.e., context (the setting in which and the purpose for which a given technology is used), requirement (the level of privacy that the technology must provide for a user to be willing to use the technology), belief (a user's perception of the level of privacy provided by a given technology in a given context), and relative value of privacy (how much a user cares about privacy in this context and how willing they are to trade off privacy for other attributes) in an economic (rational) model to understand the adoption of PETs. Using this model, they found that increased media coverage of Apple against FBI [14] signaled to users that the iPhone was more privacy-enhancing than Android devices. Such a shift in user belief would increase the adoption of the iPhone as a privacy-enhancing technology. Our work goes beyond the economic model proposed by Caulfield et al. by also covering *emotional* reasons for the adoption and use of VPNs.

2.2 VPNs as PETs

Using VPNs serves as one of the means through which people can safeguard their privacy [15, 16]. However, people can mistakenly perceive VPNs to completely protect their online privacy [17]. VPNs do not fully guarantee user privacy based upon their own practices and those of the website(s) the user is accessing [6]. Specifically, VPNs afford users privacy and anonymity through the alteration and re-routing of the user's IP address through the VPN provider's servers and encryption of all the data packets sent out from a user's device to the server through a secure "tunnel" (i.e., a private network) established by the VPN client installed on the

device [18, 19]. Through this secure tunnel, the user's internet traffic is hidden from outside observers and prevents the websites being accessed from identifying the user by their actual IP address. However, websites can still track and identify a user through other means such as browser or device fingerprinting, logins and cookies [20].

2.3 Usability as a Factor in PET Adoption

With the rise of downloadable applications, software trials, and "freemium" pricing strategies, people are increasingly able to experience the usability of a technology before they commit to using it and/or spending any money on it [21]. Therefore, the usability of PETs is important, because people are more likely to adopt them when they are usable. For example, a PET like Tor[2], which guarantees user anonymity and protects against network surveillance and traffic analysis, is not commonly used due to lack of usability [22]. Likewise, although Pretty Good Privacy (PGP) is an effective means to provide communication security through encryption, most tools implementing PGP have been found to be unusable despite their attractive graphical user interfaces [23]. People have instead adopted those secure communication applications which offer end-end encryption and are usable (e.g., WhatsApp, Signal and Telegram) [24].

Extrapolating from these examples, one could argue that usability would be an important factor in the adoption and usage of VPNs. However, while most of the existing research focuses on technical capabilities of VPNs [25, 26], usability of VPNs has not been studied. In the current paper,we adopt the definition of PET usability suggested by Whitten and Tygar [23] to define "usability of VPNs" as the ability of users to reliably and successfully use VPNs whenever online, and are comfortable enough with the interface to continuing using them. We, therefore, explore factors such as a VPN's usability from an end-user perspective to learn of how they foster adoption and use [27, 28].

2.4 The Technology Adoption Model

The Technology Acceptance Model (TAM) was developed with the goal of understanding the process people go through as they accept software and information technologies [29]. According to TAM, actual system usage (i.e, *the user's behavioral response*) is determined by the user's behavioral intention (affective response) towards whether or not they will use the system. Behavioral intention, is in turn, influenced by the user's cognitive (practical) response (i.e., ability to assess or perceive the *usefulness* and *usability* of the system). External stimuli such as the *system's design features and capabilities* directly influence the user's cognitive response.

TAM has been applied to successfully predict the end-user acceptance of many technologies from various domains such as the e-commerce [30], telemedicine [31] and even employee adoption of information security [32]. In this paper, we use the TAM framework constructs (external stimuli, user motivation and actual system usage) to guide our understanding of the factors that motivate people to adopt and/or abandon using VPNs as PETs.

2.5 Judgment and Decision Making

Researchers have criticized TAM for not grounding the cognitive (practical) and affective (emotional) responses which underlie user motivation and attitude in psychological theories that describe people's decision processes [34]. TAM largely treats user motivation as a function of the perceived consequences of a user's target behavior for using the system, multiplied by the evaluation of those consequences [29]. This treatment is related to the "expected utility theory" in judgment and decision making, which suggests that people make decisions by assessing the severity and likelihood of possible outcomes and then maximizing the expected value of the outcome [35]. In conventional sense this means that when people evaluate risk cognitively (practical consideration), they make a decision to alleviate such risk based on the premise of the consequences that will result from the choice they select or the activity they engage in. In the field of privacy, this principle is encoded in the "privacy calculus", which argues that people trade off the privacy risks and potential benefits of engaging in a certain activity in a deliberate process [36]. For example, as a response to this cognitive evaluation, people could decide to use a VPN in order to protect their privacy by anonymously browsing the internet based on the severity of the consequences that accrue with visiting the sites or activities they conduct over the internet.

2 https://www.torproject.org/

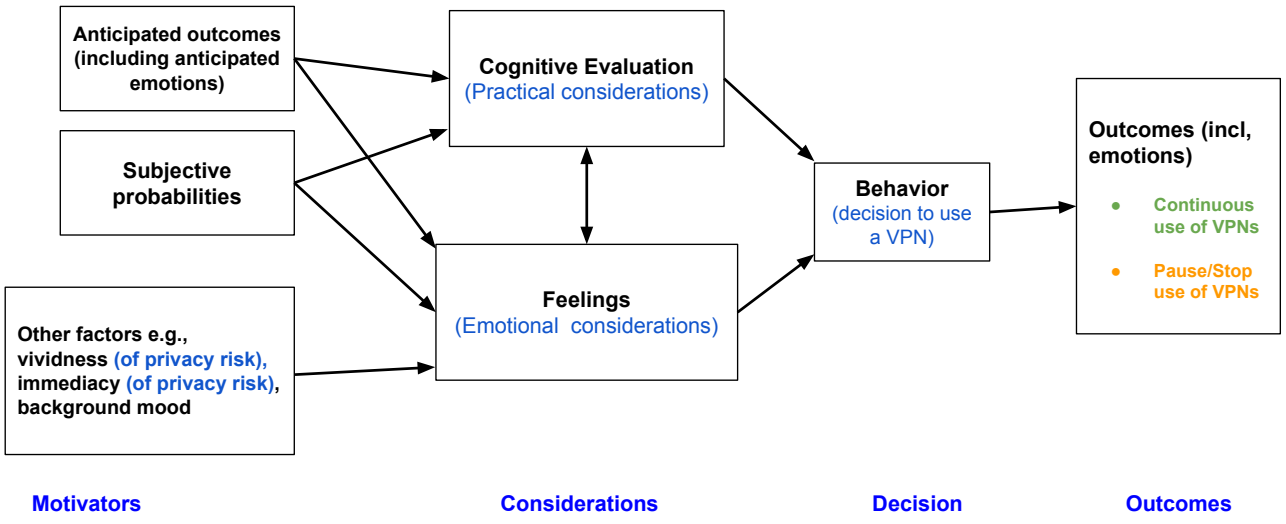

Fig. 1. The Risk-as-feelings perspective (adapted from [33]). The colored annotations represent our interpretation of the theory with regard to the decision to adopt VPNs as PETs.

A particular shortcoming of this treatment in TAM is that it ignores the separate roles that practical and emotional considerations play in the adoption and acceptance of technology [29, 34]. Even though research has shown that emotions (i.e., feelings that are usually associated by an individual with a particular act, such as joy, sadness, depression, anger, disgust, fear, like, dislike, or hate) are direct determinants of user behavior separate from practical considerations [37, 38], TAM assumes that in the decision making process, practical considerations such as perceived usefulness and ease of use of the technology are made first—emotions are only considered as a component of the expected consequences of the decision, rather than being separately experienced [33]).

In contrast, Loewenstein et al.'s [33] risk-as-feelings theory reveals that people's responses to risky situations (including decision-making) are different when the situation is cognitively evaluated (i.e., practically considered) compared to when they are based on the feelings associated with the situation, such as fear, worry, dread or anxiety (i.e., emotionally considered).

As illustrated in Figure 1, the risk-as-feelings perspective posits that people's emotional responses to the evaluation of risky situations *independently* inform decision making. While anticipated outcomes and their subjective probabilities may cause emotional responses (albeit to a much lesser extent for cognitive evaluation than emotional evaluation), these emotional responses can also result from the evaluation of factors that are not considered during cognitive evaluations, such as the vividness and immediacy of the risk. In part due to this difference in determinants, it is not uncommon for emotional responses to diverge from cognitive responses. When such divergence occurs, the emotional considerations often take the upper hand—they drive behavior and result in different outcomes.

Hence, in line with the risk-as-feelings theory [33], we make a distinction in the analysis of our study results between the emotional and cognitive evaluations of the external stimuli and internal motivations that influence people's decision to adopt and use VPNs as PETs (we use the shorthand terms "emotional considerations" and "practical considerations", respectively, see (Fig.1)). Our intent in doing this is to investigate whether there is indeed a difference in the adoption and usage of VPNs as PETs when these stimuli and motivational factors are emotionally or cognitively evaluated. If so, this would confirm the risk-as-feelings assertion that when present, people's emotional considerations exert a separate, stronger, and more robust influence on their behavior than their practical considerations.

To apply this theory and offer a better understanding on how people adopt and use VPNs as a privacy-enhancing technology, we define emotional and practical considerations as follows:

– **Emotional considerations:** The judgment and decision to use a VPN for privacy protection purposes primarily based on emotions, such as the *fear* of ISPs' uncontrolled access to and misuse of personal information, *anger* with surveillance by the government, or *dislike* of websites' large-scale tracking of web browsing activities.

– **Practical considerations:** The judgment and decision to use a VPN for privacy protection purposes based on an objective to accomplish a practical task or need, such as obtaining secure and/or anonymous access to entertainment content, websites, social networks, remote files/machines, or the Tor browser.

In summary, we pose the three following research questions:

RQ1: What factors motivate users to adopt VPNs as a privacy-enhancing technology?

RQ2:What barriers do they encounter in adopting VPNs as a privacy-enhancing technology ?

RQ3: What are the differences in the adoption and usage of VPNs as a privacy-enhancing technology between users who mainly have practical considerations versus those who mainly have emotional considerations?

3 Methodology

The goal of this study is to explore how people adopt and use VPNs specifically for privacy protection purposes. We conducted a survey composed of closed-ended, multiple-choice, 5-point Likert scale, and open-ended questions. To ensure that we asked the right questions and improve the validity of the survey data collected, we pre-tested all our survey questions through interviews with five VPN users and subjected it to an expert review by three human computer interaction experts. We elaborate on our survey design in Section 3.1.

Due to the low prevalence of VPN use in society [8–10], the resulting survey (which is fully listed in Appendix A) was targeted to people with a high likelihood of at least knowing about VPN. In particular, we distributed the survey to Reddit users (Redditors) of several VPN sub-communities and to Computer Science students at Clemson University via email listservs. We elaborate on our recruitment procedures in Section 3.2. The survey was completed by 90 participants, whose responses were coded and qualitatively analyzed (see Section 3.3). This study was approved by the Clemson University Institutional Review Board (IRB).

3.1 Survey Design

The main objective of our survey was to gain a deeper understanding of the external stimuli and internal motivations that propel people to learn about, adopt, and use VPNs (as standalone applications) for privacy protection purposes. Specifically, we queried respondents' awareness of VPNs, their current use of VPNs (i.e., never used, currently using, stopped/paused use), their duration of use (i.e., since when and until when, if applicable), their initial beliefs and values regarding VPNs including their motivations to start using VPNs (if applicable), the number of VPN applications they explored for use, the overall cost of their VPN use, the perceived pros and cons of VPN use, and their general sentiments about VPNs.

To quantify their perceptions regarding VPNs, we also asked respondents to state their agreement on a 5-point Likert scale (1 = Strongly disagree, 5 = Strongly agree) regarding a number of statements/items (see Appendix A). These survey items were adopted from Colnago et al.'s [39] survey and are related to the three constructs detailed below. We provide the Cronbach's alpha for each of the constructs to demonstrate their reliability [40]. Acceptable values of Cronbach's alpha range from 0.70 (acceptable) to 0.95 (excellent) [40].

– **Affordance of a VPN to protect user privacy** (5 items, alpha: 0.7):
  – Using VPNs helps me protect my privacy online.
  – It is worthwhile to put in the effort to start using a VPN.
  – It is important to learn about the benefits of using a VPN.
  – It is important to learn about the drawbacks of using a VPN.
  – I suggest that people should use a VPN at any neccessary cost to protect their privacy online.
– **Difficulty of selection and installation of a VPN application** (4 items, alpha: 0.79):
  – I had a hard time deciding on the best VPN application to use.
  – Installing a VPN was difficult.
  – Installing a VPN was easy.
  – Installing a VPN was a lengthy process.
– **Ease of use of a VPN application** (3 items, alpha: 0.8):
  – I had a hard time understanding how to use VPNs.
  – I think that VPNs are easy to use.
  – I think that VPNs are difficult to use.

Additionally, we asked respondents' different demographic questions including their gender, age, nationality and current country of residence. To account for

cultural variations in privacy attitudes and behaviors [8, 41, 42], we also asked how long each respondent had lived in the country of current residence and whether their current country of residence was different from their nationality.

3.1.1 Survey Development and Refinement

We pre-tested the initial set of survey questions with five participants who reported that they were VPN users [43]. The purpose of the pre-test was to assess the clarity, appropriateness and necessity of each of the questions to ensure that the collected data would allow us to answer our research questions [44].

During the 30 minute think-aloud walk-through of the survey, the interviewer read each question aloud and asked pre-test participants to respond verbally to each question. Beyond that, participants were asked whether the question was easy for them to comprehend, whether they felt comfortable responding to the question, and how valuable they found the question to be. In response, some participants also volunteered other questions and answer choices that we could consider adding to the survey.

Overall, the pre-test interviews provided insights into how respondents would interpret and respond to the survey questions. Moreover, the pre-test also helped us identify the different categories of VPN users that we were likely to encounter in our sample. Notably, we learned that despite knowing about VPNs, all five participants did not constantly use them—at least not for privacy purposes. Based on this finding, we explored the literature around stages of technology acceptance (see Section 2.4). This adoption literature (cf. [29]), in concert with the VPN user types that we identified and hypothesized based on our insights from the pre-test interviews, led us to come up with the following four categories of adoption and usage of VPNs as PETs:

- **Unaware** (Non-Adopters): Respondents who do not know about VPNs.
- **Never used for privacy** (Abstainers): Respondents who know about VPNs but either have never used them at all or currently use / have used them for purposes other than protecting their privacy (e.g. remotely accessing a work or school network).
- **Currently use for privacy** (Adopters): Respondents who know about VPNs and are currently using them primarily to protect their online privacy.
- **Paused/Stopped use for privacy** (Abandoners): Respondents who know about VPNs, have used them primarily as privacy-enhancing technologies for some period of time in the past, but have currently momentarily or completely stopped using them.

These categories helped us better structure the survey, as it allowed us to ask specific questions for each of the user categories (groups) to better contextualize their adoption and usage experiences. For example, abstainers would be asked about their perceptions of VPN, while adopters and abandoners would be asked about their perceptions as well as their actual experiences using VPN (Appendix A indicates which questions were shown to which user group(s)).

Moreover, the pre-test demonstrated that some of our initial questions were too long. Subsequently, we rewrote those questions to make them more brief and understandable. We also added five questions that specifically sought respondents' perceptions regarding the privacy protection affordances of VPNs, as well as additional demographic items such as nationality.

3.1.2 Expert Review

After the pre-test, three human computing expert reviewers with domain knowledge on survey methodology and usable privacy reviewed our updated survey questions to ensure that they were correctly worded and adequate enough to uncover valuable insights from respondents. They helped us remove technical words that our respondents would not easily comprehend thereby making it possible to have the respondents self-report as accurately as possible [45].

3.1.3 Pilot Test

Subsequently, we pilot-tested the survey with seven participants to understand how long it would take to complete the survey, to ensure correct branching for each of the identified adoption categories, and to ensure that collected data was correct and in the expected format. Based on time it took for the participants to complete the survey (at most 15 minutes), and comprehension of the questions, we updated a number of our questions, the design aesthetics, and the branching logic of the survey, until no additional questionnaire problems remained.

3.1.4 Final Survey and Administration

The final survey instrument was administered via the Qualtrics web-based survey tool [46], which allows for a branching survey. For example, the first question asked whether respondents knew what a VPN is, and the response to this question determined the next set of questions. This ensured that respondents only saw and responded to questions relevant to their situation. As our study was targeted to individuals who are likely to use VPN (students, users on VPN forums), the most detailed questions were administered only to participants who indeed (previously or currently) used VPNs for privacy protection purposes.

3.2 Recruitment and Respondents

We conducted our survey between September and November of 2018. Our recruitment goal was to find respondents who primarily use VPNs as a privacy-enhancing technology (PET). While the use of VPN to remotely accessing a work or school network is fairly common [47], its use for privacy protection purposes remains low [8, 9]. Considering that participants who do not know what VPNs are would not provide many relevant insights for our study, we decided to forego random sampling from the population at large as a recruitment strategy. Instead, we specifically targeted people who were at least aware of what VPNs are, using two recruitment methods. First, we posted recruitment posts on a number of Reddit sub-communities about VPN: r/VPN[3], r/VPNTorrents[4] and r/Privacy[5]. Second, we sent recruitment emails via email listservs of Computer Science students at Clemson University. Our survey instrument captured where the responses came from based on the two distribution avenues (i.e., posts on Reddit and email listservs). This recruitment method resulted in a sample size of 90 respondents: 39 Redditors and 51 students (Fig. 2). Respondents were entered into a raffle to win a $50 Amazon e-gift as incentive to complete the survey.

3.3 Coding and Analysis

At the end of the study period (November 2018), the survey responses were downloaded from Qualtrics for coding and analysis. After removing incomplete responses, the responses of the remaining 90 participants were organized based on the VPN use and adoption category they belonged to (see Section 3.1.1).

Two researchers qualitatively analyzed [48] the responses to all the open-ended questions in the survey to learn of the respondents' attitudes regarding VPNs and their experience using VPNs. Thereafter, the researchers did a content analysis [49] to code the responses of the adopters and abandoners to the two questions that were specifically focused on the factors that motivated them to use a VPN as a PET: "How did you finally end up using a VPN for personal privacy protection purposes?" and "Upon learning about VPNs, what sparked your desire to actually use them for personal privacy protection?" Specifically, based on Loewenstein et al.'s [33] risk-as-feelings theory, the answers to these questions were coded as either emotional and practical considerations. The code was assigned based on whether the answer demonstrated an emotional need (e.g., "I really dislike the idea of being followed about online. [...] To me, that's not okay.") or a practical need (e.g., "I was on a network that restricted access to websites I needed access to.") The inter-rater reliability (Cohen's Kappa) of the raw agreement between the two independent coders [50] was 0.65. A kappa above 0.6 is usually considered satisfactory [51].

We did not find any qualitative response differences between Redditors and students. We therefore merged these samples in our further analysis and in the discussion below. For clarity purposes, however, we will use **R** and **S** to distinguish the quotes from these different samples.

4 Results

4.1 Quantitative Survey Results

Among the 90 respondents (39 Redditors and 51 students) who took the survey, the vast majority (88) reported knowing what a VPN is (Fig. 2). Among those, 49 used it primarily to serve other needs that did not include protecting their privacy online and 2 had not used it despite knowing about it. The remaining 37

3 https://www.reddit.com/r/VPN/
4 https://www.reddit.com/r/VPNTorrents/
5 https://www.reddit.com/r/Privacy/

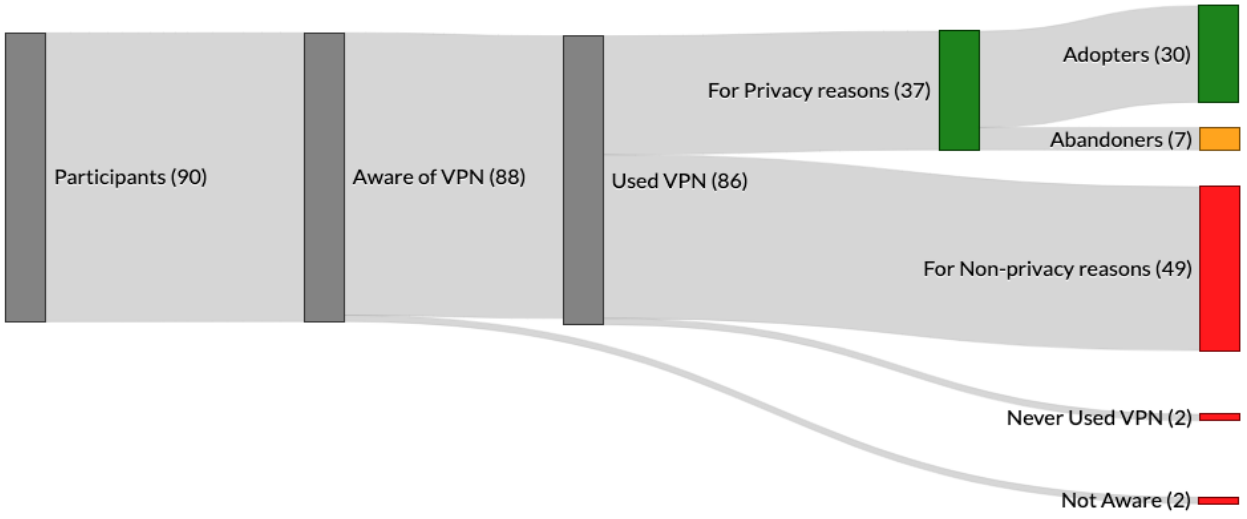

Fig. 2. A breakdown of the respondents in our sample by VPN use and adoption category (see Section 3.1.1).

		VPN User Groups	
	Total	**Abandoners**	**Adopters**
	N=(37)	**N =(7)**	**N =(30)**
Gender			
Male	25	6	19
Female	6	1	5
Unknown	6	0	6
Age			
18-24	21	6	15
25-34	4	1	3
35-44	3	-	3
45-54	2	-	2
55-64	2	-	2
65-74	1	-	1
Unknown	4	-	4
Nationality			
USA	28	7	21
Azerbaijan	1	-	1
Canada	1	-	1
Cyprus	1	-	1
Gabon	1	-	1
Germany	1	-	1
Great Britain	1	-	1
Portugal	1	-	1
Russia	1	-	1
Slovakia	1	-	1

Table 1. Demographic data : Gender, Age and Nationality of the main respondents in the study categorized by the VPN user groups (Abandoners and Adopters.)

reported using VPNs to specifically protect their privacy online; 30 of them reported currently using VPNs as PETs (*adopters*; shown in green in Fig. 2) while 7 of them reported having temporarily or permanently stopped using VPNs as PETs (*abandoners*; shown in orange in Fig. 2). These 37 respondents are the main basis of our results and findings, since they allow us to learn how people come to adopt and use VPNs as a privacy-enhancing technology. Their demographics are shown in Table 1.

For these 37 participants, we examined the quantitative data (perception scales) and qualitative data (open-ended questions) from the survey to examine the motivations and external stimuli that influence people's adoption and use of VPNs as PETs. We report the results of this analysis using the TAM framework constructs as a guiding framework, using external stimuli, user motivation, actual system usage, and hindrances as the main structure of our result section. Note that "hindrances" constitute the performance impacts concept that was originally conceived as part of TAM but was later removed [29].

For each of these aspects, we show the similarities and differences between adopters and abandoners. We provide quotes (labeled with S for students and R for Redditors) to support our observations. Under the user motivation section (Section 4.2), quotes are also labelled as either *Emotional Reasoning* or *Practical Reasoning*, based on how they were coded.

4.2 People's Motivation to Adopt VPNs

Considering the quantiative results of the measured perception scales, both adopters and abandoners report finding it easy to select and install ($M_{abandoners} = 2.60$, $SD_{abandoners} = 0.33$, $M_{adopters} = 2.38$, $SD_{adopters} = 0.09$), and use ($M_{abandoners} = 1.90$, $SD_{abandoners} = 0.33$, $M_{adopters} = 1.82$, $SD_{adopters} = 0.09$) VPNs. They also expect and perceive VPNs to protect their privacy by default ($M_{abandoners} = 3.66$, $SD_{abandoners} = 0.33$, $M_{adopters} = 4.17$, $SD_{adopters} = 0.09$). While our sample of especially abandoners is not sufficiently large to make statistical comparisons, at the surface level, these results seem to suggest that adopters and abandoners are initially about equally motivated to adopt and use VPNs.

However, considering our qualitative analysis, we find that the *considerations* underlying users' motivations to use VPNs as PETs are rather different between adopters and abandoners. Below, we elaborate on these qualitative findings and demonstrate how adopters decide to use VPNs as PETs primarily based upon an *emotional* consideration to protect their privacy, whereas abandoners initially decide to use VPNs as PETs based upon a *practical* consideration to protect their privacy (i.e., to support an online activity that fulfills a specific need).

4.2.1 Adopters' Motivation

Among the adopters, we found that their motivation to adopt VPNs as PETs was primarily based on emotional considerations, such as the fear induced by past breaches of their private information, or their dislike of perceived violations of their privacy. In our thematic analysis we categorized these emotional considerations along the following lines:

- **Heightened privacy concerns**: Ten respondents reported having little control over how their personal information is collected, accessed, and used by various online entities. In particular, they were concerned about third parties tracking and accessing their data without their explicit consent or even their awareness. As a result, they were motivated to use VPNs as an online tool to help safeguard and address these privacy concerns ("[I want to use a VPN] just for privacy concerns" R, *Emotional Reasoning*; "Constant breeches of personal consumer information like credit card numbers and addresses at major firms like Target and Sony." S, *Emotional Reasoning*; "For the most part, I just hold my privacy in a higher regard than many other people these days. I know just how much data can be collected about you and how easy it is to use 'anonymous' data to identify specific people." S, *Emotional Reasoning*). Additionally, some respondents reported actually being hacked in the past, so they used VPNs as PETs to better safeguard their online privacy ("I have been hacked a couple times and it piqued my interest in cyber security. VPNs are one of the things I found online that I could implement easily." S, *Emotional Reasoning*).
- **Fear of Internet surveillance**: Thirteen respondents are wary of their ISP or their government covertly monitoring their online activities. As such, they reported being compelled to use VPNs to safeguard their privacy and also to quell their fears of online surveillance ("I wanted to be safer from government and ISPs level logging and profiling, and disliked the impingement on my privacy and freedoms. Snowden and the UK 'Snooper's Charter' firmed this resolve." R, *Emotional Reasoning*; "I do not like when my data is tracked." R, *Emotional Reasoning*, "[I used a VPN for] Privacy from ISP and forums." R, *Emotional Reasoning*)
- **Dislike of the lack of or unfavorable change of privacy legislature**: Five respondents reported being upset with constant changes in legislature that lead to less privacy protections, or the lack of legislature that protects people's online privacy. This compelled them to start using VPNs to take matters into their own hands to protect their online privacy ("Introduction of SOPA-type bills in congress" S, *Emotional Reasoning*); "Snowden / Assange [revelations of US government spying programs]." R, *Emotional Reasoning*). A prominent example that was often mentioned was the Congressional Review Act, which repealed privacy rules developed by the Federal Communications Commission in March 2017.
- **Media Attention**: Two respondents reported that their privacy concerns are fueled and amplified, in part, by concentrated media attention on privacy breach incidents such as the Target and Sony company hacks ("The media reported on data breaches and misuse of personal data, prompting me to take action to prevent this from affecting me. One of the actions I took was to use a VPN. Protecting my personal information." S, *Emotional Reasoning*).

4.2.2 Abandoners' Motivation

Among the abandoners, we found that their motivation to adopt and use VPNs as PETs was mostly based on practical considerations. Such practical considerations usually involved a practical need to overcome a specific barrier or to attain a specific goal. Like emotional considerations, these practical considerations manifested themselves as privacy concerns. But whereas emotional considerations were driven by a subjective fear of negative outcomes that might result from a loss of privacy, these practical considerations were driven by a desire to fulfill a practical goal while objectively avoiding the negative privacy outcomes of pursuing that goal (e.g., the desire to anonymously download content from the internet whilst safeguarding their identity). In our thematic analysis we categorized these practical considerations along the following lines:

- **Task requirement**: Three respondents mentioned that to access and conduct particular institutional objectives such as the submission of documents that contain highly sensitive private personal information, they were required to use VPNs to securely access the institution's network and accomplish the task. ("For school it is necessary to be on a university VPN to access some university features." S, *Practical Reasoning*).
- **Need for anonymity**: Based on their online browsing habits, two respondents reported the need to obscure their identity online as a reason for the adoption and use of a VPN ("I used to pirate movies and TV shows a lot, so I was pretty much just looking to cover my own ass." S, *Practical Reasoning*; "I was browsing the internet for certain content that is possibly a gray area in terms of legality such as streaming movies from "illegal" websites and so I wanted to find a way to create some type of anonymity or at least mask my identity." S, *Practical Reasoning*).
- **Privacy concerns regarding specific actions**: Two respondents mentioned that they sought out VPN as a PET to obscure their traffic, personal information such as web browsing history from ISPs especially when they needed to accesses certain sites ("When accessing some sites I felt more comfortable security wise accessing them through a VPN to protect my privacy." S, *Practical Reasoning*; "I wanted to be able to pirate software without receiving copyright infringement notices from my isp." R, *Practical Reasoning*),

4.3 External Stimuli: How People Learn About VPN

Both adopters and abandoners reported using Google searches, expert blogs and VPN application websites to learn about and determine which VPN applications to use. Most users selected a VPN based upon its user reviews, expert or friend recommendation, capabilities and features such as server vantage points, privacy logging policies, and/or the jurisdiction in which it was located. As discussed below, the external stimuli were mostly similar for both adopters and abandoners, with only a few interesting differences.

4.3.1 External Stimuli of Adopters

Just over half of the adopters (18/30) learned about VPN's features and capabilities through information they found online, such as reviews. They accessed these reviews by conducting simple Google searches ("A quick Google search for 'Best VPN 2018'." S), or through official VPN application websites and VPN expert blogs. These websites provide reviews and recommendations on the "best" VPN applications to use. Based on such recommendations, adopters formed an opinion and subsequent decision regarding which VPN to use ("I watched a ton of reviews and decided on the most trusted/used." R), "I found the cheapest provider that had good reviews and a good reputation. I ended up buying a one-year subscription for private internet access." S).

In contrast, eight adopters learned about VPN through recommendations from online social networks ("Privacy advocates on Twitter recommended one." R), whereas one started to use a VPN application that was recommended by their school ("Clemson University provided it. I will likely ask friends in the future when I lose access." S). Other adopters selected a VPN application to use based on their own personal accrued knowledge on VPNs ("I worked in computer information systems for the Marine Corps before coming to school at Clemson University so I had some background knowledge that suggested always using a VPN - especially when connecting to sites like financial institutions [...] I would rather sit behind a VPN, even when connected over ethernet at home." S; "[It was through] luck and gambling. Still better than no VPN." S).

Finally, two adopters reported building their own VPN applications due to a lack of trust in the existing VPN choices ("I looked a bit at public VPN providers,

but a lot of them seemed sketchy or had questionable business models (i.e., they seemed like they would sell my data to advertisers). As such, I decided to set up my own VPN server on amazon web services." R). However, they reported this being an extremely long process with lots of trial and error.

4.3.2 External Stimuli of Abandoners

Roughly similar to adopters, just under half of the abandoners (3/7) learned VPN's features and capabilities through information they found online, e.g. via Google, expert blogs, and various VPN forums. But whereas adopters' search focused on finding the highest quality VPN, abandoners focused on price ("I just googled the best and cheapest options." S; "Whatever was free and had good reviews was enough for me." S).

Four other abandoners reported relying on friends ("I think the one recommended by a friend" S) and social media for recommendations ("I did research online and got a lot of recommendations from people on various forums" S) on which VPN application to use.

4.4 Actual VPN Usage

Both adopters and abandoners on average tried out more than two VPN applications before ultimately selecting one which they were comfortable using. Adopters, driven by an emotional need to protect their privacy, had used their current VPN for a period of time that ranged from several months to several years by the time of the study. Most abandoners, on the other hand, had used their selected VPN for a much shorter period of time—ranging from as little as a week to about a year at most—before completely abandoning the application. In our qualitative analysis we observed that their abandonment was usually caused by the fact that the practical need that had lead them to initially adopt VPN no longer existed. In other words, their practical considerations turned VPN usage into a temporally limited endeavor.

4.4.1 Adopters' VPN Usage

A majority of adopters (20) reported that they felt safer online when using a VPN ("Having some information taken from me, which I assume was based on my IP, made me feel insecure without a VPN when doing anything important." S; "I heard about it [VPN] and started to take my privacy seriously." R; "[I] read the privacytools.io [6] and got serious concerns of my privacy, [besides I] travel a lot and using VPN, it makes me feel safe and good" R).

Additionally, four respondents reported they felt protected against internet surveillance when using a VPN. This quelled their fears about their online activities being monitored by ISPs ("I didn't want my history to be seen by my ISP/controller, and I wanted to access sites that demand privacy to be upheld." S), government agencies ("[Awareness of the] Dragnet surveillance by the United States government."R), and corporate organizations ("The repeal of net neutrality had me bugging hard, and I needed to keep the government out of my dark webzz bizness" R; "I didn't want the government to possibly look at my [web] history. I wasn't [going to] give that data to them willingly (like using a normal browser [without a VPN])." S).

Furthermore, four respondents reported they felt more comfort in the anonymity provided by their VPN. This comfort allowed them to express their ideas and opinions without fear, thus avoiding self-censorship ("Mostly just wanted to be on a secured connection while browsing. I play games online and sometimes people will pull your IP then boot you offline and a VPN prevents that" S; "You need [VPN] to be connected to the TOR network to access TOR sites, it is free, it is completely private, I trust the tech because it was originally a DARPA project, and my continued use further anonymizes other users." S).

Many adopters put a great amount of trust in their selected VPN application—14 of them reported not reading their VPN's privacy policy and terms of service before installation. The other 16 of them did read the privacy policy, though, and some even reported changing their mind about installing and using the VPN application when they found that this privacy policy did not align with their privacy preferences on issues such as logging practices and server locations. Moreover, 8 respondents reported making changes to the default configuration of their VPN application to align its settings to their preferences ("Adjusting some settings to match my use. For example, I changed the default location [where] to connect to." S). This was usually done with the purpose of making their VPN connection more private ("[The] kill switch lets me stop all connections even when the VPN stops working, so I turned that on." S),

6 https://www.privacytools.io/

increasing obfuscation ("[adjust the VPN to my] personal preference and increase obfuscation" R), and/or getting faster connection speeds ("I needed to tinker with it to get better speeds." S).

4.4.2 Abandoners' VPN Usage

Whereas adopters used VPNs to generally feel more private, abandoners reported using VPNs to engage in specific behaviors that required them to be private. For example, they reported using VPNs to access online content without negative legal repercussions ("I wanted to be able to pirate software without receiving copyright infringement notices from my ISP." R; "I was browsing the internet for certain content that is possibly a gray area in terms of legality such as streaming movies from illegal websites and so I wanted to find a way to create some type of anonymity or at least mask my identity." S). The use of a VPN as a PET was conditional upon the practical activity they were engaging in, and the usage would continue for as long as they were engaging in the activity.

4.5 Hindrances to Using VPNs

Both adopters and abandoners reported on factors that hindered their use of VPNs as PETs. But whereas for abandoners these hindrances caused them to eventually pause or stop using the VPN application, adopters generally overcame, avoided, or simply discounted these hindrances in an effort to continue using VPNs. Below, we elaborate on these factors which led to distinct usage patterns between adopters and abandoners.

4.5.1 Hindrances for Abandoners

Abandoners, and especially those who no longer had the need to use VPNs due to a change in their goals and social context ("I graduated" S; "I stopped pirating things, so I no longer needed it." S), reported the following hindrances that led them to pause or quit the use of VPNs once their practical needs no longer existed:

- **Effort to use/renew**: Three abandoners found it cognitively burdensome to always engage a VPN in order to use it ("[I] didn't always need it." S; "[It] seemed like a pain for no good reason" S). Likewise, some would forego the burden of paying for their VPN applications ("Laziness stopped me from renewing." R).
- **Usability**: Three Abandoners were turned off by the usability issues of the VPN application, such as pop ups ("I think I didn't see the point of it, or maybe it had pop-ups." S), convoluted documentation ("The documentation was unclear" S), slowness and lagging of the connection ("Slowness and lag" S) and unnecessary requests for personal information such as credit card information.
- **Cost**: Five abandoners reported using free VPNs and were not willing to subscribe for a paid VPN service due to the lack of immediate and apparent benefits of using a paid VPN ("I was not willing to pay, but wanted some [anonymity] effects" S; "I wasn't ready to pay" S; "I'm cheap" S; "Money." S). Whereas students' and Redditors' responses were otherwise similar, this hindrance was more common among students than among Redditors. These abandoners were also more apprehensive about divulging their credit card information as part of the subscription process, in part due to their lack of trust in the VPN providers themselves ("I do not want to spend money or give my credit card information to a company I'm not sure about." S). This is despite the fact, that some perceive free VPN applications to be risky to use ("Lots of options, difficult to find which ones are credible and which are not, especially when free" S; "Some ended up being obvious scams with massive amounts of ads and malware." S). In parallel, one respondent reported having paid for the VPN after the trial period, as they still needed access to certain sites ("I needed to keep using [it], because, at the time, I was still downloading movies and TV shows left and right." S).

4.5.2 (Lack of) Hindrances for Adopters

Whereas the cost of a VPN service was found to be a hindrance to abandoners, it compelled adopters to sustain their usage of VPNs as PETs. Particularly, we observed that sixteen respondents either out-rightly paid for a VPN service or paid for it after the trial period. This was mainly due to:

- **Affordability**: Adopters found the actual subscription value affordable and thus chose to pay for the VPN application ("Good price, right timing[...]" R; "The pricing seemed reasonable and the performance was adequate." R).

- **Capability and usability**: The VPN's speed and capabilities (e.g., multiple vantage points or server locations, clear and transparent terms and services such as the "no-logs" policy, and security features such as a "kill-switch" that would prevent traffic leakage in case of tunnel failure) compelled adopters to pay for a VPN subscription rather than using a free one ("[VPN Name] provides an excellent service. It has fast speeds and plentiful geo-regional servers." R; "Some cool features. Namely, you can specify which type you want and get double encryption and pick from a list of servers. You can find a table online that ranks the servers in real time." R).
- **Personal beliefs and a lack of alternatives**: Most adopters failed to find reliable free VPNs that would offer features similar to those in paid VPNs ("No reliable free services were available." R). Moreover, most of them believed that free VPNs were not safe and thus decided to pay for a VPN service instead. This would guarantee their privacy, since the VPN would not have to use their data to earn income ("If you aren't paying for the service, you are the product" R).

5 Discussion

To our best knowledge, our study is the first to explore from an end-user perspective the adoption and usage of VPNs as PETs. Our findings showcase the distinct roles that privacy risk-related emotional (affective) and practical (cognitive) considerations play in the judgment and decision making process towards the adoption of VPNs.

We did not find a pattern of over or underestimation about the overall workings and benefits of VPN usage as both adopters and abandoners appeared to have a good understanding (i.e., mental model) of how VPNs work. However, one abandoner had a faulty mental model as indicated by the false interchangeability of VPNs for other privacy protection tools ("I don't need a VPN anymore because now I use browser extensions like Ghostery and AdBlockPlus." R) — these two mechanisms are not interchange-able as they protect different issues. This highlights the importance for researchers and practitioners to always consider the fact that people might at times have faulty mental models of VPNs (see Section 2.2).

Specifically, we find that adopters largely embarked upon the usage of VPNs as PETs primarily based on their emotional consideration of the risk to their online privacy. As a result, their adoption is more resilient compared to abandoners, who largely used VPNs to serve a particular practical purpose. Interestingly, such emotional considerations are not a major construct in TAM [29], which arguably makes this model insufficient for the study of PET adoption. Complementing TAM with the risk-as-feelings theory gave us a better framework to understand the differences between adopters and abandoners. We suggest that researchers interested in the adoption of PETs consider using this framework in their studies.

What causes adopters to be emotionally invested in VPNs? Their emotions, such as fear and worry about online privacy, were usually induced by high-profile privacy violations, such as the discovery of surveillance programs (e.g. Dragnet and other surveillance program of the United States governement, uncovered by Edward Snowden, that provided concrete evidence that governments spy on the communications of their citizens [52]), and privacy-eroding legislative efforts (e.g. the Investigatory Powers Act 2016 [53] which comprehensively set out to expand the electronic surveillance powers of the United Kingdom government, and the recent repeal of US rules that would have required ISPs to seek permission from people to collect and share sensitive personal information such as their internet browsing history [2]).

On the other hand, abandoners do not have the same profound emotions to sustain a continous use of VPNs as PETs. Instead, their adoption and usage of a VPN is largely driven by the need to accomplish a practical online activity (e.g. by-passing geofilters, or downloading movies and music (this could be either "legal" or "illegal" [54]), accessing web content, sites and services) while avoiding consequences (e.g. receiving a copyright infringement notice from ISPs or being hacked). Once these practical needs no longer exist or alternatives are found (e.g. use of legal streaming services like Netflix to watch movies or Spotify to listen to music), they tend to abandon the use of VPNs.

In the section below, we reiterate the main takeaways of our study and derive design recommendations that can bolster the adoption and use of VPNs as PETs.

5.1 Duration of VPN Use

Our findings reveal that abandoners use VPNs for a relatively short amount of time because once they achieve their practical goal, they no longer have a strong intrinsic motivation for the continued use of VPNs. As

a result, they end up using VPNs for a relatively short amount of time (at most a year) before completely abandoning them.

On the other hand, adopters' considerations in deciding to adopt and use VPNs are emotional, such as their fear of privacy breaches, annoyance with internet surveillance, perceived loss of control, and general dislike of unwanted access to personal information. Consequently, adopters use VPNs for longer periods of time (usually spanning over several years) because privacy breaches and actual loss of control are intangible and unobservable: it is not known when they will occur and what their consequences could be.

5.2 Media Sensationalism

Our findings also suggest that when highly publicized news cases such as the Target data breach [55] and Sony hacks [56] are sensationalized by the media, emotions that were once mild or non-existent rapidly build up for some people due to the vividness of the described risk. They can also trigger past experiences for people who have been involved in such attacks before. This motivates adopters to embark upon and sustain the usage of VPNs, whereas abandoners seem not to be affected by the sensationalism of privacy data breaches.

VPN service providers can send out messages to their users that provide assurances of privacy protection during these periods of concentrated media attention on privacy breaches and misues of personal data. This could then help users establish new emotional considerations regarding VPN use. For example, one adopter mentioned initially using a VPN to serve a practical need, but later transitioning to its use as a PET based on media reports on breaches of privacy and misuse of personal data on social media ("I originally started using a VPN for torrenting, but as the media began reporting more and more on breaches of privacy and misuse of personal data on social media sites and the like, I began using my VPN for regular web browsing." S). Moreover, VPN service providers should tie in with emotional considerations during the marketing of their VPN applications [57], especially at times when people start to look for technologies that can better protect their privacy.

5.3 Cost

Our findings reveal that adopters mostly pay for the VPN service or set up their own (even though they find this tedious and time consuming given the trial and error involved). This enables them to trust their VPN service, as they are certain of how the VPN provider obtains the funds to meet the costs of deployment and running of the VPN service. On the other hand, abandoners are easily dettered by the monetary cost of the VPN service. As a result, they are likely to use it for a shorter period of time, and they also tend to not pay for their VPN service. The latter is of course also a function of their income.

The cost of using a VPN also includes the time taken to figure out and choose which kind of VPN to use. This cost does not seem to be a problem as more than half (16/30) of the adopters took the time to read their VPN's privacy policy. This number of people is high if compared to other online services (i.e., could be an overestimate due to self-reporting) where users often skip reading the privacy policies given the time investment involved [58]. It demonstrates that VPN privacy policies are important to adopters in making the choice on a VPN to trust and use. While adopters might not necessarily read the policy in its entirety, they review it to determine the level of privacy protection offered by the VPN through its stated policies and practices on logging, server locations, pricing, and IP leak protection, among other features.

VPN service providers can also use these findings to market their applications. As most abandoners seem to use VPN only to serve their practical needs without paying for the service, VPN service providers need to find a way to convince them to transition into longer-term users by offering a trustworthy free application and/or by periodically reminding them of potential emotional considerations through notifications which show how the application protects their privacy. One example could be a notification with a message describing some protection statistics (i.e., "[VPN application] detected and blocked 2 potential trackers that were trying to accesses your email address as you logged into your email"), which would help potential abandoners to better understand and appreciate the value of VPNs as PETs.VPN providers could also ensure that their privacy policies are up-to-date, clear, accurate and easy to read given that adopters take the time to actually read them when choosing a VPN.

6 Limitations and Future Work

As with any survey, our results are limited by the fact that answers were self-reported, which may result in biases such as the social desirability bias (respondents might have mis-reported their answers to make themselves look better) and memory bias (respondents may have forgotten some information and thereby not have responded to some of the survey questions) [44, 59]. In addition, since we conducted a survey rather than an interview, we lacked the opportunity to follow up with respondents regarding answers we found interesting. That said, our survey provides a low barrier of entry, especially compared to an experiment (which would introduce a potentially intrusive manipulation) and an interview (which requires face-to-face communication). Doing otherwise would have negatively affected our recruitment—for example, we gave people the opportunity to give us their email address in case we had follow-up questions, but most respondents declined to participate in this. A possible improvement for future work would be to conduct a longitudinal diary study of VPN users induced by emotion.

We sampled from people who were more likely to be more tech savvy. This could have overestimated the amount of engagement and reflection typical users have in regard to the adoption and use of VPNs. Moreover, our sample size was small and highly skewed towards men. This could have led us to overstate some perspectives particularly held by men, or to ignore relevant experiences and opinions from female VPN users. Future work could use a more representative sample (larger and gender-balanced) to confirm or enhance our findings. It could also study the effect of gender and age in the adoption and use of VPN as a privacy-enhancing technology. The PEW research center [10], recently did a survey measuring user-awareness of PETs including VPNs. This sample could be utilized to get a more accurate stratified sample of VPN users.

7 Conclusion

In this paper we presented the results of a study with 90 respondents who took our survey to explore the motivations and perceptions that guide the adoption and use of virtual private networks (VPNs) for privacy protection purposes. We find that people who are emotionally invested in protecting their privacy are likely to be more resilient users of VPNs. This finding could be explored to understand the adoption and use of other PETs such as two factor authentication and privacy-enhancing practices like putting a webcam cover on device cameras. If our results indeed extend beyond VPN, this would make clear that as a privacy-enhancing community, we must go beyond the design and development of PETs and explore ways to get people more emotionally involved in protecting their online privacy. For if they have emotional reasons to use these PETs, they are more likely to overcome the hindrances that many of these technologies inevitably entail.

8 Acknowledgement

We would like to thank the respondents to this survey for taking their time to provide us with their insights. We thank Kaileigh Byrne, PhD and Ceren Gunsoy, PhD who provided us with much needed psychological insight and feedback on judgment and decision making. We would also like to thank the moderators of the subreddits who graciously accepted to distribute our survey within their communities.

This research was supported in part by a Facebook Emerging Scholar Award.

References

[1] J. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study," 2017.

[2] F. Schaub, "The implications of the fcc's net neutrality repeal," *Media and Communication*, vol. 6, no. 3, pp. 69–72, 2018.

[3] J. Gillula, "Five creepy things your isp could do if congress repeals the fcc's privacy protections," Mar 2017. [Online]. Available: https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections

[4] A. Kalia, "Here's how to protect your privacy from your internet service provider," 3rd Apr 2017. [Online]. Available: https://www.eff.org/deeplinks/2017/04/heres-how-protect-your-privacy-your-internet-service-provider

[5] P. Ferguson and G. Huston, "What is a vpn?" Tech. Rep., 1st June 1998. [Online]. Available: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-18/what-is-a-vpn.html

[6] 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*. ACM, 2018, pp. 443–456.

[7] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

[8] O. Valentine, "Vpn usage and trends around the world in 2018 - globalwebindex," 2nd Jul 2018. [Online]. Available: https://blog.globalwebindex.com/chart-of-the-day/vpn-usage-2018/

[9] R. Marvin, "Breaking down vpn usage around the world," 21st Sep 2018. [Online]. Available: https://www.pcmag.com/news/363869/breaking-down-vpn-usage-around-the-world

[10] A. Smith and A. Smith, "What americans knows about cybersecurity," Tech. Rep., 22nd Mar 2017. [Online]. Available: http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

[11] M. E. Johnson and N. Willey, "Usability failures and healthcare data hemorrhages," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 35–42, 2011.

[12] J. J. Borking, "Why adopting privacy enhancing technologies (pets) takes so much time," in *Computers, privacy and data protection: an element of choice*. Springer, 2011, pp. 309–341.

[13] T. Caulfield, C. Ioannidis, and D. Pym, "On the adoption of privacy-enhancing technologies," in *International Conference on Decision and Game Theory for Security*. Springer, 2016, pp. 175–194.

[14] R. Knight, "National security or consumer privacy a question even siri couldn't answer," *IPCLJ*, vol. 1, pp. 1–11, 2016.

[15] R. W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security Privacy*, vol. 15, no. 5, pp. 55–64, 2017.

[16] M. G. Maceli, "Encouraging patron adoption of privacy-protection technologies:: Challenges for public libraries," *IFLA Journal*, vol. 44, no. 3, pp. 195–202, 2018. [Online]. Available: https://doi.org/10.1177/0340035218773786

[17] M. D. Molina, A. Gambino, and S. S. Sundar, "Online privacy in public places: How do location, terms and conditions and vpn influence disclosure?" in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '19. New York, NY, USA: ACM, 2019, pp. LBW2616:1–LBW2616:6. [Online]. Available: http://doi.acm.org/10.1145/3290607.3312932

[18] R. Venkateswaran, "Virtual private networks," *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, Feb 2001.

[19] N. P. Hoang and D. Pishva, "Anonymous communication and its importance in social networking," in *16th International Conference on Advanced Communication Technology*. IEEE, 2014, pp. 34–39.

[20] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. ACM, 2016, pp. 1388–1401.

[21] J. Nielsen, *Designing Web Usability: The Practice of Simplicity*. Thousand Oaks, CA, USA: New Riders Publishing, 1999.

[22] G. Norcie, K. Caine, and L. J. Camp, "Eliminating stop-points in the installation and use of anonymity systems: a usability evaluation of the tor browser bundle," in *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS)*. Citeseer, 2012.

[23] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0." in *USENIX Security Symposium*, vol. 348, 1999.

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

[25] A. Alshalan, S. Pisharody, and D. Huang, "A survey of mobile vpn technologies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016.

[26] H. Hamed, E. Al-Shaer, and W. Marrero, "Modeling and verification of ipsec and vpn security policies," in *13th IEEE International Conference on Network Protocols (ICNP'05)*. IEEE, 2005, pp. 1–10.

[27] W. Quesenbery, "The five dimensions of usability," in *Content and complexity*. Routledge, 2014, pp. 93–114.

[28] P. Lew, L. Olsina, and L. Zhang, "Quality, quality in use, actual usability and user experience as key drivers for web application evaluation," in *International Conference on Web Engineering*. Springer, 2010, pp. 218–232.

[29] F. D. Davis, "A technology acceptance model for empirically testing new end-user information systems: Theory and results," Ph.D. dissertation, Massachusetts Institute of Technology, 1985.

[30] L. R. Vijayasarathy, "Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model," *Information & management*, vol. 41, no. 6, pp. 747–762, 2004.

[31] P. J. Hu, P. Y. Chau, O. R. L. Sheng, and K. Y. Tam, "Examining the technology acceptance model using physician acceptance of telemedicine technology," *Journal of management information systems*, vol. 16, no. 2, pp. 91–112, 1999.

[32] C. M. Jones, R. V. McCarthy, L. Halawi, and B. Mujtaba, "Utilizing the technology acceptance model to assess the employee adoption of information systems security measures," *Issues in Information Systems*, vol. 11, no. 1, pp. 9–16, 2010.

[33] G. F. Loewenstein, E. U. Weber, C. K. Hsee, and N. Welch, "Risk as feelings." *Psychological bulletin*, vol. 127, no. 2, pp. 267–286, 2001.

[34] R. P. Bagozzi, "The legacy of the technology acceptance model and a proposal for a paradigm shift." *Journal of the association for information systems*, vol. 8, no. 4, pp. 243–254, 2007.

[35] P. J. Schoemaker, "The expected utility model: Its variants, purposes, evidence and limitations," *Journal of economic literature*, pp. 529–563, 1982.

[36] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of social Issues*, vol. 33, no. 3, pp. 22–42, 1977.

[37] R. L. Thompson, C. A. Higgins, and J. M. Howell, "Personal computing: toward a conceptual model of utilization," *MIS quarterly*, pp. 125–143, 1991.

[38] H. C. Triandis, "Values, attitudes, and interpersonal behavior." in *Nebraska symposium on motivation*. University of Nebraska Press, 1979.

[39] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, ""it's not actually that horrible": Exploring adoption of two-factor authentication at a university," in *Proceedings of the 2018 CHI Conference on*

Human Factors in Computing Systems, ser. CHI '18. New York, NY, USA: ACM, 2018, pp. 456:1–456:11. [Online]. Available: http://doi.acm.org/10.1145/3173574.3174030

[40] M. Tavakol and R. Dennick, "Making sense of cronbach's alpha," *International journal of medical education*, vol. 2, pp. 53–55, 2011.

[41] H. Cho, B. Knijnenburg, A. Kobsa, and Y. Li, "Collective privacy management in social media: A cross-cultural validation," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 25, no. 3, pp. 17–35, 2018.

[42] M. Namara, D. Wilkinson, B. M. Lowens, B. P. Knijnenburg, R. Orji, and R. L. Sekou, "Cross-cultural perspectives on ehealth privacy in africa," in *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, ser. AfriCHI '18. New York, NY, USA: ACM, 2018, pp. 7:1–7:11. [Online]. Available: http://doi.acm.org/10.1145/3283458.3283472

[43] J. S. Dumas, J. S. Dumas, and J. Redish, *A practical guide to usability testing*. Intellect books, 1999.

[44] K. Baxter, C. Courage, and K. Caine, *Understanding your users: a practical guide to user research methods*. Morgan Kaufmann, 2015.

[45] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek, "A summary of survey methodology best practices for security and privacy researchers," Tech. Rep., 2017.

[46] "Qualtrics: The leading research & experience software." [Online]. Available: https://www.qualtrics.com/

[47] S. E. McGregor, E. A. Watkins, M. N. Al-Ameen, K. Caine, and F. Roesner, "When the weakest link is strong: Secure collaboration in the case of the panama papers," in *26th {USENIX} Security Symposiumy (2017)*, 2017, pp. 505–522.

[48] M. B. Miles, A. M. Huberman, and J. Saldana, *Qualitative data analysis: A methods sourcebook*. Sage, 2014.

[49] M. Vaismoradi, H. Turunen, and T. Bondas, "Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study," *Nursing & health sciences*, vol. 15, no. 3, pp. 398–405, 2013.

[50] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and psychological measurement*, vol. 20, no. 1, pp. 37–46, 1960.

[51] M. L. McHugh, "Interrater reliability: the kappa statistic," *Biochemia medica: Biochemia medica*, vol. 22, no. 3, pp. 276–282, 2012.

[52] Z. Bauman, D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. Walker, "After snowden: Rethinking the impact of surveillance," *International Political Sociology*, vol. 8, no. 2, pp. 121–144, 2014.

[53] I. P. Act, "Parliament uk. retrieved 12 january 2017," 2016.

[54] D. Lee, "'netflix for piracy'popcorn time saved by fans," *BBC News–Technology*, vol. 17, 2014.

[55] N. Manworren, J. Letwat, and O. Daily, "Why you should care about the target data breach," *Business Horizons*, vol. 59, no. 3, pp. 257–266, 2016.

[56] T. Sharp, "Theorizing cyber coercion: The 2014 north korean operation against sony," *Journal of Strategic Studies*, vol. 40, no. 7, pp. 898–926, 2017.

[57] C. Fennell and R. Wash, "Do stories help people adopt two-factor authentication?" *Studies*, vol. 1, no. 2, p. 3.

[58] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *Isjlp*, vol. 4, p. 543, 2008.

[59] R. Tourangeau and T. Yan, "Sensitive questions in surveys." *Psychological bulletin*, vol. 133, no. 5, pp. 859–883, 2007.

A The Survey

Display the consent form.
Thereafter, we display the questions below:

Awareness about VPN.
Q1. Do you know what a Virtual Private Network (VPN) is?
o Yes o No

Display This Question If: Q1 = ***No.***
Q2. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. View the video below for more information: https://www.youtube-nocookie.com/embed/_ll_rfifCII?rel=0&start=32

Q3. What did you understand about VPNs from watching the video?

Q4. What do you think would make you use a VPN?

Display This Question If: Q1 = ***Yes.***
Q5. Please select one that applies:
o I have never used a VPN application
o I paused or stopped using a VPN application
o I currently use a VPN application

Display This Question If: Q5 = ***I have never used a VPN application.***
Q6. Are you considering using a VPN any time soon?
o Yes o Maybe o No

Perceived Reason to use a VPN(*For those have never used a VPN application*)

This question was displayed for all responses to Q5 but framed accordingly e.g the framing for those that had never used a VPN application would be; ***What reasons would you likely use a VPN?*** *while that for those that that had stopped using a VPN application would be:* ***What were the reasons for your use of a VPN application?***

Q7. What [were/ are] the reasons [for your/ would you likely] use a VPN? [Select all that apply]

- □ Personal privacy
- □ Remotely access work/school network
- □ Access the web freely
- □ Other[7]

Q8. What steps in detail are you taking towards the use of a VPN?

Display These Questions If: Q1 = No And Q2 Is Displayed ***Or*** *If Q5: = I have never used a VPN application And Q6 = Yes Or Q6 = Maybe.*
Q9. What do you see as the main advantages, if any, of using a VPN?

Q10. What do you see as the main downsides, if any, of using a VPN?

Q11. How do you currently protect your privacy online?

Q12. Based on what you know so far, how likely are you to use a VPN?
- o Very unlikely
- o Somewhat unlikely
- o Neither likely nor unlikely
- o Somewhat likely
- o Very likely

The following questions for the three constructs 1) Affordance of a VPN to protect user privacy, 2) Ease of use of a VPN application, and 3) Difficulty of selection and installation of a VPN were asked for all responses to Q5 but framed accordingly e.g the framing for those that had never used a VPN application would be; ***Using VPNs will help me protect my privacy online.*** *while that for those that had stopped/currently use a VPN application would be;* ***Using VPNs help[s/ed] me protect my privacy online.***

Affordance of a VPN to protect user privacy.
Please select how much you agree with the following statement about VPNs:
Q13. Using VPNs [will help/help[s/ed]] me protect my privacy online.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree
- o Strongly agree

Q14. [I think that] it is worthwhile to put in the effort to use a VPN.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree
- o Strongly agree

Q15. [I think that] it is important to learn about the benefits and drawbacks of using a VPN.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree
- o Strongly agree

Q16. [I am motivated to / I] carefully consider[ed] whether I want[ed] to use a VPN.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree
- o Strongly agree

Q17. [I should consider using/I suggest that people should use] a VPN at any necessary cost for my [their] online privacy protection.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree
- o Strongly agree

Ease of use of a VPN application.
Please select how much you agree with the following statement about the usage of VPNs:
Q18. [I think that] learning how to use a VPN [would be/is] difficult.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree
- o Strongly agree

Q19. [I think that] a VPN [would be/is] difficult to use.
- o Strongly disagree
- o Disagree
- o Neutral
- o Agree

7 5/37 abandoners and adopters had a substantially different answer from the ones we provided as options

o Strongly agree

Q20. [I think that] a VPN [would be/is] easy to use.

o Strongly disagree
o Disagree
o Neutral
o Agree
o Strongly agree

Difficulty of selection and installation of a VPN application.

Please select how much you agree with the following statement about the usage of VPNs:

Q21. [I think that I would have/ I had] a hard time deciding on the best VPN application/provider to use.

o Strongly disagree
o Disagree
o Neutral
o Agree
o Strongly agree

Q22. [I think that] installing a VPN [would be/is] difficult.

o Strongly disagree
o Disagree
o Neutral
o Agree
o Strongly agree

Q23. [I think that] installing a VPN [would be/is] easy.

o Strongly disagree
o Disagree
o Neutral
o Agree
o Strongly agree

Q24. [I think that] installing a VPN [would be/is] a lengthy process.

o Strongly disagree
o Disagree
o Neutral
o Agree
o Strongly agree

Actual Reason for use of a VPN (*For those that paused and or continue to use a VPN application*)

A question similar to Q7 was asked but framed according to the situation i.e stopped use/currently use a VPN

If survey recipient response to Q7 did not include ***"Personal Privacy"****, then they are sent to the end of the survey. Otherwise, we displayed the questions below thus making the remainder of the study based on respondents use of VPN for personal privacy protection reasons only.*

Q25. In detail, how did you finally end up using a VPN especially for personal privacy protection purposes? [You can include all the reasons that led you to using a VPN and all the next steps you undertook thereupon]

Q26. How did you learn about VPNs for personal privacy protection purposes?

□ Friend/Social Media recommendation
□ Online/Website (e.g VPN affiliate, VPN site, Blog etc) recommendation
□ Work/School recommendation
□ Other [8]

Q27. Upon learning about VPN, what sparked your desire to actually use it for personal privacy protection?

Q28. How did you find and decide on the best VPN provider that met your needs for personal privacy protection?

Period and Type of VPN Used

Q29. How many VPN applications/providers [have/did] you [tried/try] out?

o 1
o 2
o 3
o 4
o 5+

Display This Question If: Q29= 1.

Q30. Which VPN application/provider did you eventually decide to use for personal privacy protection?

Display This Question If:Q29 >= 2

Q31. Which VPN application/provider did you first decide to use for personal privacy protection?

Q32. Why did you finally decide to use that VPN application/provider?

Q33. For how long [have/did] you use[d] that VPN application for personal privacy protection?

o Several years

8 6/37 abandoners and adopters had a substantially different answer from the ones we provided as options

o About a year
o Several months
o About a month
o Several weeks
o About a week
o I do not remember
o Other

Display This Question If: Q5 = I paused or stopped using a VPN application And Q7 = Personal privacy.
Q34. Why is it that you paused or stopped using a VPN for personal privacy protection?

Q35. [Is/Was] the VPN application you [first] use[d]:
o Free o Paid o Paid with a trial period

Display This Question If: Q35: = Free.
Q36. What factors, if any, made you decide to use a free VPN application?

Display This Question If: Q35: = Paid .
Q37. What factors, if any, made you pay for the VPN application?

Display This Question If: Q35: = Paid with a trial period .
Q38. Did you end up subscribing for the VPN application after the trial period?
o Yes o No o I am not sure

Display This Question If: Q38: = Yes.
Q39. What factors, if any, made you subscribe to the VPN application after the trial period?

Display This Question If: Q38: = No .
Q40. Why did you decide not to subscribe for the VPN application after the trial period?

Q41. Did you have any problems during the installation process of the VPN application?
o Yes o No o I do not remember

Display This Question If: Q41: = Yes.
Q42. What were some of the problems you faced during installation process?

Q43. How did experiencing these problems make you feel?

Q44. Did you make any other configurations to the VPN application after its installation?
o Yes o No o I do not remember

Display This Question If: Q44: = Yes .
Q45. Why is it that you made these configurations?

Q46. Did you review the VPN provider's privacy policy or terms of service before installation?
o Yes o No o I do not remember

Display This Question If: Q46: = Yes.
Q47. Based on these policies, is there anything that stopped you from using the VPN application from this VPN provider?

Q48. What are the benefits, if any, that you found using a VPN?

Q49. What are the disadvantages, if any, that you found using a VPN?

Q50. What problems, if any, did you encounter in the process of finding, deciding, installing and using a VPN?

Q51. Do you have any other comments about your usage of a VPN?

Demographics
Q52. Gender
o Male o Female o Prefer not to answer

Q53. Age
o 18 - 24
o 25 - 34
o 35 - 44
o 45 - 54
o 55 - 64
o 65 - 74
o 75 or older
o Prefer not to answer

Q54. Nationality [Current country of residence]; Country: Afghanistan (1) ... Zimbabwe (198)

Q55. If current country of residence is different from the nationality, how long have you lived in your country of residence? (We ask this question because there are cultural differences in how people deal with their personal information).