A SHORT, QUALITATIVE ANALYSIS OF VIRTUAL PRIVATE NETWORKS

By

Alexandra Bonder
Bachelor of Humanities, Carleton University, 2010

A major research paper
presented to Ryerson University and York University

in partial fulfillment of the requirements for the degree of
Master of Arts
in the joint program of
Communication and Culture

Toronto, Ontario, Canada, 2018

Author's Declaration

I hereby declare that I am the sole author of this MRP.

This is a true copy of the MRP, including any required final revisions.

I authorize Ryerson University to lend this MRP to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this MRP by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP may be made electronically available to the public.

A SHORT, QUALITATIVE ANALYSIS OF VIRTUAL PRIVATE NETWORKS

Master of Arts, 2018
Alexandra Bonder
Communication and Culture
Ryerson University and York University

ABSTRACT

This paper provides an overview of the current state of Virtual Private Networks (VPNs) by combining a general analysis of key issues with the perspectives of employees working at five popular VPN companies. This paper argues that VPN technology cannot be analyzed in a meaningful way without reference to the values and motivations of the people of which the companies comprise. A key finding is the differences observed between different employees' understanding of terms essential to VPN competence: "security" and "privacy". These differences highlight the difficulty of judging VPNs objectively, as, their perceived functionality ultimately depends on an affective alignment of values between user and company.

Acknowledgements

I would like to acknowledge my MRP supervisor, Professor Gregory Elmer, who has supported me throughout my time at Ryerson University, always encouraging me to think critically and creatively.

I would also like to acknowledge my second reader, Professor Catherine Middleton, who reignited my curiosity about communication policy, upon my return to academia.

Lastly, but very importantly, I would like to acknowledge my father, Arieh Bonder, whose unwavering belief in me has allowed me to complete this project.

Table of Contents

INTRODUCTION

In 1998, writing on Wired.com, in a column dedicated to “deflating this month’s overblown memes”, author Steve Steinberg described Virtual Private Networks (VPNs) as a fad with a life expectancy of 18 months. “The wonderful thing about virtual private networks,” he wrote, “is that its myriad of definitions give every company a fair chance to claim that its existing product is actually a VPN. But no matter what definition you choose, the networking buzz-phrase doesn't make sense. The idea is to create a private network via tunneling and/or encryption over the public Internet. Sure, it's a lot cheaper than using your own frame relay connections, but it works about as well as sticking cotton in your ears in Times Square and pretending nobody else is around.”

Twenty years later, VPNs still exist and thrive, being used by millions of individual users all over the world. Though once used primarily by businesses to provide secure, remote server access to employees, individuals are now using VPNs for purposes that go far beyond their original corporate roles, from accessing geo-blocked content to evading state sanctioned censorship of social media sites and more (Longworth). And yet, many of the same issues alluded to in the above short quote remain true today.

The aim of this paper is to get a better appreciation of the intentions of VPN creators in order to gain a more holistic understanding of VPNs beyond the technology itself. As the political theorist Michel Foucault says, the effects of power are not only negative. Rather, power creates its own reality (194). If this is the case, VPNs, do not only create free spaces, but also inject these spaces with meaning. What type of meaning does the VPN world hold, and, on a larger scale, what impact do VPNs have on online security, beyond simply upholding concepts of a “free Internet”? Ultimately looking at

VPNs through this lens may help us to define VPNs more accurately, and help to determine if they can indeed act as powerful tools for online security and privacy.

In order to do this, I have chosen to conduct interviews because the competence of VPN technology is highly reliant on how it is being administered. And though it is never possible to completely understand the true intentions of those working at VPN companies, I hope to provide a small peek into their own values and motivations and how these may potentially inform the functionality of their product.

BACKGROUND

What exactly is a VPN? And are VPNs actually effective in providing the security and privacy for citizens that they claim to offer? Are the promises made by VPNs, in fact, more hype than substance?

The purpose of VPNs is to provide subscribers with secure and private Internet connections. This is carried out through the application of security protocols, most commonly the use of “tunneling”, the hiding of a user’s IP address, and the encryption of data (Microsoft 2001). Tunneling in personal use VPNs, generally refers to the transmission of VPN protocols, encapsulated with more VPN protocols, transmitted over a protected network. This insures that whatever being passed over the network is kept private until it is received on the other side of the network (“How VPN Works”).

As governments and corporations attempt to restrict and influence Internet access, VPNs are widely seen and used as a tool to fight back against Internet constraints, and to keep the Internet “free”(Chen) (Amnesty International). Freedom can be defined in many different ways, and can be in reference to the Internet as it was first conceived, i.e. with a lack of centralized control, or it can be defined in its democratic sense, i.e. a space that allows for freedom of speech and expression (Amnesty International).

Though VPNs have been outlawed or heavily restricted in many countries, for example, in China and Russia, this has not stopped their user bases from growing ("VPN Market Worth $41.702 Billion"). Their lack of regulation is essential to their use in some countries as a tool of resistance. However, the lack of information about them, because of the absence of regulation, also leaves users vulnerable to security risks, as they have little way of knowing how secure and competent the service provided is.

This reality was brought to light in a 2016 study by Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO), which revealed that many of the most popular VPNs actually do the exact opposite of what they were assumed to do. In many cases, rather than providing privacy, they tracked user data, failed to encrypt Internet traffic, and even shared and sold user data to third parties (CDT) (Ikram) (White). As Internet Security Expert Kevin Wriggle said in a TechDirt podcast on the subject, "The median VPNs are somewhere between incompetent and actively malicious…"

From this alone, it can be inferred that VPNs, as they exist today, do not categorically provide privacy and security for citizens. And so, the "freedom" implied by the use of VPNs cannot be assured. Is this lack of security an intrinsic shortcoming of VPN technology, or the "incompetence" of subpar developers? Or rather, is a VPN's level of privacy and security a conscious choice of its creators? If so, what are the reasons behind their choices, and what are the effects of these choices on their products?

Though studies have looked at the technological functioning of VPNs, none have looked at their moral positioning and the political implications of this, information which could help to better understand the reasons behind some of their shortcomings, as well as shed light on their potential strengths as an Internet security tool for everyday citizens (Ikram) (CSIRO). I use the terms "motivations" to describe the subjective positioning of those working at VPN companies, and "political" to describe the implications of this positioning when it comes to the choices that are being made. I would argue that the value of a VPN is at least partially determined by their application. In other words, VPNs, as a category, cannot be judged by their technology alone. They must also be evaluated within the context of their creation, which includes examining the subjective political/ethical positioning of their creators.

When the Australian CSIRO first published their 2016 study, at least one VPN company, TunnelBear, took the initiative to hire a third-party security auditing group to evaluate the legitimacy of their platform and to confirm its ability to provide security and privacy (TunnelBear 2017). TunnelBear did this despite claiming to have had a 200% increase in sales, due to media coverage of the United States' Federal Communications Commission's (FCC) "attack" on net neutrality (Silverman). This seems to have proven genuine interest in the quality of their product - an ethical stance - that allowed them to improve their product. However, one might ask why it took negative publicity to instigate action? Understanding the "why" might help to better predict how VPN companies could seek to improve themselves in the future.

A BRIEF HISTORY OF VPNS

As outlined by Janet Abbate, in the book, Inventing the Internet, the Internet was initially created to establish a more secure communication infrastructure in case of a major terrorist attack (2). Before its creation, military communication relied on telecommunications infrastructure that transmitted data through centralized hubs (4). Basically, data was passed through a single series of hubs, from one party to another. The centralization of these hubs made this type of communication physically vulnerable. If one hub were to go down, communication between two parties would be terminated (6). The Internet, on the other hand, passes data through millions of routers or “Secure Internet Servers”. Even if hundreds of routers were to go down, data could automatically re-route itself along a different series of routers to get to its target.

The only problem is, although the Internet is more physically secure than traditional telecommunications infrastructure, data-wise it is not (Gupta, 5). Each router through which data passes can be easily accessed; its content can be viewed by those maintaining the server, making it vulnerable to security threats (for example, hacking or government surveillance) (Gupta, 4). VPNs were created to help remedy these vulnerabilities, and were originally used as an affordable way for organizations to connect remote points, such as users, databases, or whole offices, to an organization’s central secured network (Mohta) (LaBorde) (Dawson). Many cite the first VPN as being created in 1995 by Gurdeep Singh-Pall, who is currently Vice President of Skype at Microsoft, but who was, at that time, a Microsoft computer engineer (Crunchbase).

So what exactly is a VPN? Internet security giant, and one of the first VPN providers, Cisco, provided a “common sense and simple” definition for VPNs in 1998.

“A VPN is a private network constructed within a public network infrastructure, such as the global Internet.” In other words a VPN is a secure and private space created within the larger, open Internet (Robinson). VPN expert John Longworth provides a little bit more information, defining them as,

> VPNs are used to protect data from being accessed or altered as it travels over another network (e.g. the Internet). This is possible through the use of a wide variety of computer protocols that securely ‘wrap’ your data in a layer of encryption and ensure that the destination for that encrypted data is authenticated (i.e.: the person or system is who it says it is) and authorised (allowed) to ‘unwrap’ it. In other words, VPNs allow users to securely access a private network and also share data remotely.

VPNs work by combining security protocols and layers of encryption. For example, a VPN usually uses “tunneling” protocols, which, in common terms, means creating a virtual “tunnel” between routers (Norton). These “tunnels” create a private network within the larger open Internet through which data can be passed. In addition, if the VPN detects it is being attacked, it will automatically re-route, to create a new protected tunnel along a different set of routers (Upfal). The information within the tunnel is encrypted, so even if attackers penetrate the tunnel, it would be difficult to decipher the data carried within (Norton). There is also ideally a layer of “authentication” to ensure you are who you say you are, which prevents anyone else from intercepting your communications, disguised as you.

One important effect of VPNs is that, to outsiders, your IP address will appear to come from wherever the VPN server is located. An IP address is a unique string of numbers that identifies your specific computer over a network. It also holds information about where your computer is geographically located. This allows Internet Service Providers (ISP), the government, or other regulatory bodies to create barriers around your Internet experience. For example, because of copyright laws, certain shows on Netflix might only be available in the US versus Canada. It is important that those in the "private" network established by a VPN are not only unaware of the content of the data, but of the private relationship itself (Cisco). As Internet security protocols and encryptions are constantly being updated, a well-functioning VPN will use the most secure and up-to-date ones, in order to maintain the functions mentioned above, intrinsic to competent functioning (Cisco). This is why VPN companies often advertise the fact that they do not keep "logs" (i.e. personal details) of user data (Nord) (TorGuard) (TunnelBear).

Using most commercial VPNs is relatively easy. An individual will download a client VPN on to their computer, usually logging in with a username and password. This will connect the individual to a server VPN. The individual's IP address will now appear to be that of the server VPN (Microsoft). The user can now, supposedly, carry out his or her Internet activities with complete confidence about the security of their transactions.

THE DEPICTION OF PERSONAL-USE VPNS IN THE MEDIA

For the purposes of this paper, I will define "personal-use VPN" as a VPN that is being used by a private user, versus a VPN that has been established by a company or organization. It is difficult to find information as to when the first personal-use VPNs began to gain popularity, but articles describing personal-use VPNs seemed to gain mention in the mid to late 2000s. News articles from major outlets during that time usually mentioned VPNs as tools to combat Internet restraint and censorship. For example, a 2011 BBC article, quoted VPN, Hotspot Shield as reporting a 1000% increase in usage during the Arab Spring ("Turkish people turn to VPNs"). Another early market to adopt personal VPN technology, beginning in 2010, were Chinese users, who were attempting to circumvent the Great Firewall of China (Nie). Another early instance of VPN use was in 2011, when the Iranian government released plans to build its own national, limited Internet service (Bazley). In such cases, the consequences of using and administrating a VPN are clearly and primarily political. "Political", in this case, meaning the VPN is being used as a tool to avoid censorship, mobilize people, in an environment that is hostile to such things.

Though VPNs may have first gained popularity for personal use due to their political potential, most VPNs generally advertised themselves as providing the same things as VPNs that are being used for business purposes, that being security and privacy. And, it turns out many people are indeed using VPNs. Two GlobalWebIndex studies found that 1 in 4 people had used VPNs in 2016, with this number up to 1 in 3 in January 2017. While Indonesia was the country with the highest concentration of VPN use from 2013 to 2016, with 41% of users relying on a VPN connection in 2016, in 2017 Turkey took the top spot with close to 50% of Internet users using VPNs. Heavy government censorship was cited as the reason for this uptake (GlobalWebIndex).

Countries where VPNs are illegal also have significant concentrations of VPN users, with China at 29% and Vietnam at 35% (GlobalWebIndex). US saturation is at a lower 25%, although since this study was put out in 2016, there is a chance things may already have changed. One VPN company, TunnelBear, claims its North American sales have rocketed throughout 2017, with policy changes surrounding net neutrality in the United States (Silverman).

VPN use also skews to a younger demographic, with a separate study by GlobalWebIndex stating: “If we split the overall figures for VPN usage by age then it’s 16-34s who dominate. In fact, with 16-24s on 35% and 55-64s on just under 15%, the youngest demographics are over twice as likely to be using VPNs as the oldest ones. Such a pattern suggests that overall numbers will rise still higher in the years ahead.” (Young)

Though security and privacy may be the main purpose of VPNs, as Jason Mander, of GlobalWebIndex says, "In some countries, China, Indonesia and Thailand being prime examples, people use VPNs to overcome governmental restrictions on sites like Facebook and Twitter. In Western Europe, privacy is the biggest factor. But by far the most popular one globally is the need to access [geographically blocked] entertainment content” (Nave). This refers to content that is not available to the consumer due to either licensing or political barriers.

Although the general purposes of using VPNs may be similar globally, the consequences of doing so vary from country to country. For example, in Vietnam, where VPNs are illegal, what you say and consume online can have serious consequences. For example, in the past year, activist Tran Thi Nga was sentenced to nine years in prison, female blogger, Ngoc Nhu Quynh was sentenced to 10 years, and four other activists, Pham Van Troi, Nguyen Trung Ton, Truong Minh Duc and Nguyen Bac Truyen, are still awaiting trial. All the aforementioned were arrested, and/or charged based on their online activity. In the United Arab Emirates, using a VPN could cost you a fine of up to

$7,000,000 CA (“Federal Decree-Law no. (5) of 2012”). In early 2017, the owner of a Chinese VPN provider was jailed seven years.

In countries where you can be jailed for any type of online activism, or where there is heavy online censorship, the reasons a citizen would want to protect their privacy and security are obvious. But why would a Canadian, or an American, who has far greater civil liberties, and with access to an Internet that is relatively free of censorship, need a VPN?

One reason is to circumvent geo-blocking; i.e. gain access to geographically restricted content, usually due to copyright laws. For example, American Netflix has a different offering than Canadian Netflix, therefore Canadians might use (or at least try to use) a VPN to access this content. Whereas there have been no legal ramifications of using a VPN so far in Canada, there is vocal discouragement from some content distributers and creators, such as Bell Media and Netflix, who view this type of access akin to piracy (Fullagar) (Evans). Many Canadians, however, do not see circumventing geo-blocking as “piracy” but rather, view it as their intrinsic right to access whatever they want online.

Canadians also use VPNs for more general privacy and security concerns. For instance they may be accessing the Internet on an open connection at a local café, and want to ensure others cannot track their details. There are also general concerns about surveillance by corporations, and the government (Khazan). As infamous leaker Edward Snowden has proven, the Government, even in rich, democratic nations, is liable to stick its nose into places where it (arguably) does not belong. But, although most Canadians and Americans may care about security and freedom in theory, the majority has proven to care to a lesser extent about security and freedom in practice. A 2015 American study by Pew Research found that “Americans feel privacy is important in their daily lives in a number of essential ways… Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age.” (Madden and Lee) At the same time, the studies show that although Americans believe policy should be put in place to protect their privacy, “few have adopted advanced privacy-enhancing measures” (Madden and Lee). This is all to say that VPNs are used to access different types of content in different countries, and the need for VPNs to actually provide a high level of privacy and security differs from country to country.

MAIN CRITICISMS OF VPNS

Although VPN companies have been widely heralded as essential to security and privacy online, they have also been widely criticized for a number of reasons. One common criticism is that they provide a haven for illegal activity, although what constitutes criminal activity can be vague and wide-ranging. For example, as one interviewee pointed out, illegal activity associated with VPNs in North America consists of more isolated and “acute crimes”, for example, a person downloading child pornography (Reed et al.). For select content creators and distributors downloading copyrighted material, or bypassing geo-blocked content via a VPN, may be frowned upon and discouraged but, even then, not considered illegal. This is the case in Canada, where it is considered legal grey territory (Jackson). In other countries, for example countries with strong censorship laws, like Egypt, the government may be concerned that VPNs allow people to access content, organize, and speak against laws and policies in a way that would constitute illegal activity.

If we look at “acute” crimes, an interesting paradox arises. Often the same cases that put dangerous criminals away also reveal real security breaches in the services themselves. For example, certain VPN companies have been known to hide the identity of drug dealers and those involved in child pornography, amongst other nefarious actors (Reed et al.). Since VPN companies, as part of their intrinsic functioning, are not supposed to keep logs of their users, it makes it difficult for authorities to find the perpetrators of such crimes, although not impossible. Technically they should not be able to, since, a competent VPN company, as defined by Microsoft, “should not know” who is using their service. Exactly what they should not know is vague, and varies from company to company. For example, some VPN companies may ask for a name when you sign up for their service, while others may ask for only an email. If your email contains your name, it will be easy for the company to know who is using their service, and potentially share this information. In the VPN world, this security function is known as “not keeping logs” and many VPN companies will advertise “no logging” directly on their websites. However, VPN companies, under legal pressure, have often proven this is not the case.

One example can be seen in the case of 24-year old Ryan Lin. In March of 2017, Lin was arrested and charged with cyber stalking, amongst other related crimes, with help from information from his VPN service Pure VPN (one of the largest VPN providers). As stated in the official criminal complaint, records from Pure VPN show that the same email accounts, Lin's Gmail account, and the teleport Gmail account, were accessed from the same WANSecurity IP address (“United States of America v. Ryan S. Lin”). Significantly, Pure VPN was able to determine that their service was accessed by the same customer from two originating IP addresses: the IP address from the home Lin was living in at the time, and the software company where Lin was employed at the time.

Take HotSpot Shield, a Silicon Valley-based and well-promoted VPN company that was founded far back in 2005, and was credited for being used to help activists during the Arab Spring in Egypt, Tunisia and Lebanon (Whittacker). Advertising initiatives for HotSpot Shield have included a political billboard reading, “Angela Merkel was hacked should have used HotSpot Shield” (see image 1).

This leads us to another critique of VPNs: their potential maliciousness. In a 2016 article by popular Internet security website ZDNet entitled “Why Hotspot Shield's co-founder puts privacy over profits” co-founder David Gorodyansky explained that 97% of his users got the service for free, through an “ad-supported” version of the service (Whittacker). He added that they did not know data-per user or names, and they promised “shielded connections, security, privacy enhancement for individuals and small businesses and an “ad-free browsing” environment (Whittacker). However in the CSIRO report previously mentioned, it was found that HotSpot Shield actively tracked its users, injecting Javascript for tracking and advertising purposes, and redirected “e-commerce traffic to partnering domains”. In light of these revelations, the Centre for Democracy and Technology has submitted a complaint to America’s communications regulator, The Federal Communications Commission (FCC), stating, in summary that their service is “unfair and deceptive” in its promise of “secure, private and anonymous” access to the Internet (“Complaint, Request for Investigation”).

should have used hotspot shield
Angela Merkel ~~was hacked~~.
AnchorFree.com
Hotspot Shield: Security, Privacy, Access
CBS
Diamond Nails & Spa

Image 1

For the average user, it is often very difficult to tell the intentions and legitimacy of a VPN company. Take Israeli-based Hola, for example. In 2015, Hola had an overall 46 million users, many of them opting for the “free” version (Andy). As first reported by TorrentFreak, but confirmed by security firm Vectra, with additional confirmation by Hola’s founders, Ofer Vilenski and Derry Shribman, the free version routed traffic between VPN users. Essentially, a user’s IP address was re-associated with other traffic so that the company did not have to buy bandwidth (Andy) (Vectra Threat Labs). This left users unprotected from the traffic that was now being associated with their IP.

Hola also sells their user bandwidth to others through their own affiliated company, luminati.org (“Multiple Critical Vulnerabilities”). When a free user’s bandwidth is sitting idle, Hola would allow third parties to buy it. These third parties used it to host botnet attacks (“Multiple Critical Vulnerabilities”). A botnet attack is when a string of computers are used together, often to spam on a large scale. In this case, the consumers were also the product. Is this really a VPN or simply a “geo-unblocking” service, that doesn’t really provide privacy or security?

More disturbing is something computer science researcher and popular Internet personality Eli Upfal pointed out in a 2016 post entitled “Are Free VPN Services As Safe As Paid VPN?”, “Let me tell you what. If I was in charge of the fucking NSA and I had billions upon billions upon billions of dollars to spend, you are damn motherfucking right I would drop 10 million dollars to create one of the best VPN services the world has ever seen…if I was in charge of the NSA I would create free VPN services. If I was part of the Russian Intelligence Service I would create free VPN services. If I was part of the Chinese Intelligence Service I would create free VPN services. Because isn’t that a great, phenomenal idea?” (Upfal). Indeed, it looks like this has been the case, starting in Syria in 2012 to devastating effects. Freedom House reported that, “Due to the prevailing need for circumvention and encryption tools among activists and other opposition members, Syrian authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful Trojans.” (“Syria”). Basically, the VPN service would appear to be protecting the anonymity of individuals, but would in fact be feeding all data to Syrian authorities.

THEORETICAL FRAMEWORK FOR THE ANALYSIS OF THE UNDERLYING PHILOSOPHIES OF VPNS

As it can be seen in the preceding sections, VPNs have been both praised for their capacity to create “freedom” and criticized for things such as hiding criminals, and ignoring copyright laws (Reed et al.). In addition, VPNs have also found themselves in controversy for saying one thing and doing another, like in the case of Hola. My goal is to try to get an initial understanding of the motivations and decision-making processes that direct VPNs, as well as an understanding of the political implications of their application and operations. This analysis will be based both on the research collected on the operations of VPNs and on interviews carried out with VPN providers. I will critically analyse my data through the theoretical perspectives of Zizi Papacharissi and Chantal Mouffe, two philosophers whose work has provided a useful prism through which to view and assess the interactions of individuals and organizations.

Of particular interest to me, is Papacharissi's description of "affect" in her book Affective Publics, and Mouffe's description of decision-making, as described in Agnostics: Thinking the World Politically. Applying these conceptual understandings to the data I collected on VPN providers could help provide a better understanding of the values held by the VPN providers interviewed and the political implications of these values in the context of the operation of their companies.

Affect, most generally, is focused on the "forces other than conscious knowing" that position us to make choices, join movements, and ultimately direct us within the world (Gregg and Seigworth). My goal in interviewing those working at VPN companies is to look at affective qualities that feed into both motivations and decision-making processes. These are ultimately the qualities that direct and define concepts like "security" and "freedom" when these concepts are applied in the world. In other words, concepts like "security" and "freedom", which are essential to VPN technology, have different meanings depending on who is defining them, and how they are being applied. I want to understand how they are being defined, and the implications of varying definitions.

Mouffe and Papacharissi both argue that we are connected to each other “affectively”, that is, based not on rationality alone, but on multiple strong primordial affinities, which create and influence our subjective understanding of the world (Agnostics 46) (Papacharissi 8).

Papacharissi describes new media as being particularly affective (4). Through new media, storytelling is facilitated across the world, triggering affective responses, and community building among different causes and geographically distant people (68). This allows people to “feel” their way through various movements and their impacts, despite never having experienced them first-hand (4). The new communities on the Internet are, in many ways, imagined — they are not based on lived experiences (4). And yet they can add momentum to any movement by bringing multiple differing perspectives together for a shared goal (37). Papacharissi uses the social media platform Twitter to trace these affective connections through activist-driven political movements. For example, the Arab Spring, which saw an international community come together to support the singular causes of oppressed peoples (6).

I will argue that the “VPN world”, i.e. those who work for VPN companies, are affectively connected to both other companies and their users, creating a force of mutual affect. The owners of VPN companies make their own affectively derived positions concrete in the running and execution of their companies. Rather than just providing support through their voice, like a Twitter user, they also provide a service. In the running of their businesses they reveal a point of view, which becomes realized through their decisions. And this does not happen in a vacuum; the similarities and differences in how these companies are run creates an unofficial, ever changing, standard of conduct in an industry that is impossible to formally standardize. Such companies are "policed" by each other, along with community members, for example, those who are interested in Internet security, and customers. But what informs these standards? Mouffe believes that decisions are necessarily exclusive (Agnostics 3). As she said in a 2005 interview, "…if you choose one thing, you necessarily exclude the other. Decisions have to be made, and to decide on one alternative is to exclude the other." (Pluralt) This means you have to show preference to certain reasoning over all others. Though decisions may be arrived at affectively, the results will have real effects, which, can be analyzed in a more objective manner (6). For example, if a VPN owner says that they believe in "privacy and democracy" but is confronted with the choice of either helping authorities track down a child predator or refusing to give away data, which value will end up dominating? How does this choice, in a broader sense, change what it means to provide "privacy and security" for that company? And from what affective perspective is one able to come to this choice by?

The practical reality of a VPN, and the affective reasoning of VPN employees, can be contrasted to reveal a point-of-view, which can then be used as a starting point to analyze their overall take on security and freedom.

INTERVIEW OVERVIEW

Given the above discussion and as a means to seek a better understanding of the role VPNs play in today's world, I interviewed employees of five popular VPN companies.

The primary purpose of these interviews was to gain a better understanding of the basis upon which their companies were run, in the absence of formal regulation.

To identify my candidates, I started by interviewing two people who had been referred to me by friends. My initial plan was to ask these employees to refer me to other employees at different VPN companies. Unfortunately, both connections were unable to refer me to anyone. The general impression I received throughout my interviews was that there was intense competition between companies, and there were few personal connections between employees at different companies. As one of my interviewees told me when I mentioned people in the industry were hard to track down, “we sell privacy and anonymity, so you didn’t select the easiest people to get in contact with” (Company C). I then reached out to over 50 popular VPN companies via contact details provided on their websites, and when available, LinkedIn. These companies could be found on multiple lists from top privacy, security, and VPN-focused websites (Eddy). Since my interviews were anonymous, I will refer to the companies as Companies A through E. Each employee interviewed has also been given a pseudonym.

To provide a brief description of each company, the first, Company A, is a popular and highly rated VPN service, one of the few that has publicly sought to gain legitimacy by inviting third party scrutiny of its operations. On their own website, Company A described itself as “really, really simple privacy apps” which provided “simple, private, free access to the open Internet you love.” From this company, I interviewed Luke, the head of marketing and Jack, a programmer. I was connected to Jack through a friend, who connected me to Luke, as he thought Luke might be able to answer questions he could not. There were no other employees available to interview. I asked if they knew of anyone else in the VPN world I could talk to, but they did not.

Company B was co-founded by leaders in the anti-copyright movement. The first headline on their website read, “Big Brother is watching YOU ...we are not”. Reviews of the VPN service were relatively good, although one website, BestVPN.com, did describe them as keeping limited amounts of user data. I connected to Karl, of Company B, by reaching out on their online FAQ chat. Karl offered tech support for Company B, as well as working as a developer.

The third company I spoke with, Company C, was more difficult to find information on, and its services had mixed reviews online. Company C’s homepage described it as allowing you to “bit torrent anonymously, bypass throttling, and unlimited speeds”. I connected with Thomas of Company C through a friend. Thomas is one of three employees who works at Company C, and does site maintenance, marketing, and tech support.

Company D was very well rated by most websites surveyed. Their website lead with sales messaging for special pricing before describing “total security” and “absolute privacy” as their main goals. I connected to Heather, of Company D, by reaching out to the company directly. Heather does tech support, as well as marketing.

Company E was also highly rated. They advertised themselves as a “Security and Privacy” VPN but open with a “Streaming Guarantee”, promising users would be able to watch live events with a strong and fast connection. At the time of this paper, the World Cup was being aired, and soccer images were present on Company E’s homepage. Philip of Company E was the head of marketing. I reached out to him by contacting the company directly.

Both Company A and Company C listed their addresses in Toronto. On their homepages, each company at least alluded to “privacy”, and most, with the exception of Company C, alluded to “security”.

INTERVIEW QUESTIONS AND METHODOLOGY

The questions I posed to the five companies were in the form of a semi-structured interview, as described by Anne Galletta in the book, “Mastering the Semi-Structured Interview and Beyond”. This involved encouraging more candid answers and conversations that provided a better understanding of the context from which VPN companies have emerged.

My questions are provided below. In addition, in the tradition of semi-structured interviewing, I asked follow-up questions based upon my interviewees’ answers and on the general flow of our conversation. I divided my questions into two categories: Personal Motivational Questions, and Practical Questions. I did this because, as stated previously, my goal is to try to get an initial understanding of the motivations that may inform the decision making processes within VPN companies as well as an understanding of the political implications of their applications and operations, i.e. their “real consequences”. People, according to Papacharissi, have personally motivated reasons for acting, based on their own backgrounds, but some of these reasons, although reached to on an individual level, all feed into larger, common ideals (71). By speaking to individuals about their own personal thoughts, I can begin to consider what themes inform the decisions being made at VPN companies, from the inside. I am asking “factual questions” to get background on the actual reality of the companies, and contrast this reality with the motivations of those working at them.

The five VPN companies I interviewed have approximately 90,000,000 million users in around 183 countries worldwide. So, although there were a small number of interviews, the overall impact of the companies interviewed is significant. The smallest VPN company I spoke with had over 50,000 users and the largest had 50,000,000 users.

Each interview lasted an hour to an hour and a half. Three interviews were conducted via video chat, one interview was conducted in-person, and one interview was conducting over an encrypted chat line, at the request of the employee. As previously mentioned, I reached out to over 50 of the most popular VPN companies, and these were the companies that responded to my requests.

Interview questions grouped by categories:

Personal Motivation Questions:

- What is your background?
- Why did you start a VPN company?
- Were there reasons, beyond financial reasons, that you started a VPN company?
- Have you started any other companies?
- Are VPNs a passion or a job for you?
- Why is VPN technology important?
- Do you feel strongly about the capabilities of VPN technology as it relates to the current state of the Internet?

- Do you see yourself working in this sector long term?
- Are there any moments in your company’s history that have made you feel proud?
- What is the most exciting part of VPN technology for you?
- What is the most exciting part of the Internet for you?
- Are there any roadblocks you see in the future of your company?
- Are there any alternative technologies that you see promise in?
- Would you ever pivot, or redefine your company?

Practical Questions:

- Where do you have servers?
- Where do most of your users come from?
- What is the main reason they use your VPN?
- Do you keep any user data?
- Would it be possible for you to give away user data to authorities?
- Are there circumstances where you would give away user data to authorities?
- What is your VPN primarily for?
- Do you consider it better for some uses than others?
- Do you feel responsible for those who use your VPN?
- There are some VPNs that have been in the news for not doing exactly what they say they are going to do. Do you have an opinion on this?
- To you, most general, what separates a competent — or good — VPN from an incompetent — or bad — VPN?
- Where do you see the future of VPN technology headed?

- Have you ever been in a moral or legal dilemma concerning the administration of your VPN?

QUOTE STYLE

This paper focuses on the motivations, feelings, affects, and opinions of those involved in VPNs and the impact of these on the delivery of their technology. For this reason I have provided longer format quotes, so that the reader can appreciate the different personalities of each interviewee. This "personality" is something that is difficult to capture by paraphrasing, or summarizing quotes, although I have also done this where appropriate.

RESULTS AND ANALYSIS

One overriding conclusion that emerged from my interviews was that the VPN world is particularly affective. Though it is based, to a large extent, on shared values and goals (i.e. privacy and security online and a "open" or "free" internet), it is made up of people from geographically distant places, who all have their own unique interpretation as to what make for a functional VPN, and more, generally, what the internet specifically should be, as it relates to privacy and security. Moreover, each position makes up a part of the same ongoing conversation, where there are different sides, but no clear "right" or "wrong". Drawing conclusions about the competence of a VPN relies on understanding why a company makes the choices it does through consideration of its motivations. Two main themes that emerged from my interviews and help to highlight this affective nature, and which, when analyzed together, provide a partial understanding of the motivations of VPN companies are trust and values. Though the two themes sometime overlap each other, they each have distinct attributes that are worth analyzing alone. Moreover, different responses relating to each category often highlight contradictions in the very areas in which they overlap. I will argue, based on my analysis of the interview responses, that the extent of security and privacy provided by VPNs are at least partially determined by the values and motivations of the particular VPN company.

With respect to “trust,” the primary question is, how does one trust a VPN company? This question is two-fold. First, how do you trust a VPN, technologically speaking, to be functional, and second, how can you trust the ones who are maintaining and running the technology? A VPN could have the technological capacity to provide a certain level of security, but if the VPN company decides, for example, to log data or sell data, the technology becomes obsolete from a privacy and security standpoint.

Ultimately, trust, in the VPN business, is an elusive quality. VPN companies can “manufacture trust” through their marketing and using key words that people can identify with, especially in the emotionally charged space of security and privacy. For example, even though, technologically speaking, all VPN companies are supposed to be doing the same thing, i.e. providing a secure, private, Internet service, their motivations may differ. And, in turn, their users may also have different usage goals, and therefore, different thresholds upon which to base their trust when determining whether their trust in a VPN company is well founded.

And so this leads to the second theme to be discussed: values. Essentially, it’s impossible to analyze trust without analyzing the motivations of VPNs and the personal ethos from which these motivations arise. As a consequence, these will be the next focus of this paper after the discussion of trust.

Given the small number of interviews that were able to be carried out, the interviews will be used primarily to inform the issues under discussion here, supported by evidence gathered in the media, rather than providing any conclusions in of themselves. It is also important to note that the wide reach of these companies, in terms of the number of customers they have, give this sample group intrinsic value. I begin with the issue of trust.

TRUST

While conducting my interviews, the issue of trust often surfaced, often when we began to speak about the collection of user data. This led to questions like, “how can your users trust you do not keep data?” which led to the more general question, “how can your users trust you?” No company was able to give a definitive answer. As Luke from Company A told me on the issue of trust, “Trust is the perennial problem, nobody has the solution.” Karl, of Company B, echoed this idea, “the VPN provider pinky swears that, while they could find out and tell the world who you are, they will not do so.” Thomas, of Company C, also concurred, “Our customers really can only take our word for it that we don’t keep any logs, and track their information…and we really don’t. But there’s no way to know if we’re telling a lie.” Heather of Company D, said about the same thing, “This is just a matter of belief. You either trust us or you don’t. Maybe some tech savvy people can look into the code or run some tests or something, but like, just regular users just believe what other users say, what reporters say and what we say on our site.”

Philip, of Company E did acknowledge that trust is an issue, but pointed to third party audits, consumer reviews, amount of users and privacy policies as a good place for people to begin to analyze if they can, or cannot, trust their VPN company. This brings us to solutions for the trust issue. Thomas gave me the same answer as Philip,

> Well there are a lot of websites that try to run some tests and they're independent researchers that try to find leaks or issues in VPNs and security apps in general when they track this they publish the results after that users know if a particular VPN is bad or whatever.

Company A and D all alluded to similar tactics for trusting a company, though all companies acknowledged that this is not 100% sufficient.

The problem with reading the privacy policy of VPN companies is that sometimes they can be obtuse or even misleading. One example is PureVPN, one of the most popular VPN services, who VPN review site BestVPN.com found to keep many logs, included logging names, email addresses, phone numbers, IP addresses, bandwidth data and connection timestamps, despite claiming to keep "no logs" (bestvpn.com). Relying on popular opinion may be of use for users who are looking to use a VPN for certain uses (for example, if you are streaming content, the speed of the VPN will be valuable), but do not provide an educated opinion on security and privacy measures. In terms of crowd-sourced online reviews, as has been recently seen with Facebook's data-sharing scandal in spring of this year, popular opinion is not always right. In this example, millions of people used Facebook, and yet, at its peak popularity, user data was actually being compromised on a mass scale (Madrigal). According to a recent literature review, trust is a precondition for people's adoption of electronic services, and positive reviews are an initial determining factor for initiating this trust (Beldad). And as Papacharissi points out, spreads some democratic ideas, in its equalizing nature. If we apply this to the concept of mass online use, or mass-reviews, they do seem like a properly democratic mode of judgment. But as French philosopher Alexis de Tocqueville opines, “In times of equality, because of their similarity men have no faith in one another; but this same similarity gives them an almost unlimited trust in the judgment of the public; for it does not seem plausible to them that when all have the same enlightenment truth is not found on the side of the greatest number.” (409). So, although these means may help people trust a VPN, they are not fool proof.

One other alternative answer to “how do you trust your VPN company” came from Karl:

> At the start I used Company B in particular for privacy reasons. That is how I got to know the service, and I liked the concept. Then I got in contact with the staff, volunteered a bit in the project, and ended joining the staff…when it comes to anonymity in the VPN sense (one key node doing the "hiding", as opposed to the chained concept of TOR where one just gets lost in a twisty web), trust is important. Company B came from the people who ran [Internet Company X], and that is pretty much the best pedigree possible.

Here Karl implies that it is personal experience with the company, and the reputation of those behind it, that makes him prefer VPN technology — when in the right hands — to other Internet security methods (in this case, TOR), and legitimizes (or lets him trust) Company B. TOR is a different anonymizing network that passes IP address through a number of different nodes, those in charge of each node only being aware of the IP address before and after it. This makes traffic difficult to be traced back to a single computer. Unlike VPNs, TOR is not run by a single group, but rather relies on volunteer networks (Rankin). Luke, of Company A, echoed Karl's sentiment saying:

> I think the biggest defence to be completely honest, is that we have 40 people here who legitimately care about privacy and like you can tell it's all we talk about all day…

A second employee of Company A, Jack, added, "I know a bunch of people on my level who would just quit if we started logging. Like people wouldn't work here anymore."

Thomas, of Company C's, answer may appear at first like more of a shoulder shrug than an answer saying as a reason to trust, "…you know, we're like a small company; they (our users) don't really have a reason not to trust us." And as further proof went on to say, "I use it myself to download and not get caught, buy stuff off the Dark Web, so you know, it's nice…I know my boss isn't going to rat me out."

Though this may appear to be different than Luke, Jack and Karl's answers, it has some similarities. The Company C employee trusts his company because he personally trusts the person who runs it. He trusts him so much he knows he won't "rat him out"; this implies a shared set of values.

Again, it is the knowledge of the people who work at Company A and Company B and Company C, who, in the eyes of these employees, provide the biggest objective security assurance to Company A users. Of course, the users themselves, more often than not, do not have the opportunity to "know" their VPN company on this personal level.

But to what extent is trust important to users? As previously stated, some initial level of trust is necessary to attract people to a company (Beldad). But trust will inevitably mean different things to different users, as it's based on affectively derived preconditions, such as values and emotions (Beldad). For example, those looking to access Netflix, may not care if their data is being collected by the VPN company, in so long as they can trust their VPN to provide them with a strong connection to Netflix. Others, who are would like their VPN to provide privacy and security for its own sake, may have a different definition of trust, which is based on the actual technology. They will want their VPN company to take security and privacy as seriously as they do, for its own sake. In either case, if those in charge of the VPN have values that are aligned with your own, a strong of a bond of trust is possible. This brings us to the next theme to be discussed in this paper, the theme of values.

VALUES

In Isaiah Berlin's essay, "Two Concepts of Liberty" he reveals the paradox of freedom. According to Berlin, a person is never completely free, if we consider "freedom" nothing more than a lack of restraint; our own aspirations, or a society's aspirations, impose limits on our complete freedom (Two Concepts), and direct us. Berlin calls freedom, as a lack of restraint, "negative freedom". To Berlin, this type of freedom is worthless without boundaries. Boundaries, whether they are found in laws, or our own values, allow us to actually use our freedom to do what we choose to, and to pursue a meaningful life. And so, negative freedom must be balanced with "positive freedom"; the freedom to pursue "the good life" whatever that may be. Berlin has been criticized for drawing too fine a line between "positive freedom" (the restraints that direct us to pursue our values) and coercion. For the purposes of this paper, this is beside the point. The useful part of this distinction is the idea that when people use VPNs they are not simply experiencing a lack of restraint, they are also experiencing the values of the company, values which, direct the company's choices, and thus affect the user experience.

VPNs ideally provide a secure and private space, where a person is able to, ideally, do what he or she wants to do. VPNs let us, ideally, use the Internet in an unrestrained and unlimited manner. And yet, the values that VPN companies hold do have the capacity to restrain us. They set limits to our freedom, as users support a world-view that is necessarily value laden. Even in their ideal state, VPN technology cannot give us complete freedom. They come with their own values that direct us, and change our experience of the Internet.

In trusting a VPN company, we choose to promote whichever values they promote, and make ourselves vulnerable to their own ethical decisions, a decision which, as previously described, is based on affective qualities like values and emotions (Beldad). In other words, we are not just subscribing to freedom as a complete lack of boundaries; we are subscribing to an alignment of our values with those of the VPN. Trust, like freedom, is not something objective that someone, or some company, either has or does not. It is, rather, something that is dependent on the interaction between those seeking a relationship and that trust, thus requiring mutual, shared values. And yet, as VPNs continue to grow in popularity, what exactly constitutes a VPN of "value" is continuously being redefined, internally and externally as conversations from the world of internet security, customers, and amongst companies themselves, create affective boundaries, through the interplay of "emotions, affect, and feeling" that help to determine ideological standards (Papacharissi 3).

As it turns out, there are some commonalities among the values held by different VPN companies, but there are also differences. Analyzing this helps to shed light on the boundaries of the VPN world today, and how this may inform Internet security in the future.

To begin to understand "values" we can start by analyzing Company C. As previously demonstrated, Thomas trusted his company to do the right thing because he trusted his boss, who would "not rat him out". This employee of Company C described his boss as someone "super paranoid" who "smokes a lot of weed, so that doesn't help [with the paranoia]" and who has "also done some shady things in his past". He met his boss in a Parisian nightclub, and knew nothing about the VPN world. He was hired on to Company C after a short friendship. He did not know his boss' real name until a year and a half into his employment. He saw his position as purely a job, though he did find the space interesting. This company is marketed as a Canadian file-sharing focused service but whose identity will be kept anonymous. Though this may seem like a strange rationale for trusting someone, Thomas, who alludes to using the VPN for nefarious reasons, sees kinship with his boss, who seems to promote what would look to others as a morally dubious life style. From Thomas' perspective this "live and let live" life style is what gives him trust.

Thomas went on to reveal the possible security problems with the VPN, explaining that the protocols being used were now considered obsolete by Google. He admitted what was enabling them to get good reviews. They paid money to websites like TorrentFreak, to place them on Top 10 lists, which he claimed, "everyone does" (Company A, incidentally concurred with this observation, saying "It's kind of a necessary evil”). When I ask Thomas where in Canada they headquartered, the response was “That’s just a bullshit thing. We’re officially registered in America…Canada sounds better”. However, we cannot assume based on these facts that Company C was completely devoid of a moral compass. Thomas went on to outline a situation where the VPN made an ethical choice to, ultimately, go against their own privacy terms and conditions, because they felt morally compelled to do so. He described a circumstance where Canadian authorities traced an individual uploading pornography back to one of their VPNs IP addresses. His boss activated the collection of logs, which is counter to the VPN’s security policy, to catch the perpetrator. If anyone logged back on to the sites, they would be able to, hypothetically, trace them to a user account. They were never able to catch the perpetrator, who, according to Thomas, “…probably has like, you know, 20 VPN accounts or something like that, switching them back and forth…piggybacking VPN companies…if one of them is shady and keeps logs, it will connect you to another VPN company.” Ironically, in this case Thomas’ own VPN company was the “shady” VPN. I asked why they had chosen to break their own privacy rules. Thomas replied:

> Of course with the child pornography, we were like ok. We can help you in anyway possible…because it’s fucking child pornography. No — we do not condone that. Even if we’re like, “yeah free internet”, blah blah blah, it’s child pornography…freedom of speech, whatever…that’s not something we accept.

He then went on to describe situations where his employer would not help authorities:

> If they had come to us being like oh a hacker…we wouldn’t have done much to help them. It’s not the same thing…we receive thousands of DMCA notices for copyright violation; we just don’t do anything about them.

I mentioned that there was a definite moral line there for him, to which he replied, “Exactly, I’m guessing we would have been the same if they asked us about some serial killer.”

I outlined the highly publicized case where Pure VPN had been able to help authorities track down an Internet stalker, as outlined in Part 1 of this paper, which, seemed to reveal the company had been keeping data. The employee explained that this was not necessarily the case. They could set up “honeypots”, i.e. to start keeping data after the fact. In my understanding, either way, they are keeping user data. From a security perspective, whether it is being done before or after the fact does not make a difference for those whose data is being compromised.

This employee seemed to use his “common sense” morality to make justifications for the company’s decisions and state. If we look at VPNs as things that are supposed to provide security and privacy, it would seem that this VPN is something that falls short. But if we look at morality in a larger sense, summarizing this employee’s position, he recognizes that most people use the VPN to access restricted material online. For this purpose he thinks the VPN could be better, but is good enough. And he thinks that principles like “freedom of speech” and “free internet” are not as important when the issue becomes the need to assist in capturing a child predator. This employee has no grand illusions about the Internet. He’s a guy with a job; he’s a pragmatist.

When I relayed Company C’s handling of the honeypot-child-pornography story to Company A, they were visibly shocked. Luke asked if it was Pure VPN, alluding to their dubious reputation before responding with:

> It’s so sketchy, it just makes me feel better about what we do. You know, Company A would never dream about those sorts of things, like we’re… I think that comes back to my comment about us not being the moral arbitrator… like once you start down that road of choosing who deserves privacy and who doesn’t deserve privacy, you get in a really awkward position, where now you have to decide for the entire world.

Company A took a more “black and white” or idealist approach to the VPN world. For them, user data is not to be compromised under any circumstance. Luke explained to me that a VPN is simply a tool. It can do good and it can be used to do bad. But Luke believed, that in the grand scheme of things, more good was being done through their service than bad. Compromising user data, even if it was to help catch a child predator, would only serve to compromise the good their company is doing. As Luke tells me,

> Do I like that our way to prove that we don’t log things is defending people that are being, you know, blamed for, [or] suspected of committing crimes? No, but that’s the North American example where we have much more acute crime…like if you get the same request for information on someone living in Iran for just using a VPN, regardless of what they’re using it for, they’re just using a VPN, it’s often illegal in some of these countries, so these are the cases that I especially want to have the system set up, so that the same rules of law apply, so that we’re not the ones making the moral judgment...it’s not my place to choose where we are on the spectrum, it’s my place to create a tool and allow people to use it. And I

> think at the end of the day, I think the world is a lot better that it exists rather than not existing.

Unlike Thomas, the employees from Company A were passionate about their jobs, and driven by the fact that they were “doing good” in the world. Luke described this again, in more depth:

> …the big meaningful things for us are when we do things like offer free data to an entire country to get around censorship. My time since I’ve been here, I’ve done it for Turkey a couple of times, I’ve done it for Venezuela I’ve done it for Iran, a whole host of countries, and it’s just such a great feeling that you get out of it, that you’re adding back, you’re actually giving back to communities and you’re not just creating a tool in isolation that may be useful but isn’t really adding back to society in any way.

So although Luke had argued, when presented with possible nefarious uses for using a VPN (e.g. distributing child pornography) that the company had simply created a tool, and they should not be the moral arbitrator of how that tool was used, in this latter quote, he argues quite the opposite. They were not creating a tool in isolation; they were giving back to the world, by “doing good”. This was by actively giving data to countries for free, something quite outside their role as a VPN company. This reveals that security and privacy were not only being offered for their own sake (or for the sake of a “negative freedom”, or unrestrained freedom, as described by Isaiah Berlin) but for the hope that something good, in this case democratic values, would come from it. To this point, Jack, a second employee from Company A said:

> …the way I view VPNs, it's as access to information, and the way I view access to information is as a valuable tool for democracy… this is a channel that people use to explore ideas and think about things and to communicate, and to think privately which is an important part of our society.

Thomas from Company C, actually did echo this sentiment of the importance of VPNs in a non North American context, saying:

> I know journalists, for example if they are based in Egypt and they're talking shit about the government, then they want to be protected, because they if they're not connected to a VPN and start posting articles about how the government is they could find out where he is in Egypt and come get him, you know?

But when asked if he feels proud of any moments in his company's history, he gives a different answer:

> Yeah, well I guess it's kind of cool to know you're helping some people you're helping people download and…(laughs)…it's kind of cool, because I use it myself to download and not get caught, buy stuff off the Dark Web, so you know, it's nice.

Thomas was not attempting to influence the content, and thus did not take any ownership over what other people were doing. He was providing a tool, and people were using it, for good or bad. Is it possible for a company to distance itself from the bad, but claim responsibility for the good? I asked Heather of Company D if they had ever had any moral dilemmas concerning the administration of their VPN:

> I mean we are all people and we all have hesitations, but we strongly believe that we do better than worse…anything can be used for bad, if it's used by a bad person. That's why we believe we create VPNs for a good reason.

And what was this "good" reason? Heather continues,

> [Our CEO] actually decided to create a VPN because he believed the freedom of information is something worth working for…it's unfair to limit people in whatever resources he wants to visit…it was right after Snowden (i.e. right after Edward Snowden released classified information from the National Security Agency (NSA) revealing global surveillance programs)…we should develop VPNs to contribute to the free Internet.

The mention of Snowden hints at a strong belief in anti-surveillance (Osborne). Company D did, however, as outlined by bestvpn.com, keep some logs (for examples, how many people are using the VPN at one time), for reasons like providing a better customer experience. This could point to a slight discrepancy between making their product appealing to the general public and a complete adherence to non-surveillance principles. It is also important to note that Company D hails from the Ukraine, although their business is officially registered in the U.S. The Ukraine has far more government surveillance than North America, and for this reason the employees may be more sensitive to such issues. Company D believes that a lack of surveillance will lead to "good" and is a good in itself, despite the potential for "bad people" to abuse its platform.

We can see how Company C, Company A and Company D all differ. Company C takes a pragmatic approach, believing less in grandiose ideals about the Internet and more in a case-by-case moral code. Company A believes in actively helping their non-North

American users spread ideals of democracy. Company D was founded off principles of non-surveillance, and comes from a country where surveillance is rampant. Philip, of Company E, again provides a different answer:

> For me it's really important that people can experience the Internet the way it's meant to be. For example when I have friends from other countries that tell me they can't connect I just find that a little weird, so we unblock for that.

Here we see him take a pragmatic approach, much like Company C. He personally finds it "a little weird" that there are countries where the Internet cannot be joined freely; where people can't access what he can. The notion of the Internet being experienced "the way "it's meant to be" refers to its decentralized nature; where there is no single body mediating usage (Barrat & Shade, 298). He, however, does not consider this position, a position at all, but rather as a sort of "non-position":

> Non-western countries focus a lot on controlling the Internet where western countries too try to have some level of surveillance of the Internet, and I think for us as a VPN company we don't want to be an activist in the middle of these arguments and we don't want to take a political stance…as simple as an adult you have the right browse as you like and we would like to protect your privacy from advertisers, malware, trackers etc. So I personally, and this doesn't necessarily reflect the company, this is my personal opinion, for me it is extremely important because it allows a user to do what he wants on the internet and at the same time blocks advertisers from tracking him and [lets him] experience the web in a much cleaner way.

It is easy to claim to be apolitical when you are equating your VPN with doing things you consider to be good. In Philip's case, as outlined in the paragraph above, "protecting your privacy from advertisers, malware, trackers, etc." But what if someone is doing something bad? I relayed the child pornography case to him and ask what he would do. Philip replied,

> … it does come down to an ethical dilemma, but for us, who are extremely focused on making sure that we uphold our promise to our users… I don't know how to answer this because on one hand this would not be my decision, and on the other hand, I don't have previous experience to use to indicate what we would do.

By suggesting that Company E has never been dealt with this specific circumstance, so Philip is hesitant to answer either way, speaks to the moral ambiguity surrounding such decisions, which have to be dealt with on a case-by-case basis. Again, this ambiguous answer is very different from Company A's, who, was adamant about never compromising their data no matter the case.

When I ask Company B if they ever have been morally conflicted about their platform, I am a bit surprised by their answer. As described before, Company B was founded based on strong principles of privacy, and free sharing of information. TheBestVPN.com did find that it stored some user data, including email addresses. Karl says when I ask if he feels ethically responsible for what users do using their VPN:

> Kind of…there are moments when our users have misbehaved…I'm thinking harassment/spamming…(but) we might be a bit trigger happy at some points.

Karl forwards a blog article in which they were “trigger happy” in his opinion. The article describes a competitor VPN company that “tricked” Company B into booting a user off their platform for spreading right wing/racist propaganda, that had in fact been planted by the competitor, in an apparent attempt to smear Company B, accusing them of not being “neutral” as a VPN company “should be”. Company B responded that they received screenshots of the fake-perpetrator’s aggressions, and the behavior clearly went against their terms and conditions. As stated in Company B’s response:

> The ToS clearly states that we will not protect users spreading right wing material. The author of the aforementioned article states that in his personal opinion a VPN service should be neutral. We see this differently. If a user spreads right wing propaganda then he/she/it is on the wrong side of history. We are not going to tolerate that our work is used to further the agenda of people who think that:

- Just because your skin has a different color,
- You have a different religion,
- You have a different sexuality,
- Or a disability

Here, Company B draws a strict line as to what would cause them to compromise user data; bigoted behaviour. Karl admits that it is hard to know exactly where the moral line between acceptable and non-acceptable behavior lies, and when action should be taken, but says that a VPN should not provide users with a “free for all” when it comes to their Internet use.

CONCLUSION

As has been described in this paper, VPNs as a technology are ultimately dependent on the choices that the humans who create and maintain them. That is why I have spent time highlighting some key points in conversations with those who work at VPN companies as they reflected the theme of trust, and their own personal values throughout the course of this study. Ultimately, the attitudes of the VPN providers interviewed shine a light on the limits of VPN technology as it exists in the world, and the level of security it provides. VPNs function in a way that is affective, so to say, the principles they function according to are not based on industry norms, but affectively derived and highly personal values. Even in a small sample size there is much variance and disagreement on what the limits of “security” and “freedom” are, and where these concepts should be tapered in place of other values (for example, stopping cybercrime, like child pornography). It is clear that there is no playbook on making principled or ethical decisions surrounding the administration of a VPN. Although all the companies interviewed said that they stand for privacy and security, the definition of these terms actually blurred in practice. Two of the five companies, Company C and Company B, were upfront about where their adherence to the pure concepts of privacy and security stopped. In Company C’s case, it was child pornography, and in Company B’s case it was racism. They both admitted, however, that it was difficult to know when to step in on these issues and each, ultimately, applied a case-by-case approach to taking any action.

Company A, on the other hand, affirmed that there was no circumstance under which they would compromise their principles. The way they saw it, any such compromises would undermine all the “good” their VPN did. Company D and E, although not as explicitly, suggested a similar conclusion. The “good” their VPNs provided was worth any “bad” behaviours.

The definition of “good” also differed from company to company, ranging from helping bypass government censorship to protecting people from nosey ISPs, to keeping the Internet “open the way it was meant to be”. This begs the question, “does consciously and actively applying boundaries on freedom and privacy by VPNs really take away from the ‘good’ they do?” Can a VPN company help journalists in Uganda exercise principles of democracy and also help Canadian authorities track down child predators? Are these two things really mutually exclusive?

On the flip side of this question lies a paradox. Refraining from giving away customer logs at any cost is a choice that is not “neutral”, but political. For example, working to keep the Internet “open” is a choice, and assuming the Internet is “meant to be” a certain way is an opinion. In Company A’s case, giving free Internet access to those looking to spread “democratic principles” is reflective of a very particular worldview that is quite apart from “security” and “privacy”, even if these principles do, at points, overlap with democratic principles. My point is that even companies who claim to never compromise principles of security or privacy, do in fact, and still make ethical decisions, that compromise other widely held ethical beliefs. These compromises arise the moment concepts like “privacy” and “security” are applied within a dynamic world. Their application in the world requires decisions to be made that change them from positive ideals to affectively derived interpretation of ideals. This shows how particularly affective VPN companies are, with a lack of formalized regulations and standards.

I would argue that in so far as VPN companies are simply providing a free and secure space, they are not doing good or bad. They are simply providing a tool for individuals to use the Internet as they see fit, whether this be to circumvent copyright or protest the government. It is these individuals who inject that space with content, which can be both “good” and “bad”, and must affectively feel their way into a space that aligns with their own world view as a standard for “trust” in an unregulated environment.

Some VPN companies confuse Berlin’s two concepts of freedom. They equate the freedom they provide, freedom in the negative sense, with democratic principles. Though negative freedom may be a democratic principle, this freedom alone, does not necessarily imply democracy. Democracy entails a series of values and sentiments that go beyond a simple lack of boundaries, for example the values of equality and the purposeful separation of church and state. As Papacharissi explains, the Internet pluralizes but does not necessarily democratize a space.

As an example, the employees of Company A found pride in the “good” uses that came from their VPN, for example, family members reuniting in countries that were politically volatile. They felt justified in running their company, as they found it “important for democracy”. But in so far as a VPN company does nothing more than provide a free space, are they really doing something “good” or “bad”? If it is the users who take action through the VPN, how responsible is a company for these actions? Moreover, can their service simply be a neutral “tool” when someone uses it for “bad” purposes, for example for “acute crimes” in North America, but a “democratic service” when someone uses it for “good”?

Another example may shed more light on this question. In 2014, during the "Egyptian Revolution" Facebook CEO Mark Zuckerberg at first distanced himself from taking any credit for the actions of Egyptians during protests. But, at a shareholder meeting, he claimed that Facebook was indeed a vehicle for democracy, and that was his main purpose. As the revolution went awry (an equally repressive regime took power), he again rejected ownership over any actions resulting from the use of Facebook, and went back to saying Facebook was nothing more than a tool. In this case, in the situation of VPN users, the Internet pluralizes but does not necessarily democratize. So having technology companies that facilitate spaces for negative freedom, then claiming ownership over the democratic elements that emerge from that space seems like a tenuous connection to make on their part. Company A, however, does actively promote democracy in ways that are apart from their existence as a VPN provider. For example, they have on occasion, provided free, secure Internet access to protesters who were fighting for democracy.

Although the company believes they are acting ethically through the creation of a space for negative freedom, they are not necessarily promoting positive values like democracy. This is demonstrated by the fact that because they don't want to undermine their ethical position of a free internet, they do refuse to do anything that could curb it, for example helping authorities track down a child predator. But doing this would simply be curbing a negative freedom, helping track down a child predator. It would not impede on the notion of "democracy" because it is not at odds with it. It is simply at odds with a complete negative freedom. Democracy is a value that the company holds that is quite apart from the complete freedom provided by their VPN.

The above example is raised because it helps reveal the potential ethical problems or paradoxes VPN companies can be confronted with, particularly if they misunderstand their stance to be a "neutral" democracy and fail to acknowledge the political dimension of their choices (Laclau and Mouffe 96).

On the Internet, remaining neutral is not an option. As Chantal Mouffe says, each choice made ultimately exposes your beliefs, as a choice favours one option over another. I would suggest that VPN companies not shy away from making policies grounded in their own ethics, and that they should remain open about them. It is only through this that consumers can properly align themselves with a company that matches their own needs and values; thus fostering trust.

So, where does this lead us in terms of the issue and theme of trust? As admitted by the majority of VPN companies interviewed, trust is a concept that cannot be fully resolved satisfactorily. Trust is a two-way street, which relies on a mutual understanding that both parties share the same values. Trust depends on a user's own values and purposes for using a VPN. As Papacharissi says, on the Internet, we affectively feel our way into communities that we relate too. Choosing a VPN is much the same. Allegiance and trust is based on affective feelings, not only on concrete evidence, which is often difficult to find.

Papacharissi says that, "what reason, belief, and ideology suggest, affect, feeling, and emotion frequently overturn in favor of the irrational" (3). Yet the rational and the irrational remain in extractible from one another, and it is only hypothetically that we are able to divide them. Even through interviewing five companies, who work in the niche area of VPNs, we are able to see interpretations that lead to different applications of policy, though all companies claim to be abiding by the same principles; security and privacy. Through one lens, these discrepancies could be seen as an immaturity and recklessness within the industry (Leyden). Through another lens, the precarious, affective nature of the technology could be an example of the nature of the Internet on a larger scale; a pluralized space through which people feel their way.

Works Cited

Abbate, Janet. *Inventing the Internet.* MIT Press, 1999.

Andy. Hola VPN Sells Users' Bandwidth, Founder Confirms." *TorrentFreak,* 28 May 2015, torrentfreak.com/hola-vpn-sells-users-bandwidth-150528/. Accessed 4 Dec. 2017.

Barrat N., Shade L. R. "Net Neutrality: Telecom Policy and the Public Interest." Canadian Journal of Communication, 2007 pp. 295-305.

Bazley, Tarek. "Iran internet plan ignites debate." *Al Jazeera,* 29 Sept 2012,www.aljazeera.com/indepth/features/2012/09/2012927132545740255.html . Accessed 4 Nov. 2017.

Beldad, Ardion et al. "How shall I trust the faceless and the intangible? A literature review on antecedents of online trust." *Source Information,* vol. 26, no. 5, 2010 Sept. pp. 857-869. Accessed 19 Aug. 2018.

Buckle, Chase. "Turkey Leads for VPN Usage." *GlobalWebIndex,* Chart of the Day, 10 Jan. 2017, www.vpnmentor.com/reviews/btguard-vpn/. Accessed 04 Jan. 2018.

Chen, Caleb. "Thousands march in Moscow, Russia to support Internet Freedom, protest VPN ban." *Privacy News Online,* 24 July, 2017, www.privateinternetaccess.com/blog/2017/07/thousands-march-moscow-russia-support-internet-freedom-protest-vpn-ban/. Accessed 25 Oct. 2017.

Company A Interview. Personal interview. 15 April 2018.

Company B Interview. Personal interview. 02 May 2018.

Company C Interview. Personal interview. 06 April 2018.

Company D Interview. Personal interview. 09 March 2018.

Company E Interview. Personal interview. 02 June 2018.

"Complaint, Request for Investigation, Injunction, and Other Relief in the Matter of AnchorFree, Inc. Hotspot Shield VPN" Submitted by *The Center for Democracy & Technology (CDT),* 1 Aug. 2017, www.documentcloud.org/documents/3911863-FTC-Complaint-on-VPNs.html. Accessed 29 Dec. 2017.

Dawson, Dave. "Determining and integrating the best applications for VPNs." *Computer Technology Review,* vol. 17, no. 9, 1997, pp. 10-12.

Eddy, Max. “The Best VPN Services of 2018.” *PC Mag,* 6 Aug. 2018, www.pcmag.com/article2/0,2817,2403388,00.asp. Accessed 6 Aug. 2018.

Evans, Pete. “Bell Media president says using VPNs to skirt copyright rules is stealing.” *CBC,* 5 Jun. 2015, www.cbc.ca/news/business/bell-media-president-says-using-vpns-to-skirt-copyright-rules-is-stealing-1.3099972.

“Federal Decree-Law no. (5) of 2012” On Combating Cybercrimes. *Khalifa Bin Zayed Al Nahyan.* ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf

Foucault, Michel. *Discipline and Punish: The Birth of the Prison.* New York, Random House, 1977.

Fullagar, David. “Evolving Proxy Detection as a Global Service.” *Netflix Media Center,* 14 Jan. 2016, media.netflix.com/en/company-blog/evolving-proxy-detection-as-a-global-service.

Galletta, Anne. *Mastering the Semi-Structured Interview and Beyond*. New York University Press, 2001.

Gregg, Melissa and Gregory Seigworth. *The Affect Theory Reader.* London, Duke University Press, 2010.

“Gurdeep Singh Pall.” *Crunchbase*, People, www.crunchbase.com/person/gurdeep-singh-pall. Accessed 04 Jan. 2018.

“GWI Social: GlobalWebIndex’s Quarterly Report on the Latest Trends in Social Networking.” *GlobalWebIndex*, Flagship Report Q1, 2017, cdn2.hubspot.net/hubfs/304927/Downloads/GWI-Social-Summary-Q1-2017.pd

Habermas, Jurgen. “The concept of human dignity and the realistic utopia of human rights.” *Philosophical Dimensions of Human Rights,* Springer, 2012, pp. 63-79

Haraty, Ramzi and Bassam Zantout. “The TOR data communication system.” *Journal of Communications and Networks,* vol. 16, no. 4, 2014. ieeexplore-ieee-org.ezproxy.lib.ryerson.ca/document/6896565/citations. Accessed 18 Aug. 2018.

Hawke, Robinson. “Malware FAQ: Microsoft PPTP VPN.” *Sans*, www.sans.org/security-resources/malwarefaq/pptp-vpn. Accessed 3 Dec. 2017.

Ikram, Muhammad, et al. *An Analysis of the Privacy and Security Risks Android VPN Permission-enabled Apps.* Internet Measurement Conference, 2016, www.icir.org/vern/papers/vpn-apps-imc16.pdf

KennWhite[Kenn White]. “Most VPNs are Terrible” *GitHubGist,* 20 Jul. 2017, gist.github.com/kennwhite/1f3bc4d889b02b35d8aa. Accessed 25 Oct. 2017.

Khazan, Olga. “Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says” *The Atlantic,* 6 June 2013, www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/. Accessed 7 Aug. 2018.

Jackson, Allan. “Coalition asks CRTC to block websites with pirated content in a bid to fight illegal streaming.” *The Financial Post.* 29 Jan. 2018. business.financialpost.com/telecom/coalition-asks-crtc-to-block-websites-with-pirated-content-in-bid-to-fight-illegal-streaming. Accessed 19 Aug. 2018.

LaBorde, Doug. “Understanding and implementing effective VPNs.” *Computer Technology Review,* vol. 18, no. 2, 1998, pp. 12-16.

Laclau, Ernesto and Chantal Mouffe. *Hegemony and the Social Strategist Towards a Radical Democratic Politics.* Verso, 1985.

Leyden, John. “90% of SSL VPNs are ‘hopelessly insecure’, say researchers.” *The Register,* 26 Jul. 2016, www.theregister.co.uk/2016/02/26/ssl_vpns_survey/. Accessed 15 Jul. 2018.

Longworth, James. “VPN: from an obscure network to a widespread solution.” *Computer Fraud & Security.* vol. 2018, no. 4, doi.org/10.1016/S1361-3723(18)30034-4. Accessed 20 Aug. 2018.

MacKinnon, Rebecca. *Consent of the Networked: The World-Wide Struggle for Internet Freedom.* Basic Books, 2012.

Madden, Mary and Lee Rainie. “Americans’ Attitudes Abou Privacy, Security and Surveillance.” *Pew Research Center,* 20 May 2015, www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Madrigal, Alexis C. “What we know about Facebook’s latest data scandal.” *The Atlantic,* 04 Jun. 2018. https://www.theatlantic.com/technology/archive/2018/06/what-we-know-about-facebooks-latest-data-scandal/561992/. Accessed 20 Jul. 2018.

Meeta, Gupta. *Building a Virtual Private Network.* NIIT, 2003.

“Microsoft Leads Initiatives for Virtual Private Networks Across the Internet.” *Microsoft,* 4 March 1996, news.microsoft.com/1996/03/04/microsoft-leads-initiative-for-virtual-private-networks-across-the-internet/. Accessed 1 Nov. 2017.

“How VPN Works.” *Microsoft TechNet,* technet.microsoft.com/pt-pt/library/cc779919(v=ws.10).aspx#w2k3tr_vpn_how_niuh. Accessed 20 Aug. 2018.

Moczulski, J.P. “Protests in Iran lead to a surge in downloads of Canadian VPN tools.” *The Globe and Mail,* www.theglobeandmail.com/report-on-business/small-business/going-global/protests-in-iran-lead-to-a-surge-in-downloads-of-canadian-vpn-tools/article37599480/. Accessed 12 May 2018.

Mohta, Pushpendra “VPNs bring interactivity to electronic commerce.” *HP Chronicle,* vol. 15, no. 7, 1998.

Mouffe, Chantal. *Agnostics; Thinking the World Politically*. Verso, 2013.

Mouffe, Chantal. Interview by Pluralt. *Studies in Political Economy*, Spring 1996, spe.library.utoronto.ca/index.php/spe/article/view/9368. Accessed 24 Oct. 2017.

Mouffe, Chantal. *The Return of the Political.* Verso, 1993.

“Multiple Critical Vulnerabilities in Hola Overlay Network Client*.” Hola Security Advisory.* adios-hola.org/advisory.txt. Accessed 20 Dec. 2017.

Nave, Kathryn. “Infoporn: how VPN use varies by country.” *Wired*, 1 Jul. 2016, www.wired.co.uk/article/vpn-use-worldwide-privacy-censorship. Accessed 04 Dec. 2017

Nie, Weiliang. “Chinese learn to leap the ‘Great Firewall’.” *BBC,* 19 March 2010, news.bbc.co.uk/2/hi/technology/8575476.stm. Accessed 4 Nov. 2017

Osbourne, Charlie. “Snowden wants to build anti-surveillance tech*.” CNET*. 21 Jul. 2014. https://www.cnet.com/news/snowden-to-build-anti-surveillance-tech/. Accessed 15 Jul. 2018.

Papacharissi, Zizi. *Affective Publics: Sentiment, Technology, and Politics.* Oxford University Press, 2015.

Paul, Ian. “VPNs have a Trust Issue: Here’s What TunnelBear did About it.” *PC World.* 8 Aug. 2018. www.pcworld.com/article/3213032/security/vpns-have-a-trust-issue-heres-what-tunnelbear-did-about-it.html. Accessed 7 Jul. 2018.

Rankin, Kyle. *Linux Hardening in Hostile Networks: Server Security From TLS to Tor.* Boston, Addison-Wesley, 2018.

Reed, Alan, et al. “Forensic Analysis of Epic Privacy Browser on Windows Operating Systems.” *European Conference on Cyber Warfare and Security,* Jun. 2017, 341-350.

Rosen, Rebecca J. "The Fight for a Fair and Free Internet". *The Atlantic*, 14 Feb. 2012.

"Russia: VPN ban is a major blow to Internet freedom." *Amnesty International,* 31 July 2017, www.amnesty.org/en/latest/news/2017/07/russia-vpn-ban-is-a-major-blow-to-internet-freedom/. Accessed 25 Oct. 2017.

"Secure Internet servers (per 1 million people)." *World Bank,* 2016, data.worldbank.org/indicator/IT.NET.SECR.P6, Accessed 07 Jan. 2017.

Silverman, Laura. "Turning to VPNs for Online Privacy Might be Putting your Data at Risk." *All Tech Considered,* NPR, www.npr.org/sections/alltechconsidered/2017/08/17/543716811/turning-to-vpns-for-online-privacy-you-might-be-putting-your-data-at-risk. Accessed 04 Dec. 2017.

Steinberg, Steve G. "Hype List." *Wired,* 2 June 1998, www.wired.com/1998/02/hype-list-25/. Accessed 4 Nov. 2017.

"Syria." *Freedom on the Net 2017,* 2017, *Freedom House.* freedomhouse.org/report/freedom-net/2017/syria. Accessed 4 Dec. 2017

"The Truth About VPNs." *Techdirt* from Techdirt, 4 April 2017, www.techdirt.com/blog/podcast/.

"TunnelBear Completes Industry-First Consumer VPN Public Security Audit." *TunnelBear,* tunnelbear.com/blog/tunnelbear_public_security_audit/. Accessed 04 Dec. 2017.

"Turkish people turn to VPNs as Istanbul protests spread." *BBC,* 6 June 2013, www.bbc.com/news/technology-22799768. Accessed 4 Nov. 2017

United States of America v. Ryan S. Lin. No. 17-MJ-4251-DHH. United States District Court. 2017, https://www.justice.gov/opa/press-release/file/1001841/download.

Upfal, Eli. "Are Free VPN Services As Safe As Paid VPN?" *YouTube,* uploaded by Failed Normal Redux, 13 Apr. 2016, www.youtube.com/watch?v=vDbPjgXstHg

"Virtual Private Network (VPN) Market Analysis by Type, Deployment, Products, End User | VPN Market Worth US $41.702 Billion by 2023 at 18% CAGR." *MarketWatch,* 12 June 2018. www.marketwatch.com/press-release/virtual-private-network-vpn-market-analysis-by-type-deployment-products-end-user-vpn-market-worth-us-41702-billion-by-2023-at-18-cagr-2018-06-12. Accessed 6 Aug. 2018.

Vectra Threat Labs. "Technical analysis of Hola." *Vectra,* 1 Jun. 2015, blog.vectra.ai/blog/technical-analysis-of-hola. Accessed 4 Dec. 2017.

Young, Katie. “1 in 5 are weekly VPN users.” 18 Aug. 2016, blog.globalwebindex.net/chart-of-the-day/1-in-5-are-weekly-vpn-users/.

Young, Katie. “4 things to know about VPN users.” 2 Feb. 2016, blog.globalwebindex.net/chart-of-the-day/4-things-to-know-about-vpn-users/

“What is a VPN? And why you should use a VPN on public Wi-Fi.” *Norton*, Security Center, us.norton.com/internetsecurity-privacy-what-is-a-vpn.html7890-.

Whittaker, Zack. “Why Hotspot Shield’s co-founder puts privacy over profits.” *ZD Net*, 12 Jan. 2016. www.zdnet.com/article/why-hotspot-shield-co-founder-puts-privacy-over-profits/.

Winckworth, Kate. “Tinker, Torrentor, Streamer, Spy: VPN Privacy Alert” *CSIROscope,* 25 Jan. 2017, blog.csiro.au/tinker-torrentor-streamer-spy-vpn-privacy-alert/. Accessed 25 Oct. 2017.