

Policy strategies for VPN for consumers in the Netherlands



Master's thesis of Nelly Ghaoui, MSc s0301345 for the Executive Master Cyber Security

Cyber Security Academy

First supervisor: dr. B. van den Berg (Leiden University)

Second supervisor: prof. dr. ir. J. van den Berg (TU Delft)

December 22, 2016



Index

Acknowledgements.....	3
Abstract.....	4
1 Introduction	5

Part One

2 Methodology and research design	10
3 Literature review and theoretical framework	15

Part Two

4 VPN: the benefits and disadvantages	23
5 Stakeholder analysis	27
6 Analysis: why is smartphone VPN for consumers currently not a standard service in the Netherlands?.....	32

Part Three

7 Industry self-regulation.....	36
8 Co-regulation	41
9 Legislation	43

Part Four

10 Conclusions and reflection.....	47
11 Policy recommendations	49

References	52
------------------	----

Interviews.....	56
-----------------	----

Appendix 1: Comparison of costs of mobile subscriptions in the Netherlands.....	57
---	----

Appendix 2: Search for information on VPN on sites telecom providers	61
--	----

Appendix 3: overview of empirical research through interviews.....	65
--	----

Acknowledgements

I would like to thank my employer for the opportunity to follow this executive master's program. The Cyber Security Academy has broadened my horizon on cybersecurity and the challenges we collectively face to secure our digital lives. I have enjoyed pioneering this program together with both the lecturers and staff of the Cyber Security Academy and I am proud to be part of the first class. I would also like to thank my fellow students. I have enjoyed our many lively discussions inside and outside of the classroom. I have learned much from your wide areas of expertise, your different perspectives and from your experience working in different parts of our field. Following this program with cybersecurity professionals has already enabled some of us to find each other in our daily work. For me, this program is as much a success because of my fellow students as it is because of the dedication and expertise of the lecturers and staff of the Cyber Security Academy. As I finish this two-year master's program, the academy welcomes its third class of students. I wish the Cyber Security Academy much success in the years to come and I hope that future students enjoy following this program as much as I have.

Abstract

Using a Virtual Private Network (VPN) has cybersecurity and privacy benefits for consumers, especially when using public wifi. However, not many consumers in the Netherlands use VPN on their smartphones even though it is a simple protective measure. This thesis explores the feasibility of possible policy strategies of the Dutch government if it decides that smartphone VPN for consumers should become a standard service within the mobile subscriptions of telecom providers. Based on interviews with stakeholders from government, business and civil society, the question is answered which of the policy strategies of industry self-regulation, co-regulation and legislation is feasible for the Dutch government to implement.

1 Introduction

Being online on the go has become a normal part of our daily lives. Our smartphones are always close at hand for reading the news, chatting with family and friends, shopping online or meeting our next partner in life. Such a blossoming mobile digital life and economy also mean that consumers have to deal with cybersecurity risks. In the Netherlands, most consumers are unaware of those risks. Empirical studies show that the level of cybersecurity awareness of Dutch consumers is low even though they regularly fall victim to cybercrime (Motivaction, 2012; Gfk, 2013; Gfk, 2014; Gfk, 2015; TNS NIPO, 2016). Eleven percent of Dutch consumers was the victim of cybercrime in 2015, which is more than double the percentage of consumers that fall victim to bicycle theft (four percent) (Statistics Netherlands and Ministry of Security and Justice, 2016). A part of the National Cyber Security Strategy is the personal responsibility of consumers for their cybersecurity, comparable to the responsibility of locking their own front door (Ministry of Security and Justice, 2013). On the other hand empirical studies show that currently consumers lack the knowledge and interest to take cybersecurity measures of their own accord (Gfk, 2014: 21). Also, economic research has shown that the market for digital goods is a market for lemons, meaning that customers cannot distinguish between digital products in the market in terms of quality. They are therefore not willing to pay a premium for higher quality (i.e. cyber secure) products (Andersen and Moore, 2006). Improving the cybersecurity awareness of consumers is beneficial, but I argue that additional measures are needed to improve their digital security. By analogy, I do not know or understand all the technical safety and security measures incorporated in my car to be able drive, but there is a complex system of expert car manufacturers and government agencies ensuring that cars are safe and secure.

In the digital world the strength of passwords is a classic issue for consumer awareness-raising. Between 2012 and 2015 the amount of consumers that use a symbol in their password has increased from 48 percent to 81 percent despite the fact that the studies conclude that consumers are generally passive when it comes to taking cybersecurity measures (Motivaction 2012: 49; Gfk, 2015: 40). At the same time many websites have introduced mandatory password strength for accounts and are moving to two-factor authentication (Gfk, 2014: 10; National Cyber Security Center, 2015a: 56). Also following the public disclosure of data breaches, companies actively contact customers to change their passwords. Recent examples are LinkedIn that contacted customers this year that hadn't changed their password after a data breach of the platform in 2012 (Tweakers, 2016b) and Yahoo that advised customers to change their passwords after a data breach of 500 million accounts (Yahoo, 2016).

These examples show that consumers can be activated to take cybersecurity measures if they are nudged in the right direction. Techno-regulation, changing human behavior through the technological design, can be an effective method (Lessig, 2006). An important question with techno-regulation is who regulates according to which values? This question is especially relevant for cybersecurity issues. This is because cybersecurity, similar to environmental issues, suffers from the problem of moral hazard (Andersen and Moore, 2006). The negative consequences of failing cybersecurity are not borne by the party that needs to take cybersecurity measures. If personal data is stolen due to a software leak, the consumer can fall victim to identity fraud or scams, not the software developer. This leads to companies externalizing cybersecurity risks to unaware consumers. In economic terms this would be a sound economic decision for companies, because investing in extra cybersecurity measures would not be rewarded by customers

in the marketplace. Data breach notification legislation is influencing the situation dynamic by bringing in an element of public disclosure (i.e. reputation damage) for companies.

In sum, this dynamic makes cybersecurity a collective good. In the interaction between consumers and businesses the market will provide a certain amount of cybersecurity to customers. But I argue that it will not provide a level of cybersecurity comparable to the level of physical security and safety in society. The main difference between physical security and cybersecurity is the role of the state. Where the government primarily provides physical safety and security, in the digital world cybersecurity has to be organized differently simply due to the private ownership of most digital infrastructure and services. And since our digital lives are almost completely interwoven with our physical ones I argue that there is a societal need to build a comparable level of cybersecurity which is higher than the market would currently provide on its own. The government plays a central role in achieving a higher societal level of cybersecurity. If it cannot play its traditional role of providing safety and security itself, it needs to focus on influencing the other players in the game. Within this dynamic the question rises which topics to focus on and what strategies to use.

With this societal perspective of cybersecurity in mind, this thesis explores the possibilities that techno-regulation offers the Dutch government to increase the cybersecurity of consumers. Comparable to the analogy of cars, if digital products and services can be made technically more secure for consumers 'out of the box' or 'under the hood' then they would be less likely to become the victim of cybercrime. There are examples of cybersecurity techno-regulation in the market. For instance, through the various versions of Windows since 2012, Microsoft has incorporated a standard antivirus program in its software called Windows Defender (Microsoft, 2016). The antivirus program is active by default and if a user installs a third-party antivirus program of their choice, the antivirus program is de-activated automatically. This ensures that Windows users always have an active antivirus program, even if they do not make an active effort themselves. This form of techno-regulation by Microsoft is relevant to the cybersecurity of consumers, since antivirus programs are their most popular cybersecurity measure (Gfk, 2014: 13, 60).

The example of Microsoft is one of a market player taking cybersecurity measures that benefit consumers. But what if the Dutch government wants to take action on a particular cybersecurity measure through techno-regulation? Since the government cannot provide all cybersecurity measures to consumers itself¹ a valid option is to influence the behavior of important intermediaries with a local presence such as telecom providers/internet service providers, banks and insurance companies (Goldsmith and Wu, 2006: 159). To achieve a form of techno-regulation in the market, the government can apply various policy strategies, such as industry self-regulation or legislation. Within this governance framework I perform a case study on a technical solution that enhances the cybersecurity and privacy of consumers, namely a *Virtual Private Network* or VPN for smartphones. The use of VPN is customary in business settings to provide remote access to the corporate network. For consumers using VPN would mitigate cybersecurity risks they face when using public networks also known as open, public or free wifi. The use of public wifi is popular amongst consumers because they don't use any of their paid mobile data (within the Netherlands and especially while travelling abroad). The use of wifi also alleviates the pressure on mobile

¹ This is also due to competition legislation prohibiting the government from providing services that the market can provide (*Wet Markt en Overheid*) (Rijksoverheid, 2016).

networks of telecom providers. A number of telecom providers offer access to wifi spots as an added service to customers. Examples are Ziggo wifispots, KPN Wifi and KPN FON (Ziggo, 2016; KPN, 2016a; KPN, 2016b). Moreover, the European Union launched an initiative this fall to promote the establishment of free wifi in public spaces in order to increase connectivity in all member states called WIFI4EU (European Commission, 2016). The initiative has an initial fund of 120 million euros.

To make connectivity as easy as possible these public networks often have no security measures or are poorly secured, which makes users vulnerable to data interception. Using a VPN would mitigate that risk because it encrypts the data connection. A number of expert authorities advise consumers to use VPN. Among them are the Dutch National Cyber Security Center (NCSC) and Europol (NCSC 2015a; Security.nl, 2014). The problem is VPN is not widely used by consumers (Gfk, 2015: 40; Security.nl, 2016). The main challenge is therefore, how to change the situation from a government perspective? This leads to the following research question: *Assuming that the Dutch government decides that all consumers in the Netherlands should have VPN on their smartphones, what would be a feasible government strategy to make this a reality?*

The research question is answered by analyzing the feasibility of three policy strategies in the case of smartphone VPN for consumers. These three strategies are industry self-regulation, co-regulation and legislation. The focus of the research question in this thesis, aiming for VPN becoming a standard service for all consumers in the Netherlands is a significant break with the current status quo. Ultimately, the choice whether or not the Dutch government would pursue smartphone VPN for consumers as a standard service is the outcome of a political process. Despite that fact the reason for choosing a hypothetical scenario is to research the possibilities and challenges of the government when it comes to policy implementation.

The reason for choosing to focus on the policy implementation of a technical cybersecurity solution is because there are a number of technical cybersecurity solutions are not widely implemented.² Researching the policy tools a government has at its disposal to change the status quo offers broader lessons in case the Dutch government would choose a strategy of techno-regulation on other issues. Compared to other cybersecurity issues, smartphone VPN for consumers is a delineated technology with a clear form of implementation. This makes it a good case to research the consequences and impact of possible policy strategies.

Another reason for choosing VPN is because it is a relatively simple technology to use for consumers. Current commercial VPN-software offers the possibility to choose a server location and to turn the connection on or off. Secondly, it is a visible measure for consumers instead of an invisible technical security measure, which also gives them a measure of self-control. When using VPN, consumers are not dependent on the security arrangements of others such as open wifi providers.

² A few examples are: DMARC/DKIM/SPF for email authentication to combat phishing emails, DNSSEC which adds a security layer to the 'address book' of the internet, IPv6 which is less a security but more a connectivity measure since IPv4 - addresses have run out a number of years ago. Transport Layer Security (TLS) is an encryption standard for websites that use customer accounts such as webshops, but it is not used by all websites. A number of encryption algorithms such as SHA-1 and SHA-2, DES and triple DES that have been cracked (some of them decades ago) but are still widely used.

Structure of the thesis

This thesis consists of four parts. Part one contains the methodology and research design (chapter two) and the literature review and theoretical framework for assessing the feasibility of the three policy strategies (chapter three). Part two consist of an analysis of the current status quo of smartphone VPN for consumers in the Netherlands. Chapter four focuses on the technology of VPN and discusses its benefits and disadvantages. Chapter five contains a stakeholder analysis. Chapter six analyzes why in the current situation, VPN is not a standard service for consumers and argues that there are possibilities are to change the status quo in the overriding interest of improving the cybersecurity of consumers. Part three focuses on the hypothetical scenario – smartphone VPN as a standard service for consumers- and possible policy strategies for implementation. It analyzes the feasibility of the three possible policy strategies of industry self-regulation (chapter seven), co-regulation (chapter eight) and legislation (chapter nine). Part four concludes with reflections and conclusions answering the research question which policy strategy is feasible to implement smartphone VPN for consumers (chapter ten). This is followed by policy recommendations (chapter eleven) on the next steps the Dutch government could take on this topic should it choose to do so.

Part One

Methodology and research design

Literature review and theoretical framework

2 Methodology and research design

This chapter contains the research methodology, the scope of the research and the operationalization of the case study of smartphone VPN for consumers.

2.1 Research methodology

This thesis is an exploratory case study on applying a form of cybersecurity techno-regulation in the Netherlands through public policy, namely smartphone VPN for consumers. The research question is based on a hypothetical scenario and the research focuses on which government strategy is feasible to get from the current situation to the hypothetical scenario. Desk research and eleven semi-structured interviews with stakeholders are used to assess the policy implementation challenges.

In this thesis the literature is used to explain the status quo and to build the framework of possible policy solutions. The interviews with stakeholders are used to assess the feasibility of policy strategies based on the theoretical policy framework. A number of theoretical approaches are used. The economic perspective on cybersecurity, specifically the work of Andersen and Moore (2006) is used to explain the current status quo. The four modalities of regulation by Lessig (2006) introduce the concept of techno-regulation as a method of changing human behavior. In this case, pursuing policy strategies to make smartphone VPN for consumers is strategy of techno-regulation. Goldsmith and Wu (2012) show that intermediaries with a local presence can be an effective target for government policy. Lodge and Wechrich (2012) are a guide to the three policy strategies of industry self-regulation, co-regulation and legislation. A number of public policy models are used to build the theoretical framework to assess the feasibility of the three policy strategies (Ballegooij et al, 2004; Bovens et al, 2001; Brugha and Varvasovszky, 2000; Lodge and Wegrich, 2012).

Parts two and three contain the empirical research. The following research methods were applied. The chapter on VPN is based on desk research. An interview with a technical expert from the NCSC corroborated the findings from the desk research and offered additional input into the technical aspects of VPN.

The analysis why VPN is not a standard service in the Netherlands is based on desk research and validated through interviews with the stakeholders listed below. Information on the cybersecurity (awareness) of consumer use of VPN is primarily based on annual quantitative studies of research bureaus into the cybersecurity awareness of consumers between 2012 and 2016. These studies were conducted for the annual national cybersecurity awareness campaign Alert Online (Motivaction, 2012; Gfk, 2013; Gfk, 2014; Gfk, 2015; TNS NIPO, 2016). These empirical studies vary to some extent in research questions and focus on specific topics from year to year, but they give an overview of the cybersecurity awareness of consumers. Their outcomes are statistically significant, making them a valid source of information on the awareness, knowledge and behavior of consumers on cybersecurity issues. In 2015 and 2016 VPN was included in the study ensuring that observations can also be made on VPN for consumers. The description of the mobile telecom providers for consumers is based on available market information. Some detailed (paid) industry reports were unavailable for this research. For the government agencies, policy documents

were consulted such as the Digital Agenda and the National Cyber Security Strategy 2 (Ministry of Economic Affairs, 2013; Ministry of Security and Justice, 2013).

A market analysis of VPN-providers is based on an overview that is actively maintained online by one person in the technical community called 'That One Privacy Guy' (That One Privacy Guy, 2016). Civil society organization Bits of Freedom also links to this source for information on VPN-providers (Bits of Freedom, 2016). This list is also mentioned in an article analyzing the difficulty of making a 'top-10'- list of VPN-providers on professional technology news site Ars Technica (Ars Technica, 2016). Even though this is information from only one source, the source is transparent about the criteria it uses and two credible sources in the technical community cite it. Another reason for choosing to use this one source over a large number of specialized VPN-comparison websites is because these websites seem unreliable. The VPN-comparison websites often do not state who operates the website (Vpnpick.com, 2016; Vpncomparison.org, 2016). Some state that the comparison is subjective (Top10vpn.com, 2016). Articles of Ars Technica and Bits of Freedom confirm that these websites are not transparent, possibly unreliable or even sponsored by providers (Ars Technica, 2016; Bits of Freedom, 2016). Therefore I chose to prefer the transparent information of a single person in the community who is committed enough to the topic to keep a list of around 170 VPN-providers with 44 comparison criteria in nine categories up to date.

The desk research also identified a number of additional market initiatives on VPN for consumers. Information on the initiatives of Google and Opera are included based on the desk research (Opera, 2016; Androidworld, 2016). Since the initiative of Surfnet called Let's Connect is a Dutch initiative an interview was carried out with Surfnet for more information on the project (interview November 2, 2016).

Part three of this thesis goes into the three possible policy strategies. The three strategies are based on the theoretical work of Lodge and Wegrich (2012). The feasibility of the possible policy strategies is assessed through interviews with stakeholders. The stakeholders represent the relevant actors on this topic from a policy perspective. From the Dutch government the following parties were interviewed: the ministry of Economic Affairs/Directorate Telecom Market, Ministry of Security and Justice/Directorate Cyber Security and the telecom oversight agency ACM (*Autoriteit Consument en Markt*). From the telecom providers I chose to focus on the three largest mobile consumer telecom providers, namely KPN, Vodafone and T-Mobile. T-Mobile and Vodafone were not interested to participate. Two interviews were conducted with representatives of KPN, one with a focus on the technical feasibility of a smartphone VPN-service for consumers and one with a business focus going into elements of the business case for a telecom provider. Next to individual telecom providers, the two trade associations in the cybersecurity field, Nederland ICT and VNO-NCW, were interviewed. Interviewing both individual businesses and trade associations is beneficial because of the difference in perspective. The representatives of a telecom provider offers insight into the considerations of an individual business. Trade associations have a broader market perspective and they also have experience with interacting with the government on policy issues. The third group of interviews covered a civil society perspective. ECP and Bits of Freedom were interviewed. Civil society organizations offer an additional perspective as compared to government agencies and private businesses in the sense that they have a broader societal perspective. For an overview of the empirical research conducted through the interviews, see appendix 3.

Lastly, no VPN-providers were interviewed. The focus of the research is on telecom providers providing the VPN-service because they have an existing relationship with consumers. In providing the service, a

telecom provider can choose to either develop and run the VPN-service themselves or enter into an agreement with an existing VPN-provider. In either option, the telecom provider is the focus of the policy strategy and more relevant to interview than a VPN-provider.

2.2 Scope of the research

The research question assumes that the Dutch government has already decided to act on the topic of smartphone VPN for consumers. This leaves issues of agenda-setting out of scope of the research. Furthermore, the research is scoped on Dutch consumers and the Dutch market as opposed to for instance European consumers. Even though the Netherlands is part of the European single market, the policy strategies to address the issue of smartphone VPN for consumers within the governance structures of the EU are different from policy strategies for the Dutch market. Focusing on the Netherlands also identifies the room the Dutch government has for national strategies within the context of a global internet and a European single market.

The business application of VPN, a common practice for remote access to a company network, is out of scope as an object of research. This is because the focus of the research is on how to improve the cybersecurity consumers in their private lives. Even though consumers are also employees, the employer provides mobile devices or remote access and is responsible for cybersecurity measures. In their private lives, consumers are responsible for their own digital devices and cybersecurity. Lessons learned from VPN for businesses that can apply to smartphone VPN for consumers are taken into consideration.

When it comes to technical aspects of VPN, the research only distinguishes between encrypted and unencrypted connections, i.e. secured or unsecured connections. Discussions on the merits or problems of different encryption algorithms that could be used by various VPN-providers is left out of scope. This is because the research question focuses on choosing a feasible policy strategy to implement smartphone VPN for consumers through telecom providers. The strength of encryption algorithms within a possible VPN-service is not relevant in this context. Such an issue becomes relevant when a telecom provider designs its service.

Lastly, the research focuses on VPN as a solution for smartphones that can be used on any wifi connection. This places open wifi providers and proprietary wifi spots provided by some of the telecom providers (such as Ziggo and KPN) out of scope.

2.3 Operationalization of the case study

The research question consist of a number of elements regarding the hypothetical scenario that need further operationalization. The research question is: *Assuming that the Dutch government decides that all consumers in the Netherlands should have VPN on their smartphones, what would be a feasible government strategy to make this a reality?*

Firstly, the hypothetical scenario is scoped on smartphones as opposed to all devices with wireless internet connectivity which would also include tablets, laptops, pc's, e-readers, gaming consoles, any and all Internet of Things (IoT)-devices etc. Smartphones are the predominant online mobile device of consumers while travelling and most likely to use open wifi. 'Dumb phones' are left out of scope, because

they generally don't have wireless internet connectivity and if they do, they do not have the same ease of online use for browsing and apps. The chances of these consumers using open wifi are small. Also, focusing on smartphones scopes the number of intermediaries to nationally rooted actors, such as telecom providers. This makes the number of actors more manageable for research and implementation. When it comes to smartphone manufacturers, smartphones support VPN-connections as a technical feature just as they support wifi or mobile data. Also, they are generally multinational businesses making it more difficult for the Dutch government to influence than nationally rooted actors such as telecom providers.

Another element of the hypothetical scenario is that *all consumers* have VPN on their smartphones. The operationalization is that VPN is a standard service for all consumers as a part of their mobile subscriptions. This means that when a consumer agrees to a mobile subscription, VPN is part of the package. This does not mean that the VPN-service is necessarily free of charge. A telecom provider can choose to raise the price of their subscription or to find another way of earn back the necessary investment of the VPN-service.

This operationalization means that the VPN-service would be a software-based or a so-called 'over the top service' with at least a VPN end-point in the Netherlands. This as opposed to a VPN implementation through home routers (see chapter four). A VPN-services through a home router assumes that a consumer with a mobile subscription also has a home subscription with the same provider. Not all telecom providers in the Netherlands also offer home internet services. An over the top service ensures that all telecom providers have the ability to implement the smartphone VPN-service for consumers. Over the top services are defined as the opposite of managed services within the network of an operator. They are application services that are available online (Telecompaper, 2013: 4). Examples of over the top services are Whatsapp, Spotify and Netflix. These services increase the demand for faster internet connectivity. They also offer some over the top services themselves or in conjunction with the application provider. Examples are Spotify and video apps such as HBO Go and *Eredivisie Live* (Telecompaper, 2013: 53-54). As mentioned above, a telecom provider can choose to develop and offer the VPN-service themselves or enter into an agreement with an existing VPN-provider. This thesis makes no further operationalization on this aspect.

Having a VPN end-point in the Netherlands ensures the possibility of lawful interception by Dutch law enforcement and compliance with Dutch copyright law. Whether a telecom provider chooses to also offer end-points in other countries is not specified further. Theoretically the service could be engineered to detect the location of the device and connect to a server in that country. Such a solution would also ensure compliance with copyright law while travelling abroad. Such an issue becomes relevant when the telecom provider designs its service.

A last element of the case study is whether or not a consumer can control the VPN connection e.g. whether they can activate and deactivate the VPN connection. The assumption is that the VPN-service in the hypothetical scenario is comparable to VPN-services as currently offered in the market. A commercial VPN-service can be activated and deactivated by the user. When using 3G and 4G a VPN connection is not a necessary security measure because mobile internet is encrypted to the cell tower by default. Therefore a permanent VPN-connection is not needed. Technically a VPN-service could be configured to detect whether or not a user is connected to wifi and whether or not the wifi connection is an open connection. These kinds of features are a standard feature of connection management in Windows software. By analogy, such a feature theoretically could be incorporated in a VPN-service in the future.

The main issue is that this thesis does not assume that a VPN-connection as part of a mobile subscription is always active and that the consumer has no control over the connection. The hypothetical proposal is that consumers get a VPN-service within their mobile subscription by default. This makes the VPN-service a combination of techno-regulation (the VPN-service is incorporated in the subscription by default) and a nudge (the VPN-connection be activated and deactivated manually). Leaving consumers the choice to also deactivate the VPN-connection raises the issue of adoption rate by consumers. If consumers do not like using VPN they could choose to ignore it completely. This would mean the desired policy goal, ensuring the cybersecurity of consumers while using open wifi, is not reached. On the other hand, the relative cybersecurity of 3G and 4G does not justify proposing a VPN-connection that is always active. Also, consumer choice is an important value for government to uphold. At the same time the assumption is that if the proposed hypothetical scenario would become a real-life scenario, telecom providers would try to enhance the user-friendliness of the VPN-service, thus boosting adoption rate by consumers. Options could be through design choices such as detecting wifi-connections as mentioned above, through the design of user-friendly apps or other creative means.

To summarize the hypothetical scenario, when a Dutch consumer agrees to a mobile subscription for their smartphone a VPN-service is included in the package. The VPN-service at least has an end-point in the Netherlands and can be manually activated and deactivated by the consumer. The next chapter is the theoretical core of the thesis in which amongst others a framework is constructed to assess the feasibility of the possible government strategies.

3 Literature review and theoretical framework

This chapter consists of a number of elements. The literature review goes into previous research on VPN, regulation of human behavior and policy strategies for internet-related issues. The theoretical framework describes the three possible policy strategies that are applied to the case of smartphone VPN for consumers. Also a model is constructed to assess the feasibility of the three policy strategies.

3.1 Literature review on VPN

Previous research conducted on VPN is generally technical in nature on how to design VPN in a business context. At the end of the 1990s VPN was considered new technology and work focused on implementation issues for applications of remote access (Scott, Wolfe and Erwin, 1999) or for online transactions in E-commerce (Oosthuizen, 1998). More recent research focuses on developments in the VPN-technology (Berger, 2006) and on the implementation of VPN in new ICT environments such as within cloud services (Fahad, Gaspar-Modelo, Saurabh, 2012). No previous research was found regarding VPN for consumers from either a technical or policy perspective. From a legal or policy perspective previous research focuses on the impact technology has on human behavior and how it can influence behavior. The work of Lawrence Lessig is taken as a starting point.

3.2 Regulating human behavior

In the field of law and IT, the four modalities of regulation as described by Lessig (2006: 123-125) have become a standard framework. He argues that there are four modalities that regulate human behavior at any given time in the physical world and also in cyberspace. These modalities are the law, the market, social norms and architecture. In formal laws the state describes which behavior is not allowed, such as murdering someone or tax fraud. The state also enforces these codes and therefore shapes the behavior of citizens. Laws are made based on the democratic process of parliamentary approval. This gives laws a legitimate base to regulate the behavior of citizens.

The market of supply, demand and pricing regulate the choices people make about which goods to buy or not. If a product is cheap, such as an apple, then many people can and probably will buy it. If a product is expensive, such as a yacht, not everyone can afford to buy the good even if they wanted to. In a perfect market each product finds an equilibrium between supply and demand. This creates issues when it comes to collective goods. Due to its collective nature and the possibility of free-riding, a collective good, such as security, would not be ensured for all citizens in a market situation.

Another issue with the regulating force of the market is that a market situation in which supply, demand and pricing happen perfectly, often does not exist. Authors such as Andersen and Moore (2006) have argued that market imperfections are applicable to cybersecurity. An example is information asymmetries can occur between supplier and consumer, similar to the 'market for lemons'. This would mean that consumers cannot distinguish between a cyber secure product and a cyber insecure product (Andersen and Moore, 2006: 612). Therefore, there is little incentive for a supplier to incorporate cybersecurity in their services. If cybersecurity measures offer no return on investment in terms of competitive advantage on quality, then no significant investment will be made by businesses. A significant number of customers

must demand cyber secure products before a business is inclined to invest in cybersecurity (Van Eeten and Bauer, 2013: 459-460).

Another market mechanism applicable to the digital economy is that of network economics. This is the idea that economic activity tends towards a small number of large enterprises. (Van Eeten and Bauer, 2013: 467; Mayer-Schonberger, 2008: 721). Everyone is on Facebook because everyone else is on Facebook. From the supplier side, this market mechanism is a strong incentive to win the race for market share and achieve customer lock-in from the moment of product launch. This mechanism creates a disincentive for suppliers to implement security-by-design, because it delays the time to market. It also slows the pace of innovation of a platform for third-party developers because they have to comply with security requirements. Andersen and Moore argue that suppliers will choose to have little security measures in place while building their market position and may add security features when market dominance is achieved (Andersen and Moore, 2007: 7). From a consumer perspective, the network economics of the digital market make changing digital products more difficult. Moving away would not only give technical problems such as interoperability. When it comes to social media, it would also give social problems for the consumer to move to another service because they would miss out on social interactions with others.

The third modality of regulating human behavior is through social norms. Which social norms to follow varies per country, culture and historical age. These norms are enforced through social control. (Lessig, 2006: 122). In extreme cases, deviating from the social norm can lead to social exclusion, a severe punishment for the inherently social human being. This means that in the earlier example of a dominant platform such as Facebook, the network economics incentive for a consumer is to stay with the dominant platform in the marketplace and the social incentive is to stay with the dominant platform because leaving would lead to a form of social exclusion. If a platform such as Facebook has little incentive to build in security measures, then the chances of cybersecurity measures emerging are small.

The fourth modality of regulation is that of architecture. In the physical world the architecture of a place regulates what people can and cannot do (Lessig, 2006: 123). A wide entrance to a building lets many people enter at once, a narrow entrance forces people to enter one by one. Lessig argues that in cyberspace the computer code is the architecture that regulates behavior (Lessig, 2006: 124). In a software program, the included features determine what a user can and cannot do. More fundamentally, the internet is a man-made space and its code is based on the values of its builders. Code, or the design of technology, can be changed to reflect different values. Lessig illustrates this point by citing how the Internet access was organized at the University of Chicago and Harvard at its introduction on campus in the mid-90s. In Chicago anyone could connect to the Internet. At Harvard only approved users were allowed access (Lessig, 2006: 34). The idea that rules of behavior are coded into the design has come to be known as techno-regulation (Brownsword, 2005: 3). Users have no choice but to comply with the design, they cannot choose to deviate from the rule. An often cited example of techno-regulation in the physical world is a speed bump. Drivers cannot ignore the speed bump or risk damaging their car. A speed bump constrains human behavior more than a traffic sign, making it an effective method of enforcement of the rule (Lessig, 2006: 128). When it comes to techno-regulation in cyberspace, the values incorporated in techno-regulation are not always apparent for the user (Leenes, 2011). Also *whose* values, that of an individual programmer or a government regulator, are being enforced is often unclear. Moreover, whether or not the techno-regulation is a legitimate constraint (as opposed to classical regulation through law) is also not always guaranteed. Despite all these issues, the main issue legal scholars have with techno-

regulation is that it removes the ability of people to *choose* their behavior. They cannot choose not to comply with the rule. This freedom of choice, including non-compliance, is an important value for government regulators when it comes to regulation through law (Brownsword, 2005: 4).

Next to techno-regulation another less stringent perspective on how to influence human behavior has become popular based in behavioral economics. This is concept of nudging. Thaler and Sunstein introduced the term as a method of influencing people's choices by creating positive default options for their 'health, wealth and happiness' (Thaler and Sunstein, 2008: 6). What is deemed a good choice depends on the actor designing so-called choice architectures. This could be a school director designing the layout of a school cafeteria to promote healthier eating or a government painting white stripes in road bends to influence drivers to reduce their speed (Yeung, 2012: 123). Thaler and Sunstein term the perspective 'libertarian paternalism' (Thaler and Sunstein, 2008: 5-6). The perspective is paternalistic because someone else tries to influence the choice of people according to a certain set of values. Thaler and Sunstein argue that a form of paternalism is justified when it comes to making people 'live longer, healthier and better' (Thaler and Sunstein, 2008: 6). They argue the perspective is libertarian because people can choose not to go with the default option. At the same time, knowing that people make choices based on bounded rationality, the assumption is that many people will go with the default option that the choice architect proposes. This notion makes nudging a potentially effective method of designing policy. The difference between techno-regulation and nudging is that with techno-regulation there is no option for the user but to comply. With nudging, the user can choose a different option than the default. Nudging has a similar issue as with techno-regulation, namely the legitimacy of the actor design the default option for people's choices and based on which values the default option is designed. A main point of criticism on nudging is that it that it comes down to manipulation. Yeung analyzes that the critique on nudging 'can be understood as largely ideological objections to policy pragmatism' (Yeung, 2012: 146). As opposed to techno-regulation, which is considered a form of shaping human behavior based on legal norms (if carried out by the government), nudging is seen as a way to influence behavior based social norms (Van den Berg and Leenes, 2013).

Both concepts are relevant to the case study on smartphone VPN for consumers. In the case study the object is to prevent people from being unprotected on public wifi. By analogy the influence in behavior is similar to promoting consumers to eat an apple instead of a hamburger. The acting party in this case is the government nudging consumers in the interest of their cybersecurity. To implement the choice architecture of smartphone VPN for consumers, the government needs a techno-regulation policy strategy.

3.3 Who to target with a policy strategy?

In the 1990s people thought that due to globalization and the borderless internet that nation states would become obsolete. National governments had no way of controlling the internet and its contents. Since then this idea has proven untrue and national governments have reasserted their position over the internet in their territory (Goldsmith and Wu, 2006:VII-VIII). An example is the case of Yahoo and the

French government at the beginning of the century where Yahoo was held to French law which prohibits trading Nazi memorabilia in France (Goldsmith and Wu, 2006: 1-10). Through this and other examples Goldsmith and Wu show that the internet has become more of a bordered internet. National governments assert some form of national control over the internet. They argue that this has some virtues. Countries have their own historically anchored culture and social norms and a responsibility to protect their citizens from harm. These social norms are reflected in the legitimate legal norms of a country. Also, locally tailored content, for instance Yahoo or Google showing the Dutch news in the Dutch language as opposed to the American news in English offer commercial possibilities for the Dutch market (Goldsmith and Wu, 2006: VIII). At the same time digital service providers need a stable basis of national legal norms to flourish, for instance when it comes to having and upholding contract law in civil courts (Goldsmith and Wu, 2006: 132-139).

Taking into account that policy action of a national government in the borderless digital world is possible and can be beneficial, the question rises how a government can achieve its policy goals. When designing a policy strategy for smartphone VPN for consumers, a central choice is who to target with the policy. Goldsmith and Wu firstly offer that the government strives for measures that are adequately effective as opposed to completely effective. A certain margin is accepted because complete enforcement of a certain standard is too costly (Goldsmith and Wu, 2006: 67). This cost is not only the economic cost of enforcement, but also societal costs such as the infringement of certain freedoms of citizens to achieve a hundred percent compliance. Government strategies are about raising the bar. To achieve its goal effectively, the government can target intermediaries with a local presence (Goldsmith and Wu, 2006: 159). The source of a particular problem can be diffuse and international in nature. Targeting the whole population to change their behavior is also diffuse. So targeting an intermediary with a local presence can be effective and efficient policy strategy because they have a key position, they fall under the jurisdiction of a national government and the number of intermediaries a government needs to engage is limited. In the digital world internet service providers (ISPs) are important intermediaries that have national networks. Many ISPs have developed from traditional telecom providers. Other types of intermediaries Goldsmith and Wu identify are information intermediaries (content providers or search engines such as Google), financial intermediaries (banks and credit card companies) and Domain name registrars that could take down websites (Goldsmith and Wu, 2006: 74-77). For the case of ensuring smartphone VPN as a service for consumers, telecom providers are the best intermediary to focus a policy strategy on because VPN can be linked to the connectivity service that telecom providers already provide to customers through mobile subscriptions. Financial intermediaries are not likely candidates because they already encrypt the connection between users and online banking services. Domain name registrars are not applicable to this case study because it is not related to illegal content on websites. Having established telecom providers as the focus of a policy strategy, the next step is to identify the possible policy strategies and a theoretical framework to assess the feasibility of the different strategies.

3.3 Theoretical framework: three policy strategies

In order to achieve the policy goal that consumers have smartphone VPN-service by default, the government can pursue three possible policy strategies. These strategies are industry self-regulation, co-regulation and legislation (Lodge and Wegrich, 2012). Industry self-regulation encompasses that the market actors organize themselves to address an issue. The method of addressing an issue is left to the

discretion of the market players. In some cases enforcement of the industry norm is also organized in the market. An example would be a system of certification. The role of government in industry self-regulation can vary. The government can be agenda-setting on a topic that market players should address and then leave the design and implementation of the solution to the market. In cases where self-regulation lead to industry-wide norms, the government can play a role in the enforcement of an industry-wide norm (Lodge and Wegrich, 2012: 104-105). In this case study, the role of the government in industry self-regulation is understood as agenda-setting on the topic of smartphone VPN for consumers. The design and implementation of the solution is carried out by telecom providers. The second possible policy strategy is co-regulation. Co-regulation is a blended policy strategy where the government requires the market players to reach a policy goal in a manner suitable to them, but that if the goal is not met the government can pursue the more far-reaching strategy of legislation. This is the so-called 'shadow of hierarchy' (Lodge and Wegrich, 2012: 105-106). In the case of VPN for consumers the government would not only be agenda-setting but also monitor the progress of market implementation. If the implementation rate in the market is not sufficient then the government would be willing to pursue the third policy strategy of legislation. Legislation is the most classic policy strategy of government. In this strategy the government creates a law mandating a certain standard of behavior and compliance is enforced through sanctions by government oversight agencies (Lodge and Wegrich, 2012: 96). Legislation has the benefit of setting the same standard for everyone in a country. At the same time legislation has such a number of disadvantages and limitations that legislation is seen as an 'option of last resort' (Lodge and Wegrich, 2012: 99). Lodge and Wegrich sum up a number of the downsides to legislation. Deciding on a norm in legislation has the possibility of over- and under-inclusion of topics and targeted groups of the legislation. Legislation is an inflexible measure. It takes a long time to make and change legislation. This means that when the standard is set it is not easily changed. This leads to a practice of general norms in formal legislation, making the standard to comply with unclear for the regulated parties. Also, legislation incentivizes the behavior of minimum compliance. Furthermore they also formulate problems of potential overzealous or uninformed enforcement, bureaucratic costs and coordination problems when regulatory authority is spread across different parties (Lodge and Wegrich, 2012: 97). In this case study, a legislation strategy would be to create a law mandating that a VPN-service is included in mobile subscriptions.

3.4 Theoretical framework: assessing the feasibility of the policy strategies

To assess the feasibility of the different policy strategies, a theoretical framework of six criteria is constructed. Each policy strategy has its advantages and disadvantages and using the same criteria for each strategy makes it possible to compare them. A number of public policy models was consulted for the criteria of the theoretical framework. Existing models were not completely suited for assessing the feasibility of policy strategies. Procedural criteria such as transparency and accountability become relevant after a particular policy strategy is chosen and is designed in more detail. Also a criterion such as subsidiarity is not applicable for the framework, because there is no issue in this case study on whether or not a lower level of government than the Dutch national government should take action. Telecom providers are nationally organized businesses, so government policy at a national level is warranted. The subsidiarity principle is commonly used for assessing European versus national policy-making (Neelen et al, 2003: 220). But as stated in the research design, this thesis focusses on the Netherlands as opposed to European policy-making.

Some of the criteria from the various models are relevant for assessing the feasibility of the policy strategies. Therefore this thesis constructs its own theoretical framework based on previous research.

The principles of good government (*algemene beginselen van behoorlijk bestuur*) focus on fair and astute decision-making by government in relation to citizens and businesses in cases such as tax returns, building permits, social benefits and so forth. The principles of good government prescribe that government decisions should be accurate, sufficiently motivated and forbid arbitrary judgement (Ballegooij et al, 2004: 87-94). 'Better regulation'-programs such as the UK 'Better Regulation Task Force' propose principles that are to some extent similar. Their five principles are proportionality, accountability, consistency, transparency and regulation being targeted (Lodge and Wegrich, 2012: 54). The proportionality principle, which is a classic principle, and therefore part of both frameworks is relevant for choosing a policy strategy for smartphone VPN for consumers. The severity of the government intervention should reflect the severity of the problem it is trying to solve. The criterion that policy should be targeted or reach its goal while minimizing side effects is also relevant for choosing from the spectrum of policy strategies. Successful policy raises the bar (Bovens et al, 2001: 24, 115). For this reason the criteria of 'proportionality' and 'reaching the policy goal' are incorporated in the theoretical framework. Another factor to consider in the framework is the impact a policy strategy has on the level playing field in the market. Since the policy strategy targets market players, the effect on the ability for businesses to compete in the marketplace needs to be taken into consideration. This is more of a rule-based perspective on a level playing field than an outcome-based perspective which focuses on all businesses having the same expected profit (CPB, 2003: 7, 83). The fourth factor to take into consideration when assessing the feasibility of policy strategies is the level of support for that particular strategy by the various stakeholders. Policy-making does not take place in the classic top-down hierarchy of government to regulated parties. Stakeholders have the ability to influence decision-making in a positive sense through support and in a negative sense through delay and opposition (Brugha and Varvasovszky, 2000). If a policy strategy is suited to reach the intended goal but has no support for the stakeholders, then that strategy has a small chance of success. A fifth criterion taken into account is the amount of time the policy strategies takes to achieve the intended goal. As stated above, the large amount of time needed for legislation is seen as a downside of that government strategy (Lodge and Wegrich, 2012: 97). Other strategies are implicitly considered to take less time. Since the potential strategies differ on the amount of time it takes to come to fruition, it could be a factor in choosing a strategy. The last criterion for the theoretical framework is an assessment of the distribution of the costs and benefits of that strategy. Which party benefits and which party pays the bill (business, government or consumers) may vary between the strategies. A quantitative cost-benefit analysis of the business case of VPN for consumers on their smartphones, or a regulatory impact assessment (Lodge and Wegrich, 2012: 201-203) was not possible due to unavailability of quantitative data from a government and business perspective. Therefore the cost-benefit criterion focuses on a qualitative assessment of the distribution of the costs and benefits of the different policy strategies. Furthermore the business case of VPN for consumers of their smartphones is constructed based on the elements of a business case and their relative importance to a telecom provider.

To summarize, the criteria for assessing the feasibility of the policy strategies of industry self-regulation, co-regulation and legislation are as follows:

1. Proportionality of the policy strategy
2. To what extent the strategy reaches the intended outcome of VPN being a standard service for all consumers on their smartphones
3. The impact the strategy has on the level playing field in the market
4. The level of support of stakeholders for the strategy
5. The amount of time the strategy takes to reach the desired outcome
6. The distribution of costs and benefits

The assessment of the policy strategies based on the theoretical framework is carried out in part three of this thesis which focuses on the hypothetical scenario that the Dutch government has decided that smartphone VPN should become a standard service needs to choose which policy strategy to achieve its goal. Before that, an evaluation is needed of the current situation of VPN for consumers in the Netherlands. This is the focus of part two. The next chapter goes into the technology of VPN. This is followed by a stakeholder analysis, an explanation why in the current situation smartphone VPN is not a standard service for consumers on their smartphones and a discussion on how the status quo can be changed.

Part Two

VPN: the benefits and disadvantages

Stakeholder analysis

Analysis: why is smartphone VPN for consumers currently not a standard service in the Netherlands?

4 VPN: the benefits and disadvantages

This chapter goes into the technical details of VPN with a discussion of the benefits and disadvantages and how consumers can currently get a VPN-service.

4.1 How VPN works

VPN, or a *Virtual Private Network*, is an encryption tool. Figure 1 below shows how VPN works graphically in the case of using public wifi in a coffee shop. Within a network or internet connection, a private network is created that leads to the VPN-server. In other words, a tunnel is created between your device and the third-party VPN-provider (all blue (dotted) lines from 'our laptop' to the tunnel endpoint). All internet traffic from your device goes through that tunnel first before it goes onto the broader internet. The traffic from your device to the VPN-server is encrypted. The traffic from the VPN-server to a website (the upper red line from the tunnel endpoint to the website) is handled through the existing security measures of the specific website. For instance, if you are checking the news (an unencrypted connection which is the red line in the figure) or logging into an online banking environment (encrypted connection), your online traffic will follow the security measures of that website. The privacy feature that VPN adds to the last part of the connection is that the origin of the traffic visiting a website seems to be from the IP-address of the VPN-server instead of your IP-address (NCSC, 2015; Pcworld.com, 2013).

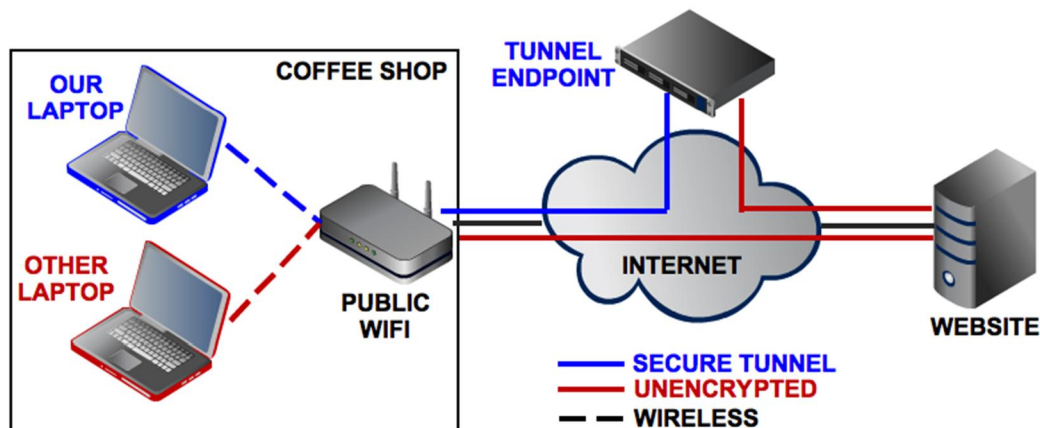


Figure 1: graphic overview how VPN functions versus no VPN-connection in case of using public wifi (Pcworld.com, 2013)

This means that the main benefits of VPN are increased online privacy and protection against data theft through so-called man in the middle attacks. VPN protects the confidentiality of a consumers' internet traffic through encryption, which can contain private data such as login credentials for email or other personal messages. If data is intercepted while using VPN, an attacker would only see encrypted data, which is useless to him. Without a VPN connection, a successful attack would see practically every key stroke of a user (KRO Brandpunt, 2014).

An extra layer of online data protection is useful in any situation at home, while travelling or at work. The added value of VPN for security is specifically relevant when consumers are travelling and using poorly secured public wifi like in a coffee shop, train or hotel abroad. These public wifi networks often have little

or no security measures to ensure maximum accessibility to customers. This means that an attacker has a number of options for malicious actions. If the public wifi does not use encryption, all data can be intercepted and read. A more advanced attack form would be that the attacker sets up his device as an intermediary point for all traffic in the network (ARP-spoofing). This attack method also gives the attacker the possibility to manipulate traffic giving him more possibilities to intercept personal data (interview, May 25, 2016). Furthermore, some public wifi points inject advertisements to customers while surfing as a method of financing the wifi point (ibid). Hijacking advertising networks to spread malware without the public wifi owner noticing (malvertising) is a common phenomenon and an added security risk to consumers using a public network (NCSC, 2016: 8).

Another situation, closely related to public wifi, in which VPN would protect the data of consumers is in cases where malicious actors set up rogue access points. Rogue access points are fake public networks that an attacker sets up in order to intercept all the data of non-suspecting people. The feasibility of such an attack method is illustrated hands-on by an ethical hacker in *KRO Brandpunt* (2014). The ethical hacker shows that with some technical knowledge and a minimal investment for the necessary equipment such an attack can be carried out with a large amount of user data as revenue.

KRO Brandpunt also illustrates the lack of awareness of the insecurity of public wifi by consumers. The same experiment was conducted in other countries such as England and Spain (F-Secure, 2014; Avast, 2016). Even though these experiments were been conducted by ICT-vendors to promote their products, the amount of users that connected to the rogue access points and the amount of (personal) data that the researchers intercepted show that unsecured surfing on public wifi or rogue access points is a relevant cybersecurity issue for consumers.

The most recent example cited, the experiment of Avast in February 2016, was targeted at attendees of the Mobile World Congress. In four hours, the researchers intercepted data of over two thousand consumers. Apart from tracking the online activity of the users, the researchers were also able to establish the identity of 63, 5 percent of the users (Avast, 2016). Combined with intercepted data such as login credentials to an email account, an attacker would have all the information they need to commit online identity fraud. If users would have used a VPN connection, the researchers would only have seen encrypted data which is useless to them. The example of the experiment of Avast at the Mobile World Congress is especially illustrative of the extent of the lack of awareness of consumers. One can assume that the attendees of the Mobile World Congress, a worldwide mobile industry event, are either professionally involved in mobile technology or have an above-average interest in the field compared to average consumers. If such a large amount of technology-interested consumers are unprotected, then one can assume that a larger group of the average consumer is unprotected while using public wifi.

A third reason why people currently use VPN worldwide is because it offers the possibility to circumvent online content that is (geo)blocked. Countries filter and block content for political, social or security reasons (Deibert, 2009). In the Netherlands the filtering and blocking of content is not an issue as it is in some other countries. Moreover, the operationalization of the case study consists of an end-point in the Netherlands ensuring compliance of Dutch law. This aspect is left out of scope of the rest of the research.

4.2 What VPN does not do

Firstly, VPN is not the silver bullet of protective cybersecurity measures for consumers. Using VPN does not fully anonymize the users' internet traffic. At the tunnel endpoint the traffic of the user can be seen by the provider. This is no different from any other ICT intermediary that could see the content of internet traffic of their users if they would want to. Under the European E-commerce directive, the liability of intermediaries is laid down when it comes to content (directive 2000/31/EC) (European Union, 2016). Within this legal framework, intermediaries are liable if they are aware of the content that passes through their systems. They are not liable if they only provide internet access. This is an incentive against intermediaries checking the content of data. In sum, there is a chance that a VPN-provider sees the internet traffic of a user, but I argue that this does not outweigh the security and privacy benefits for a consumer of using VPN. In the end, the issue comes down to whether or not a consumer trusts a VPN-provider or not. In this case study the telecom provider is the VPN-intermediary that a consumer would need to trust. I argue that since telecom providers have an existing relationships with the customers, they are an inherently trustworthy party for consumers.

Another aspect is the implications of using VPN for legitimately intercepting user data by law enforcement and intelligence services. Even though internet data is encrypted in the VPN-tunnel and the source location is masked for a website, it is possible for government services to intercept the traffic at the VPN endpoint (in the middle of the connection) or through interception techniques between the tunnel endpoint and a particular website (interview, May 25, 2016). This means that stimulating the use of VPN by consumers would not interfere with law enforcement or intelligence services.

Using VPN as a consumer does not completely guarantee that no data is 'leaked' on an unencrypted connection. A smartphone performs a large amount of online activity in the background that a user does not notice, for instance syncing its digital clock or weather information and also automatically syncing email. When a device connects to any (open) network, the device will start transmitting data automatically which happens quicker than a user can manually establish a VPN-connection. Configuring a smartphone so that it does not transmit any data before a VPN-connection is established is outside of the scope of consumer VPN-services. Such a feature is currently only seen in a business implementation of VPN (interview May 25, 2016). This means that some data will always be leaked by a consumer before the VPN is established. Usually the data that is leaked consists of the geolocation of a device and which services are active such as Gmail or Whatsapp. Again here, a consumer is dependent on the security measures that the individual service has in place. So in case of Gmail or Whatsapp, an attacker would see that the consumer uses these services, but they cannot access the content due to the encryption measures that these services use. But if a service does not use encryption, the data could be read by an outsider. This does not completely counteract the benefits of VPN, though. The cyber activity a consumer chooses to do after establishing a secured connection does benefit from the added privacy and security benefits. This is especially true when the cyber activity becomes increasingly personal, such as online dating (interview May 25, 2016).

The main disadvantage of using VPN is that it negatively effects a user's internet speed because all data makes a 'pit stop' at the VPN-provider going back and forth between a user and a website (Jager, 2016). How much internet speed is affected depends on the available bandwidth of the connection the consumer is on and the distance that the data has to travel between device, VPN-server and website (interview May 25, 2016). The type of VPN-service also plays a role. I argue that if the use of VPN becomes a standard for consumers, telecom providers and online service providers will adjust their bandwidths and protocols to accommodate the consumer. Also not all online services are compatible with using a VPN-connection. For instance, some services have implemented anti-fraud measures that are activated when a user connects through a VPN-connection. A CAPTCHA-script is activated to verify the connection is not malicious (interview May 25, 2016; interview October 19, 2016). These types of measures interfere with the user-friendliness of VPN. I argue that if VPN would become a standard service then online services would adapt over time to improve their compatibility with VPN.

4.3 How to get VPN as a consumer

As a consumer, there are two ways of setting up a VPN service. The first is to get the service/software from a third-party VPN-provider. For instance, some internationally known antivirus vendors also offer a paid VPN-service. There are also free VPN-services available where a user makes an account. The situation can be seen as similar to antivirus software. There are free and paid services. Free providers offer a basic service or could have advertisement. A paid service has more features and is probably faster. Usually a free version is used as a stepping stone to a paid version (interview, May 25, 2016).

The second way to set up VPN is through a home network. In this case the home router functions as the VPN tunnel endpoint before a user goes onto the internet. This option is unfeasible at the moment for the average consumer however. Firstly, the home routers would need to support such a feature and not many do so at the moment. Secondly, a consumer would need to manually configure the home VPN connection on both the router and all the necessary devices. This would be too complicated for an average consumer. Thirdly, if the connection is configured, a consumer needs to have a high-speed internet connection at home to make the connection useful. This is because the maximum upload speed of the home connection is the maximum download speed of the VPN-connection. In most home connections the upload speed is significantly lower than the download speed. Moreover, since the 3G and 4G speeds are increasing and mobile internet connections are encrypted until the transmission tower, it would be faster and comparably secure to use 3G and 4G than to use a home connection for VPN (interview May 25, 2016).

To summarize, the main reasons for using VPN is increased privacy while surfing, increased security when using public wifi or rogue access points. The main disadvantage is that VPN reduces internet speed to some extent and not all online services are compatible when using a VPN-connection. The simplest method for consumers to get VPN is to download the (paid) software from a VPN-provider. The market of VPN-providers is covered in the next chapter containing a stakeholder analysis of the organizational landscape in the Netherlands.

5 Stakeholder analysis

This chapter contains an analysis of the relevant stakeholders. The analysis covers consumers, the mobile telecom market for consumers, the market for VPN-providers, the relevant stakeholders within the Dutch government, and a number of separate VPN initiatives.

5.1 Consumers

5.1.1 Cybersecurity awareness of consumers

Since 2012 the cybersecurity awareness of consumers in the Netherlands, and various professional target groups in the public and private sector, have been measured annually by market research bureaus (Motivaction, 2012; Gfk, 2013, 2014, 2015; TNS NIPO, 2016).³ The empirical studies, based on questionnaires, were carried out for the Dutch government for the annual Alert Online awareness campaign. Five studies have been conducted so far. The studies of 2012, 2013 and 2014 are partly the same. A number research questions were kept the same to enable longitudinal comparison. Some research questions varied depending on the focus of the Alert Online campaign that year. The studies of 2013 and 2014 compare the results to the previous year. The report of 2015 shifts its focus, only making general comparisons possible (Gfk, 2015: 5). The study of 2016 focuses on cybersecurity skills. Because of differing methodologies, the study of 2014 is used as a baseline because of its longitudinal aspects. The study of 2016 is additionally used for the most recent data. The study of 2016 researched how well known specific cyber threats and protective measures are. The researched groups of consumers in all studies consisted of people of 13 years of age and older.⁴

Through all studies, the general measure of cybersecurity awareness of consumers is the lowest of all researched groups. “Consumers feel more aware of cybersecurity risks than they actually are, based on the measure of risk perception, versus knowledge and behavior.” (Gfk, 2014: 21). Three quarters of consumers in the Netherlands hardly worry about cybercrime, while actual the victimization of some form of cybercrime is high (TNS NIPO, 2016: 9). Most consumers answer that their digital behavior is secure (TNS NIPO, 2016: 23). At the same time around half of the consumers state that they have little to no knowledge on how to protect themselves against cyber threats (TNS NIPO, 2016: 24).

³ The researched groups varied through the annual studies. Consumers were always part of the study. In 2012 and 2013 the researched groups (other than consumers) were employees in central government, municipalities, critical infrastructure, businesses in non-critical infrastructure (Motivaction, 2012; Gfk, 2013). In 2014 the other groups were employees in central government, provinces, municipalities, regional water authorities, critical infrastructure and businesses in non-critical infrastructure (Gfk, 2014). In 2015 the other groups were employees in central government, civil servants excluding central government, small businesses, medium businesses and large businesses (Gfk, 2015). In 2016 the other groups were independent contractors, employees in the central government, civil servants excluding central government, small businesses, medium businesses and large businesses (TNS NIPO, 2016).

⁴ Through the years the number of respondents in the group of consumers varied between 578 and 1334 (Motivaction, 2012; Gfk, 2013, 2014, 2015; TNS NIPO, 2016).

When it comes to general cyber secure behavior, the research shows that consumers take passive protective measures. Having an antivirus program is the main protective measures consumers take (Gfk, 2014: 10). Installing a third-party antivirus program might be a conscious act. But after the installation is complete, the consumer becomes passive because it trusts the program to notify them if something is wrong. A significantly smaller percentage of the respondents answers that they pay attention to cybersecurity risks online. 68 percent answers that they have antivirus program, 9 percent answers that they pay attention (5 percent in 2013), and 11 percent answers they don't take any protective measures (Gfk, 2014: 60). Furthermore, consumers show more cybersecurity awareness when using computers than when using mobile devices (Gfk, 2014: 59).

In 2014, a thematic addition to the empirical study focused on how consumers find and process information on cybersecurity. The study showed that consumers have a need for clear and practical information on cybersecurity that they can use (Gfk, 2014: 14). When asked how they got their information on cybersecurity, the highest scoring sources are through the media (54 percent, TV, newspaper etc.), family and friends (46 percent), an internet provider (38 percent), bank (34 percent) and through a search engine such as Google (32 percent). The government comes in on the sixth place with 27 percent (Gfk, 2014: 94). In the study of 2016, family and friends was the highest-scoring source of cybersecurity information and skills (51 percent), next to information sites (41 percent) and ISPs (40 percent) (TNS NIPO, 2016: 73⁵).

Next to questions of finding information on cybersecurity, it is relevant to consider if the information leads to different behavior. Nearly forty percent of consumers responds that they take new cybersecurity measures based on new cybersecurity information. Furthermore, taking into account that family and friends are an important source of information, for one in three consumers new information on cybersecurity leads them to talk the topic with others and around 20 percent of consumers helped others in taking protective measures (Gfk, 2014: 97). This leads to the conclusion that providing cybersecurity information will lead to a behavioral change towards cyber secure behavior (Gfk, 2014: 12).

5.1.2 Risk of victimization of cybercrime while using public wifi

There are no statistics on the height of consumer victimization of cybercrime as a result of using public wifi. There are general statistics on cybercrime by Statistics Netherlands, through the awareness studies and specific research into identity fraud.

As mentioned earlier, eleven percent of Dutch consumers has been the victim of cybercrime, which is more than double the percentage of consumers that fall victim to bicycle theft (four percent) (Statistics Netherlands and Ministry of Security and Justice, 2016). A percentage of eleven percent is nearly two million people being a victim of some form of cybercrime.⁶ Statistics Netherlands measured sales fraud, identity fraud and hacking and was based on citizens reports of victimization to various organizations (ibid). The awareness study of TNS NIPO shows that seventy percent of consumers has received phishing emails and forty percent has had some form of malware infection. Specific research conducted into identity fraud concluded that the total amount of damage for consumers because of identity fraud in 2012

⁵ Respondents could choose multiple options, which is why the total amount is above a hundred percent

⁶ Based on the assumption of 17 million citizens in the Netherlands

was around 355 million euros with an average damage amount of 600 euros per victim (Ministry of Interior and Kingdom Relations, 2013: 22). Another study into identity fraud argue that the damage is around 400 euros per victim. Many victims are reimbursed by banks and other organizations. They estimate that the societal costs of identity fraud between 2008 and 2012 was 300 million euros (Paulissen and Van Wilsem, 2015). Despite the fact that victimization of cybercrime while using public wifi is not isolated, the data does show that cybercrime is a large problem for consumers and businesses in the Netherlands.

5.1.3 Consumer use of VPN

VPN is not widely used by consumers. Nearly forty percent of consumers do not know what VPN is (TNS NIPO, 2016: 19). In 2015, only 22 percent of the consumers responded that they use VPN when on public wifi (Gfk, 2015: 40). Even under cybersecurity professionals and enthusiast, the use of VPN is not common. Only 32 percent of the readers of Security.nl, a Dutch news site specialized in cybersecurity, responded to a poll that they use VPN on their smartphones (Security.nl, 2016, n=1759). Forty percent of the Security.nl respondents said that they do not use VPN.

5.2 Telecom providers: the mobile market for consumers

The mobile market in the Netherlands for consumers is a mature and highly competitive market. The market penetration of mobile subscriptions is high (BuddeComm, 2016; Tele2, 2013; interview October 10, 2016). There are three operators that have their own network: KPN, Vodafone and T-Mobile and a large number of so-called virtual operators use the network of these three providers for their services (ACM, 2016c: 13; Telecompaper, 2016). Tele2 and Ziggo are in the process of implementing their own network (ACM, 2016a). Ziggo and Vodafone are currently in the process of establishing a joint venture (Nu.nl, 2016). Consumers can change operators easily at the end of their subscription periods. Keeping their phone number when changing providers is a legal right for consumers (ACM, 2016b). The cost of mobile subscriptions are fairly homogeneous (see appendix 1 for a comparison prices between T-Mobile, KPN and Vodafone). This means that for mobile subscriptions consumer lock-in is low. Since a few years, the telecom companies are pursuing convergence strategies, meaning that they offer larger discounts when consumers also buy other services from the same provider (Tele2, 2013). For instance combining a home internet, phone and TV package with a mobile subscription. The amount of package subscriptions is growing in the Netherlands. At the end of 2015, there were seven million consumers with package subscriptions (ACM, 2016c: 3). Next to the larger discounts, package subscriptions increase consumer lock-in. Currently, there is little information available on consumer VPN from telecom providers (see appendix 2). Of the three largest mobile telecom providers, only KPN offers information on consumer VPN online.

5.3 The market for VPN-providers

There are many VPN-providers for a consumer to choose from, around 170. None of the providers are based in the Netherlands (That One Privacy Guy, 2016). Amongst them are a small number of technology household brand names. The names of many of the VPN-providers seem obscure. In terms of quality, there are large differences between providers. For instance on the security of the VPN-service itself, but also in business practices where some don't uphold the standard of behavior that they advertise. Keeping

logs is an example (Ars Technica, 2016). The average price of a VPN-service per connection is around 3, 30 dollars a month. Prices vary. The lowest price per connection per month is 0, 16 dollars. The highest is 22, 92 dollars a month (That One Privacy Guy, 2016). I argue that this offers a view of an immature market for VPN-services. Technical experts warn that not all VPN-providers are reliable and that it is difficult to make a simple list of good VPN-providers (Ars Technica, 2016; interview May, 25, 2016; interview November 2, 2016). Moreover, comparison criteria for VPN-providers are mainly technical in nature (That One Privacy Guy, 2016). This is also the case for information on choosing a VPN-service from consumer organizations (Consumentenbond, 2016). I argue that this makes it a challenge for an average consumer to currently compare and choose a good VPN-provider.

5.4 Other market initiatives on VPN

In the market a number of other market players are currently incorporating VPN in their services. Browser vendor Opera has developed a native VPN-service within its browser for desktop computers and for mobile platforms (Opera, 2016; Tweakers, 2016a). For its Nexus smartphones, Google has developed an app called 'Wifi manager' which uses a VPN-connection when users connect to public wifi (Androidworld, 2016).

The Dutch ISP for research and educational institutions Surfnet has developed an open source VPN-service called Let's Connect/EduVPN (Let's Connect, 2016). Surfnet is a non-profit organization. Surfnet developed the VPN-service initially for research and educational institutions. The service consists of remote access to the network of the institution and secure browsing through VPN for employees and for students (interview November 1, 2016). Surfnet developed the service over a two-year period focusing on both the use of strong cryptography and user-friendly apps (ibid). Consumers are not the primary target audience of Surfnet, but because of their choice for open source software, the application will also become available for consumers to use when they launch the service at the beginning of 2017. The entire implementation of EduVPN will be a paid service that Surfnet offers its constituents of research and educational institutions (ibid). The open source nature of the software also means that organizations such as ISP's can access the software, rebrand it, develop their own features and implement it without commercial license costs. Dutch ISP XS4All is also a participant in the project and is looking into doing a pilot with the application (ibid). Furthermore, Surfnet is trying to promote the service internationally amongst its peers. Lastly, they are looking towards integrating more security features within application in the future. For instance protection against malware (ibid).

5.5 The Dutch government

In telecom sector, the Telecommunications law (*Telecommunicatiewet*) is the legislative framework (Overheid.nl, 2016). The Telecommunications law contains a collection of regulations, also implementing a number of EU directives, for the entire telecom field. Relevant for this thesis are a number of elements. The law regulates the access that virtual operators have to the mobile network owned by KPN, Vodafone and T-Mobile. The law also regulates the aforementioned rights of consumers when buying telecom services. Next to the right to keep their phone number when switching operators it regulates what rights consumers have when entering into a subscription. For cybersecurity issues, the telecom providers have a duty of care set down in article 11.3 (Overheid.nl, 2016). The telecom providers are required to take

appropriate technical and organizational measures to ensure that personal data is protected and providers are required to inform customers about cybersecurity risks. The Netherlands Authority for Consumers and Markets (*Autoriteit Consument en Markt, ACM*) is the supervising authority for this section of the law. The Radio Communications Agency (*Agentschap Telecom*) is the supervising authority for continuity aspects of telecommunications. Policy-making for telecom and digital services is the responsibility of the Ministry of Economic Affairs. The ministry of Economic Affairs promotes entrepreneurship and innovation. So ensuring a level playing-field in the market is an important aspect (Ministry of Economic Affairs, 2013: 4). In its vision on the telecom market the ministry sees less of a hierarchical role for itself and primarily wants to apply so-called network governance (ibid: 5). The ministry focuses on market dialogue first and will only use regulation when it is absolutely necessary (ibid: 4). The Ministry of Economic Affairs takes an economic perspective to policy-making. For instance, if it ascertains that there is some form of market failure, the ministry identifies the type of market failure (information asymmetry, externalities etc.) and takes steps to counteract that particular form of market failure (interview October 10, 2016).

In addition to telecom policy in general, the government's cybersecurity policy is summarized in the National Cyber Security Strategy (NCSS2). The NCSS2 is coordinated by the Ministry of Security and Justice and every ministry is responsible for carrying out measures in the sectors for which they are responsible. Cornerstones of the cybersecurity policy are the personal responsibility of government, businesses and consumers for their own cybersecurity and public-private partnerships (Ministry of Security and Justice, 2013). At a European level the Network and Information Security (NIS) directive came into force in July 2016 and is currently in the process of transposition. Amongst other elements, the NIS-directive (article 14.1) requires operators of essential services (this includes telecom providers) to take cybersecurity measures (Overheid.nl, 2016; European Union, 2016b).

When it comes to cybersecurity knowledge and expertise, the Dutch NCSC is the central organization in the Netherlands. The NCSC is a part of the National Coordinator for Counterterrorism and Security of the Ministry of Security and Justice. The focus of the NCSC is on the cybersecurity of the central government and critical infrastructure. It also shares its knowledge and expertise with a wider public through various publications (interview October 19, 2016). Through those publications, the NCSC sets out cybersecurity good practices. The advice to use VPN while using public wifi is one of those publications (NCSC, 2015).

When it comes to stimulating consumer awareness on cybersecurity, there are two government initiatives. The first is the yearly Alert Online awareness campaign since 2012 (Alert Online, 2016a). The campaign focuses on government agencies, businesses and consumers for the duration of two weeks in October each year. The campaign is not a traditional government awareness campaign which limits its coverage. The second initiative is the website *Veiliginternetten.nl*. The website is a portal aimed at providing consumers with information and guides on what cybersecurity measures to take (Veiliginternetten.nl, 2016a). The advice to use VPN when using public wifi is part of both information channels (Alert Online, 2016b, Veiliginternetten.nl, 2016b).

6 Analysis: why is smartphone VPN for consumers currently not a standard service in the Netherlands?

Based on the stakeholder analysis, desk research and validated by interviews I argue there are a number of factors that explain why smartphone VPN for consumers is currently not a standard service in the Netherlands. The second section of this chapter argues how these factors can be counteracted in the overriding interest of the cybersecurity of consumers.

6.1 Explaining the status quo

6.1.1 Consumers do not know about VPN and using it would mean an active effort

Despite the cybersecurity benefits of VPN, it is not widely used by consumers. The low percentage of consumer use of VPN is consistent with the passive stance that consumers have on cybersecurity. Getting a VPN-service is an active measure (possibly with costs), because it is not installed and active as a default on their smartphones. This in contrast to a firewall on a pc which is active by default. The limited knowledge of cybersecurity also plays a role. Consumers have limited knowledge of the online risks and the risks of using public wifi on the one hand. And they insufficiently know about the existence and benefits of VPN on the other hand. The limited use of VPN under cybersecurity professionals and enthusiasts of Security.nl does form an inconsistency though. They do have sufficient knowledge on the risks and benefits of VPN compared to average consumers. An explanation can be that they are similar to average consumers in the fact that they also are passive to some extent when it comes to taking new protective measures. The example of Avast intercepting the data of two thousand users at the Mobile World Congress also seems to fit the idea of a passive professional. In economic terms, you can say that market demand for VPN is low.

Furthermore, even if consumers would be interested in using VPN, choosing a VPN-provider is difficult for an average consumer. This means that informing consumers on benefits of VPN in itself will not automatically ensure an adoption rate of all consumers.

6.1.2 Telecom providers have no incentive to offer VPN-services

Cybersecurity measures require investments by telecom providers. This includes building VPN into their smartphone subscriptions as a default or as an extra paid service. Currently there is insufficient customer demand for smartphone VPN for consumers. This means there are insufficient external incentives for a telecom provider to justify the investment. Firstly, investing in VPN would raise the business cost of telecom provider, thus potentially losing competitive position. The mobile service that telecom providers offer is 3G and 4G connectivity, which is encrypted. Based on this perspective, telecom providers would more likely advise consumers to use mobile internet instead of developing a VPN-service. Secondly, if a telecom provider decides to start offering VPN-services, it also has to compete with third-party VPN-providers that do not have to take telecom infrastructure costs into account, as telecom providers do. Lastly, the internal incentive to provide VPN based on rising customer support cost is not applicable.

Consumers are insufficiently aware of risks using public wifi. This lowers the chances that customers would ask for customer support on this specific issue from telecom providers. In sum, the incentive structure for telecom providers needs to change in order for them to start offering smartphone VPN to consumers.

6.1.3 Government interferes as little as possible with the market

The government or governance layer, enables and constrains the behavior of people and organizations in society. In a regulatory state, especially in the EU framework of the single market, the basic stance of the Dutch government is to interfere with the market as little as possible. Government should ensure a level playing field for market suppliers. Currently, the Dutch government does not have any specific policy on the use of VPN by consumers. This means that the status quo is the market dynamic between consumers and telecom providers as described above. If the Dutch government would want to actively change the status quo, it has a wide range of tools at its disposal. Which policy strategies are possible, is the focus of the next section.

6.1.4 In sum

The competitive mobile market is the central arena around which all actors revolve. At the same time all the incentives in the arena are not favorable for smartphone VPN for consumer to become a standard service in mobile subscriptions. The basic motor of the market starts with consumer demand for a service such as VPN. Currently there is insufficient consumer demand to get that engine started. Average consumers lack the knowledge and risk perception to want a VPN-service incorporated in their mobile subscriptions and to therefore justify a telecom provider to invest in a smartphone VPN-service for consumers. The role of the government in this market dynamic is limited. There are no active policy measures focusing on VPN other than informing consumers through information channels such as Veiliginternetten.nl and Alert Online. Within these initiatives, VPN is one of many cybersecurity measures that are recommended for consumers. This position of the government, fits into the spirit of the current policies. The government prefers the market to organize solutions. In sum this means that all roads lead to the market where the deck is currently stacked against introducing smartphone VPN for consumers as a standard service.

6.2 Changing the status quo

Having identified factors that explain the current situation, there are arguments to be made on how the status quo can be changed.

6.2.1 More actively informing consumers leads to behavioral change

If clear and practical information on VPN is provided to consumers, a percentage will probably start using VPN, speak to others about the topic and help others install the service. The most active effort that consumers need to make is to install the service. If they are helped by family and friends, the investment in terms of effort is small. Considering that VPN is a simple technology to use, a large-scale information

campaign will boost VPN into being a household term of cybersecurity measures. This would stimulate market demand from consumers for VPN.

6.2.2 A smartphone VPN-service for consumers can boost the reputation of telecom providers and market dominance in VPN-services has not yet been established

Consumers might not specifically ask telecom providers for customer support on issues regarding public wifi and VPN. However, awareness studies show that ISPs are a relevant source of cybersecurity information for consumers. And with the significant amount of cybercrime it is likely that telecom providers increasingly receive questions from consumers on various cybersecurity issues. Considering the immature market for VPN-providers, which lacks recognizable and therefore inherently reliable brand names, offering a smartphone consumer VPN-service can be interesting to telecom providers to boost the reputation of telecom providers as a reliable party on cybersecurity issues for consumers. Another incentive for telecom providers is that market dominance in the field of VPN-providers has not yet been established. This means that becoming active in the field of VPN-services, a telecom provider has the possibility to step into the race of national and international market dominance. Being a recognizable brand name is a significant advantage that telecom providers have over almost all other VPN-providers currently in the market.

6.2.3 For policy-makers smartphone VPN for consumers is low-hanging fruit

Implementing smartphone consumer VPN is currently uncharted policy territory in which all progress is beneficial. VPN is an existing and scoped cybersecurity solution. It is also to some extent straightforward to make progress on this topic compared to other cybersecurity issues such as IoT-security or big data. I argue that this makes smartphone VPN for consumers low-hanging fruit from a policy perspective. The government also has market-oriented policy tools at its disposal to reach its policy goals.

6.2.4 Conclusion: change is possible

In the overriding interest of the cybersecurity of consumers, there are sufficient possibilities and incentives to change the status quo and for the government to pursue a policy strategy for smartphone VPN. Which policy strategy is feasible to invest in is the focus of the next segment. Part three consists of three chapters, one chapter per policy strategy of industry self-regulation, co-regulation and legislation. Each chapter analyzes the feasibility of the strategy based on the six criteria of the theoretical framework.

Part Three

The feasibility of possible government strategies

Industry self-regulation

Co-regulation

Legislation

7 Industry self-regulation

The role of the government in industry self-regulation is understood as agenda-setting on the topic of smartphone VPN for consumers. The design and implementation of the solution is carried out by telecom providers. This makes the business case of VPN for consumers on their smartphones a relevant factor to take into account. After the section concerning the business case, the feasibility of industry self-regulation is assessed.

7.1 Elements of a business case for a telecom provider for smartphone VPN for consumers

Currently there is no existing business case from telecom providers for smartphone VPN for consumers that the research could find or access. Also, business cases contain sensitive corporate information when it comes to numbers and figures. Therefore this research cannot give any quantitative insights regarding the costs and benefits of such a service for a telecom provider. Instead the elements of a business case for such a service are identified.

A business case for smartphone VPN for consumers would take the following elements into account. Firstly, how large is the customer base for the service? On the one hand, what is the customer base that is interested in the product up front? This would be a limited amount of cybersecurity conscious consumers (interview, September 26, 2016). On the other hand, what is the percentage of customers that are confronted with the problem the service addresses (interview, October 26, 2016)? This is a larger customer base when you take the victimization of cybercrime into account. A telecom provider tries to gain insight into the amount of customers that have cybersecurity problems based on customer calls and complaints (interview, October 26, 2016). Secondly, an important element of a business case is how a service improves customer satisfaction and consequently customer loyalty (interview, October 26, 2016). Customer satisfaction is measured through a scoring system such as the Net Promoter Score (how likely is a customer to recommend this organization to others?) (interview October 26, 2016). More specifically customer satisfaction is measured through two factors, customer calls and churn rates. Customer calls weigh into a business case because of their handling costs (interview, October 26, 2016). Van Eeten and Bauer also identified the cost of customer support as a significant incentive for businesses to act on cybersecurity issues (Van Eeten and Bauer, 2013: 459). The churn rate is a measurement of customer loss. Customer loss is measured because it costs more to attract a new customer than to retain an existing customer. A business analyzes why customers leave and tries to adjust its services to minimize customer losses. Isolating individual services as a factor to churn rates is not easy and a business needs to make some assumptions on that account (interview, October 26, 2016). When it comes to security services, such as VPN, a relevant question is to what extent customers understand that they need the service and how much effort does a provider need invest to convince customers of its benefits (interview October 26, 2016). Aside from influencing the height marketing investments, it also influences a decision whether or not a service is offered as in an opt-in or opt-out-model. It also influences whether or not it is offered as an additional paid service or complimentary for particular customer groups or for free up to a certain amount of devices. The potential margins on cybersecurity services are not as large as other services of a telecom provider such as TV-packages. But at the same time a provider wants to show customers that a service has value (interview October 26, 2016). Another factor to take into account is how the service fits into the reputation of a business and if a consumer expects the particular telecom provider to offer a

security service such as smartphone VPN. A factor in such a consideration is to what extent the telecom provider wants to be a one stop shop for consumer services and customer support (interview October 26, 2016). This ties into the overall business strategy of individual telecom providers.

Lastly, a business case for smartphone VPN for consumers takes development and running costs of the service into consideration. Firstly, the ICT-costs of either developing a smartphone VPN-service for consumers or contracting a VPN-supplier. Regardless of either option there are costs that relate to technically imbedding a VPN-service within the network of a telecom provider and ensuring compliance to legal requirements such as lawful interception (interview September 26, 2016). Also imbedding the service in the overall billing system needs to be carried out (interview, October 26, 2016). In the case of contracting a VPN-provider, license costs per customer need to be taken into account. When a telecom provider decides to develop the VPN-service themselves they need to invest in secure software development of the service and user-friendly apps (interview September 26, 2016; interview October 26, 2016; interview November 1, 2016). Running a VPN-service has some impact on the speed of data connections of users and consequently on the use of the bandwidth of telecom providers. Establishing a VPN-connection has the most impact on the speed of the connection and is also related to the computational strength of the individual smartphone. As soon as a connection is established the impact on speed is reduced significantly (interview September 26, 2016). To what extent running a VPN-service has an impact on the use of the bandwidth of telecom providers depends on technical design details. Some of these technical implementation issues were addressed in the operationalization of the case study in chapter two. For instance whether or not a VPN-connection would always be active or only when a consumer uses public wifi is one of those implementation issues.

To conclude, aside from the various individual elements of a business case for smartphone VPN for consumers a relevant question is how much impact such a service would have on telecom providers. From a technical perspective a smartphone VPN-service for consumers is feasible for telecom providers (interview September 26, 2016; interview October 12, 2016; interview November 1, 2016). A break-even business case is also considered feasible from a non-profit perspective (interview November 1, 2016). A determining factor is whether or not telecom providers are interested to offer the service depends on the outcomes of the business case (interview September 26, 2016; interview October 20, 2016; interview November 1, 2016). 'The benefits need to outweigh the cost' (October 25a, 2016). Policy strategies are considered negative external incentives for a business to act (interview, September 26, 2016). At the same time, the overview above shows that benefits can be also be less tangible if they are considered beneficial to the overall business strategy and reputation of a telecom provider.

7.2 The feasibility of industry self-regulation

Having established the elements of a business case of smartphone VPN for consumers on their smartphones for telecom providers, this section assesses the feasibility of the policy strategy of industry self-regulation based on the criteria of the theoretical framework.

7.2.1 The proportionality of industry self-regulation

Government and business both consider industry self-regulation the most proportional policy strategy of the three options because it is the least intrusive for the market (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016; interview October 25b, 2016; interview November 3, 2016). Proportionality is also determined by the size of the problem the policy strategy addresses. Since the problem, how much consumers are victimized when using public wifi, cannot be quantified specifically, questions are raised by the private sector about how appropriate and therefore proportional even a policy strategy of industry self-regulation would be (interview October 20, 2016; interview October 25a, 2016). The private sector points out that in practice industry self-regulation is more intrusive and binding than it seems. If the outcome of industry self-regulation based on market dynamic does not achieve the full policy goal, then more far-reaching policy strategies usually follow (interview October 25a, 2016). This makes the private sector perspective to (the proportionality of) industry self-regulation comparable to co-regulation.

7.2.2 To what extent does industry self-regulation reach the intended outcome?

The intended outcome is that VPN becomes a standard service for all consumers in their mobile subscriptions. Industry self-regulation is not expected to fully reach that outcome, because telecom providers can decide whether or not to offer the service depending on the business case (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016; interview October 25b, 2016). Government and business representatives both offer additional notes on this point. The ministry of Economic Affairs stated that product accessibility and product differentiation are also policy considerations (interview October 10, 2016). If the price of mobile subscriptions would increase across the board then a mobile subscription would become a less accessible product for consumers with small budgets, which is undesirable. Product differentiation relates to the freedom of consumers to choose between different services based on their personal responsibility. A consumer should be able to choose for more cybersecurity risks and pay less for their subscription (ibid.). Both these policy considerations mean that it would be an acceptable policy outcome if industry self-regulation raises the bar in the market that some telecom providers offer smartphone VPN-services for consumers instead of all mobile subscriptions containing VPN. The additional perspective that business representatives and ACM offered is that in the past, industry self-regulation was used to achieve sector-wide codes of conduct (interview October 12, 2016; interview October 20, 2016; interview October 25a, 2016). In those cases industry self-regulation as a policy strategy was the outcome of a political process and/or there were a large amount of customer complaints on a certain commercial practice. In those cases an entire sector is called to action through industry self-regulation as an alternative to legislation. Examples are paid SMS-subscriptions and the costs for mobile data outside of the subscription package (interview October 12, 2016; interview October 20, 2016). In such cases of industry self-regulation there is no room for individual business considerations.

7.2.3 The impact of industry self-regulation on the level playing field in the market

If industry self-regulation leaves the choice to offer the service to the judgement of individual telecom providers, then the prognosis is that a number of telecom providers will offer the service and others will not. However, stakeholders generally agree that any impact on the level playing field in the Netherlands is not problematic (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016). This is seen as regular competition in the market. If industry self-regulation leads to an industry-wide code of conduct then the playing field in the market is level (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016). Stakeholders do note a possible negative impact for the Netherlands in the level playing field in the European single market. A Dutch policy strategy might make it more difficult for foreign telecom providers to enter the Dutch market making the Netherlands less attractive for international telecom providers (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016). Since the intended operationalization of industry self-regulation leaves room for individual business considerations then the negative impact on the level playing field for foreign telecom providers is small.

7.2.4 The level of support of stakeholders for industry self-regulation

Comparable to the criterion of proportionality, the level of support of the various stakeholders for industry self-regulation is high because it is the most market-oriented of the possible policy strategies (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016; interview October 25b, 2016; interview November 3, 2016). It leaves telecom providers the room to act according to their business strategy. As previously mentioned there are also some concerns if industry self-regulation is appropriate.

7.2.5 The amount of time industry self-regulation takes

None of the stakeholders have a clear idea on how long a strategy of industry self-regulation would take to achieve the desired outcome. Estimations are one to two years before a telecom provider offers the service (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016). To some extent the implementation time by telecom providers depends on whether or not they have already formulated a business case for a consumer VPN-service. (interview October 10, 2016).

7.2.6 The distribution of costs and benefits

In the case of industry self-regulation the costs of a smartphone VPN-service for consumers are initially borne by telecom providers, but ultimately the consumers pay for the service based on the business case for telecom providers (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016).

7.3 Conclusion on the feasibility of industry self-regulation: feasible

Taking all variables into consideration, industry self-regulation is a feasible policy strategy. The disadvantages of industry self-regulation regarding achieving the desired outcome and introducing possible elements of a non-level playing field in market are not seen as problematic to stakeholders. Industry self-regulation could raise the bar in the market and society regarding a security service such as smartphone consumer VPN, while leaving room for market players to compete based on their own business strategy. The main point of attention regarding industry self-regulation is the different perspectives on how compulsive it is for market players and consequently the amount of stakeholder support that this policy strategy would have. Despite the fact that an industry-wide code of conduct was not the intended form of industry self-regulation in the operationalization of this hypothetical case study, the fact that several stakeholders perceive industry self-regulation as such is relevant to take into account. It is also relevant to note this difference in perspective when looking for common ground between stakeholders.

8 Co-regulation

In the case of smartphone VPN for consumers the government would not only be agenda-setting but also monitor the progress of the market in adopting VPN for consumer services. If the implementation rate in the market is not sufficient then the government would be willing to pursue the third policy strategy of legislation. This makes co-regulation a hybrid form of the other two policy strategies of industry self-regulation and legislation.

8.1 The feasibility of co-regulation

Due to its hybrid nature which includes the shadow of legislation, stakeholders perceive co-regulation a form of legislation or postponed legislation (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016). As mentioned in the previous chapter, industry self-regulation is also perceived by the private sector as co-regulation (interview October 25a, 2016). This makes the assessment of the feasibility of co-regulation as a distinctive policy strategy compared to the others less clear and more comparable to legislation.

8.1.1 The proportionality of co-regulation

Due to the shadow of legislation, co-regulation is seen as a disproportional policy strategy (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016). Policy-makers point out that the government should already be willing to make legislation on a certain topic before it starts down the path of co-regulation (interview October 10, 2016).

8.1.2 To what extent does co-regulation reach the intended outcome?

Co-regulation can reach the intended outcome, because the entire sector of telecom providers needs to act (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016; interview October 25b, 2016). This is the same scenario as in the previous chapter where industry self-regulation encompasses the entire telecom sector. The telecom sector points out that cases of co-regulation in the past were the outcome of a political discourse calling the government to act in the telecom sector on behalf of consumers. In those cases, for instance with telemarketing codes, the sector preferred to have the freedom to design a suitable solution themselves than have legislation design a solution for them (interview, October 20, 2016).

8.1.3 The impact of co-regulation on the level playing field in the market

Comparable to legislation, co-regulation would create a level-playing field in the telecom sector in the Netherlands. At the same time that would raise issues in the European single market as mentioned in the previous chapter (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016).

8.1.4 The level of support of stakeholders for co-regulation

Since co-regulation is seen by (public and private) stakeholders as a form of legislation by the government, the support for co-regulation for smartphone VPN for consumers is low (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016). From a public policy perspective co-regulation (and legislation) in this case also raise an international diplomatic consideration in relation to the current debate on encryption (interview October 19, 2016). At face value, VPN is seen as an anonymizing technique comparable to Tor and consequently as a technique that enables malicious actors and curtails law enforcement. Despite the fact that VPN technically does not curtail law enforcement, this perception of VPN is relevant to take into account. In the current international debate on encryption some countries are calling for the restriction of encryption for national security purposes. The Dutch government has taken a middle position in this debate (Ministry of Security and Justice and Ministry of Economic Affairs, 2016). A decision of the Dutch government to systemically incorporate VPN into the smartphone connections of all Dutch citizens through co-regulation (or legislation) could be perceived as the Netherlands leaving that middle ground in international relations (interview October 19, 2016). Co-regulation does have the support from a civil society perspective because it combines the incentives of the carrot and the stick. Even an investigation into legislation can be sufficient incentive to move market players into action (interview October 25b, 2016).

8.1.5 The amount of time co-regulation takes

Comparable to industry self-regulation, the stakeholders had no clear view on the amount of time co-regulation would take (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016). Based on previous remarks on salience of an issue, I argue that if smartphone consumer VPN is a salient issue then co-regulation would take a comparable amount of time to industry self-regulation around one to two years from initiation to implementation.

8.1.6 The distribution of costs and benefits

The distribution of costs and benefits in co-regulation are seen as comparable to industry self-regulation. The costs of a smartphone VPN-service for consumers are initially borne by telecom providers, but ultimately the consumers pay for the service based on the business case for telecom providers (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016).

8.2 Conclusion on the feasibility of co-regulation: feasible, but has little support

Substantively co-regulation would achieve the intended outcome that all consumers get VPN as a standard service on their smartphones. Co-regulation would succeed calling the entire telecom sector to action. But because of the shadow of legislation, co-regulation has little support from public and private stakeholders. A strategy of co-regulation is feasible if the topic is salient.

9 Legislation

The third potential policy strategy for smartphone consumer VPN is the classic strategy of legislation. Interviews show that for legislation, the Dutch government has a number of options.

9.1 Legislative options

The first option for the government to make smartphone VPN for consumers a legal requirement for telecom providers is to produce new legislation. Legislation can be specifically tailored to the situation or can be more general in nature (interview October 10, 2016). Tailored legislation would focus specifically on VPN for consumers and make VPN a standard service mobile subscriptions. The advantage of specific legislation is that the solution is focused. It establishes telecom providers as the responsible actor and that VPN should be part of their mobile subscriptions. This focus is also a disadvantage, because it does not take future technological or market developments into account. For this reason, legislation can also be more general in nature. General legislation would be more abstract than the technical solution of VPN. It would focus on a generic norm which would be more along the lines of a requirement to encrypt data connections. The advantage of more generic legislation is that it is technology neutral. A disadvantage of general legislation is that a requirement to encrypt data connections is significantly more far-reaching than the intended goal related to VPN. Such a requirement would be at odds with other societal interests, mainly with the interest of law enforcement. VPN does not hinder law enforcement. A legal requirement to encrypt all connections would conflict with the societal interest of investigating and prosecuting cybercrime. Another disadvantage of general legislation is that the scope of actors that it would encompass also significantly increases beyond the original purpose of smartphone VPN for consumers.

Another legislative option for the Dutch government to establish smartphone consumer VPN as a standard service is to introduce the measure as a specification of existing legal requirements for telecom providers. In this scenario, the government could look to the legal provisions regarding the duty of care that telecom providers have under the Telecommunications law and the NIS-directive. Both laws have the same requirement that a telecom provider needs to take ‘appropriate technical and organizational measures’ to ensure cybersecurity (Overheid.nl, 2016; European Union, 2016b). The Telecommunications law additionally requires telecom providers to inform consumers about cybersecurity risks (Overheid.nl, 2016). Under the Telecommunications law, the oversight agency ACM can make policy guidelines to further specify this duty of care. An analogy can be drawn to the Data Protection Authority which published more detailed guidelines on data protection legislation (interview November 2, 2016). In 2007/2008 the ACM (then still OPTA) consulted with the telecom sector about making policy guidelines for cybersecurity, but decided against doing so at that time (ACM, 2008). Despite choosing not to make guidelines in the past, it is still a regulatory possibility. At the same time, the question is whether or not smartphone VPN for consumers is within the scope of the legal provisions. Both laws focus primarily on the security of the systems and services of the telecom provider and the protection of customer data (interview October 10, 2016; interview October 19, 2016). This would mean that providing a cybersecurity service such as smartphone VPN for consumers would not fit in the current legal definition of the duty of care of telecom providers. However, the Telecommunications law does keep room for additional

measures through orders in council (*algemene maatregelen van bestuur*). I argue that it is possible from a policy perspective to specify that security services for consumers such as VPN become a part of the duty of care of telecom providers.

9.2 The feasibility of legislation

Having established the legislative options for the Dutch government, the next step is to assess the feasibility of one option, namely creating new specific legislation establishing consumer VPN as a standard part of mobile subscriptions. New legislation is chosen because it is the most clearly scoped solution of the three legislative options.

9.2.1 The proportionality of legislation

Legislation for smartphone VPN for consumers is seen as a disproportional policy strategy by all stakeholders (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016; interview October 25b, 2016). With such a far-reaching policy strategy the telecom sector raises questions if they are responsible for how consumers use their smartphones. Security problems of open wifi can be seen as a feature of smartphones and not as the service such as 3G and 4G that telecom providers offer customers (interview October 20, 2016).

9.2.2 To what extent does legislation reach the intended outcome?

Since the new legislation would be specifically tailored towards requiring all telecom providers to have VPN as a standard service for consumers in their mobile subscriptions, it would reach the intended outcome (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016; interview October 25b, 2016). A note on an external effect of legislation is that VPN might give consumers a false sense of security. VPN might be perceived as the silver bullet to solve all cybersecurity problems (interview October 25b, 2016). This means that legislation concerning smartphone VPN for consumers would need to be flanked by awareness-raising communication on the benefits of VPN.

9.2.3 The impact of legislation on the level playing field in the market

New legislation would create a level playing field in the Dutch market. As with the other policy strategies, Dutch legislation would create an uneven playing field in the European or international market (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016). VPN-legislation would increase the level of compliance for a telecom provider which would have a negative impact on access to the Dutch telecom market for new or foreign providers (interview October 10, 2016; interview October 20, 2016).

9.2.4 The level of support of stakeholders for legislation

There is no support amongst public and private stakeholders to create new legislation for smartphone VPN for consumers (interview October 10, 2016; interview October 19, 2016; interview October 25a, 2016). Policy-makers prefer market-oriented solutions based on public-private partnerships. Legislation is at odds with that preference. Also they prefer legislative topics to be at a higher level of abstraction than a specific technical solution such as VPN (interview October 10, 2016). International diplomatic considerations as mentioned in the previous chapter also weigh in when considering legislation (interview October 19, 2016).

9.2.5 The amount of time legislation takes

Legislation is expected to take at least three to four years to produce, gain parliamentary approval and implement (interview October 10, 2016; interview October 19 2016; interview October 20, 2016). It is possible that a legislative process would be delayed or unsuccessful due to opposition from stakeholders.

9.2.6 The distribution of costs and benefits

As with other policy strategies, telecom providers need to invest in the VPN-service and consequently consumers will pay for the service through their mobile subscriptions (interview October 10, 2016; interview October 19, 2016; interview October 20, 2016; interview October 25a, 2016). In a legislative policy strategy, the government incurs additional costs for producing legislation and organizing oversight (interview October 10, 2016). Unique to the legislative policy strategy is that it starts a discussion whether the government should compensate all telecom providers for the initial investment costs of establishing the smartphone VPN-service for consumers (interview October 19, 2016; interview October 20, 2016).

9.3 Conclusion the feasibility of legislation: unfeasible

New legislation for smartphone VPN for consumers would reach the policy goal, but there is no support for a legislative strategy. This is mostly due to the disproportionality of the policy strategy. VPN solves the cybersecurity risks of consumers on public wifi, but they face more cybersecurity risks that VPN does not protect against. Legislation for only VPN would be an inappropriate a policy measure. Even if the government decides to pursue legislation, the chances are high that the legislative process would be delayed or unsuccessful due to lack of private sector support. This makes legislation an unfeasible policy strategy.

Part Four

Conclusions and reflection

Policy recommendations

10 Conclusions and reflection

10.1 Conclusions

Having assessed the feasibility of each of the policy strategies the government has at its disposal to implement smartphone VPN for consumers in the Netherlands, the research question can be answered. The research question is:

Assuming that the Dutch government decides that all consumers in the Netherlands should have VPN on their smartphones, what would be a feasible government strategy to make this a reality?

Of the three policy strategies, industry self-regulation is the most feasible. It has the most support of the three strategies because it is the most market-oriented. Telecom providers can design a solution most suitable to them based on their own business case. The business case for telecom providers can be based solely on commercial benefits of the VPN-service, but it can also tie into the business strategy of a telecom provider. If they offer a VPN-service for consumers, they can also use the service for strengthening their reputation on cybersecurity. A disadvantage with industry self-regulation is that the business case of telecom providers is so central that if they decide not to offer the smartphone VPN-service to consumers, then little changes and the policy goal is not reached. On the other hand, government representatives state that raising the bar is sufficient. If a number of telecom providers decides the offer smartphone VPN for consumers, then they would have ability to choose whether or not they want a VPN-service in their mobile subscription. This would be an agreeable policy outcome. This outcome would also mitigate any issues of level playing field in the market, because telecom providers make their own business choices. Central questions for the government with industry self-regulation are, how many consumers reached through industry self-regulation is enough? And to what extent is the government willing to pursue more far-reaching policy strategies if telecom providers decide against offering the service? The private sector is keenly aware of the possibility of more stringent policy strategies. This is why they perceive a policy strategy of industry self-regulation as if it were co-regulation. At the same time, the government does not automatically move to more heavy policy measures on all topics. ACM explored the possibility to make cybersecurity policy guidelines under the Telecommunications law in 2007/2008 and decided against it after consulting the telecom sector.

With regard to the other potential policy strategies, co-regulation would also reach the intended policy outcome. It would also give the telecom sector the room to design a solution suitable to them, and would ensure that all telecom providers offer smartphone VPN for consumers. Despite these advantages, co-regulation has little support from both public and private stakeholders up front due to the shadow of legislation. Civil society argues that this characteristic of co-regulation is needed to get market players to act, even if legislation does not follow. Legislation is considered to be a disproportional policy strategy by all stakeholders in relation to the cybersecurity problems VPN solves. The cybersecurity problems of using public wifi are not large enough to justify new legislation to ensure VPN on the smartphones of all consumers. A policy strategy of legislation also raises concerns regarding the Dutch international diplomatic position regarding the international debate on encryption. Despite the fact that VPN does not hinder law enforcement, the perception of VPN can be different. A less far-reaching policy strategy of

industry self-regulation would strike a better balance of promoting VPN for consumers. Even though the focus of the thesis was on the Dutch market, all stakeholders noted the importance of the position of the Netherlands in the European and international market. A policy strategy should take into account how smartphone VPN for consumers can be achieved while preserving the accessibility of the Dutch market to new or foreign providers. Industry self-regulation also strikes a balance on this issue, because it leaves room for (international) telecom providers to build their own solution. Smartphone VPN for consumers is not as large a service to offer as other telecom services such as national mobile phone coverage, limiting the business impact for new or international telecom providers.

10.2 Reflection

Reflecting on the outcome of the empirical research, the study confirms the regulation literature that there is a general preference from both public and private parties for policy strategies of minimal intervention in the market and that the government can incrementally move up the scale of intervention if needed. On the other hand, the empirical research showed that the policy strategies cannot be as clearly distinguished in practice. Public and private perspectives to policy strategies differ to the extent that the three policy strategies seem to converge in the direction of legislation. Industry self-regulation is perceived by the private sector as co-regulation. And co-regulation is perceived by the government as a form of legislation. The convergence of both perspectives complicate the possibility to find common ground between public and private stakeholders. I argue that public-private dialogue on the differences in perspective is needed to facilitate a change in attitudes towards the societal benefits of smartphone VPN for consumers instead of solely focusing on the commercial attractiveness. The service might not be commercially attractive for all telecom providers, but it can be attractive for some of them also in terms of strengthening their brand name. If a number of telecom providers introduces the service, it would raise the bar in Dutch society. Consequently the initiative could also be exported to other countries as a Dutch best practice.

Reflection on the criteria for assessing the three policy strategies shows that the criterion of time was not a relevant factor for choosing a policy strategy. Most stakeholders had no clear view of the time a specific policy strategy would take. Proportionality of the policy strategy and level of support by stakeholders were more determining factors for choosing a policy strategy. The research also showed that the original policy goal of the scenario that smartphone VPN should become a standard part of mobile subscriptions can be adjusted if it has more support from stakeholders. I argue that this is in line with the Dutch culture of public-private dialogue and consensus-building.

11 Policy recommendations

With the empirical research concluded into potential policy strategies for the Dutch government for smartphone consumer VPN, there are a number of policy recommendations on how to move forward with the topic of consumer VPN based on the current situation.

10.1 Make consumer VPN a part of the cybersecurity policy agenda

All policy-related stakeholders had not thought of VPN for consumers prior to this research. VPN is currently a topic limited to the domain of technical cybersecurity experts. Carrying out the research for this thesis has in itself raised the awareness of public and private representatives on VPN. The government should consider if it wants to promote consumer VPN more systematically and formulate a policy goal for the future in the Netherlands and in the EU. Without formulating a specific policy goal, the next recommendations offer possible actions the government can take.

10.1.1 Invest in raising consumer awareness on VPN

VPN is now part of broader awareness-raising efforts in the Netherlands, but research shows that most consumers don't know what VPN is. Highlight VPN as a topic for future awareness campaigns to promote recognition and to show how simple the technology is.

The duty of care provisions in the Telecommunications law requires telecom providers to inform consumers about cybersecurity risks. The government could enter into a public-private dialogue with telecom providers on how to collectively take consumer awareness on VPN to a higher level as an addition to existing awareness-raising efforts.

If consumers are aware of the importance of VPN, choosing an existing VPN-provider is complex for an average consumer. Existing comparisons between providers are technical in nature and many comparison websites seem unreliable. Helping consumers choose a VPN-provider through independent comparisons would be a next step in facilitating consumers to take the step from cybersecurity awareness to action. The government is not allowed to promote commercial products, but it can consider how to stimulate other parties to ensure that independent comparisons on consumer VPN are conducted. Civil society, consumer organizations or (collective action of) telecom providers are avenues to explore.

10.1.2 Consider a certification scheme for VPN-providers

The current market for VPN-providers is diffuse and immature in terms of quality of service. The government can consider setting up a certification scheme for VPN-providers. This certification mechanism can be established at an international (EU)-level because currently all VPN-providers are based outside of the Netherlands.

10.1.3 Promoting VPN through public wifi providers

Next to focusing on telecom providers, the government can consider focusing on large providers of public wifi for VPN awareness-raising. The government could identify a number of the largest public wifi providers in the Netherlands and start a dialogue on how to promote the use of VPN at public wifi points. Increasing the cybersecurity of public wifi points themselves will be at odds with their interest of accessibility of the public networks. Simply due to the amount of people that potentially use a public wifi point, using a VPN will still be advisable. As an alternative measure, the government could set up a public-private partnership with large public wifi providers that they communicate the importance of using VPN on public wifi through flyers etc. That information could link to the independent comparisons of VPN-providers as mentioned above.

To gain more insight into the cybersecurity risks of public wifi, the government can more specifically research the extent of this problem. This research could underpin the societal interest to promote VPN for consumers.

The most far-reaching policy measure the government can undertake in this context would be to formulate legislation requiring all public wifi points in the Netherlands to inform users about cybersecurity risks and to promote using VPN.

10.1.4 Stimulate ISPs to explore a business case for consumer VPN and facilitate the sharing of good practices

Telecom providers or more broadly ISPs remain a recognizable intermediary for consumers for internet connectivity. The government could stimulate that ISPs make their own business case for a consumer VPN-service as an additional (paid) service. It is probable that a number of ISPs in the Netherlands have not yet considered developing the service. By stimulating them to consider a consumer VPN-service it is possible that it results in a positive business case for some of them. The government could facilitate sharing good practices in the market where possible, such as the open source VPN-initiative of Let's Connect.

10.2 Consider packaging cybersecurity measures for consumers

VPN is one of many beneficial cybersecurity measure for consumers. The government and ICT-businesses could consider to what extent a package of beneficial cybersecurity measures for consumers can be composed, developed and brought to consumers that raises the bar across the board. Currently there are commercial products for internet security that offer more than one feature, but those products do not span the entire eco-system of all (mobile) platforms. For instance, consumers still need to buy an antivirus program and VPN separately. The government could facilitate initial research and public-private discussions into the idea of packaging cybersecurity measures for consumers. It would be up to market players to develop solutions. This could be implemented in the Netherlands but also at a European level since many ICT-businesses are multinational organizations.

10.3 Consider the cybersecurity duty of care in relation to consumers

Currently the focus of cybersecurity legislation and duty of care provisions focus on the security of the own systems of telecom providers and other organizations in the critical infrastructure. The provisions do not extend towards the cybersecurity of consumers. There seems to be a disconnect. A duty of care implicitly implies that a business has a certain amount of responsibility for the cybersecurity of its customers. Business to business, cybersecurity in the value chain can be boosted through contract management. The only form of contract management a consumer can do is not to use a service. The government could explore this disconnect further and consider to what extent a duty of care of businesses should have a broader scope. For instance intermediaries with a direct relationship with consumers could have a responsibility to actively facilitate consumers to be more cyber secure. This means redefining the roles and responsibilities of businesses and consumers for cybersecurity. The answer to this question is ultimately the outcome of a political process in the Netherlands and in the EU. But the question becomes relevant to consider in the next step of maturity in the field of cybersecurity.

10.3 Concluding remarks

This thesis has combined the technical aspects of cybersecurity with the policy aspects of the field. VPN is an existing technical solution to improve the cybersecurity of consumers. It's wider implementation in society that can be given a boost if it is backed by policy initiatives. There are still many challenges for society to face when it comes to securing our digital lives. This thesis has contributed by analyzing the potential implementation of one cybersecurity solution in-depth. The saying goes that Rome was not built in a day. A cyber secure society also needs to be built one digital brick at a time. VPN for consumers is one of the digital bricks society needs to lay.

References

- ❖ ACM (2008), *Vervolg zorgplicht internetaanbieder*, <https://www.acm.nl/nl/publicaties/publicatie/9616/Vervolg-zorgplicht-internetaanbieders/>, last consulted November 21, 2016.
- ❖ ACM (2016a), <https://www.acm.nl/nl/onderwerpen/telecommunicatie/telefonie/toezicht-op-telefonie/> 'hoe ziet de markt voor mobiele telefonie eruit?'; last consulted, July 20, 2016.
- ❖ ACM (2016b), <https://www.acm.nl/nl/onderwerpen/telecommunicatie/telefonie/nummerportabiliteit/>, last consulted July 20, 2016.
- ❖ ACM (2016c), *Telecommonitor vierde kwartaal 2015*, April 22, <https://www.acm.nl/nl/publicaties/publicatie/15722/Telecommonitor-vierde-kwartaal-2015/>, last consulted: November 24, 2016.
- ❖ Alert Online (2016a), <https://www.alertonline.nl/over-deze-campagne>, last consulted: July 20, 2016.
- ❖ Alert Online (2016b), <https://www.alertonline.nl/tips>, last consulted: November 25, 2016.
- ❖ Andersen, R. and T. Moore, (2006), 'The economics of information security', *Science*, **314**, 610-613.
- ❖ Anderson, R. and T. Moore (2007), 'Information Security Economics – and Beyond', *Computer Laboratory, University of Cambridge*, http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf, last consulted: May 6, 2016.
- ❖ Androidworld (2016), *Google WiFi-manager zorgt voor veiligere verbinding Nexus-toestellen*, <https://androidworld.nl/nieuws/google-wifi-manager-nexus/>, August 25, last consulted: November 24, 2016.
- ❖ Ars Technica (2016), *The impossible task of creating a "best VPNs" list today*, <http://arstechnica.com/security/2016/06/aiming-for-anonymity-ars-assesses-the-state-of-vpns-in-2016/>, June 1, last consulted: November 24, 2016.
- ❖ Avast (2016), *Avast Wi-Fi Hack Experiment Demonstrates "Reckless" Behavior of Mobile World Congress Attendees* <https://press.avast.com/en-us/avast-wi-fi-hack-experiment-demonstrates-reckless-behavior-of-mobile-world-congress-attendees>, February 22, last consulted: April 30, 2016.
- ❖ Berger, T. (2006), 'Analysis of current VPN technologies', *The First International Conference on Availability, Reliability and Security, 2006. ARES 2006: IEEE*, <http://ieeexplore.ieee.org/document/1625300/>: last consulted: October 24, 2016.
- ❖ Ballegooij, G.A.C.M., T. Barkhuysen, A.F.M. Brenninkmeijer, W. den Ouden and J.E.M. Polak (2004), *Bestuursrecht in het Awb-tijdperk*, Deventer: Kluwer, 5th edition.
- ❖ Bits of Freedom, *Versleutel je internetverbinding met een VPN*, <https://toolbox.bof.nl/adviezen/vpn/>, last consulted: December 2, 2016
- ❖ Bovens, M.A.P., P. 't Hart, M.J.W. Twist and U. Rosenthal (2001), *Openbaar bestuur: beleid, organisatie en politiek*, Alphen aan den Rijn: Kluwer, 6th edition.
- ❖ Brownsword, R. (2005), 'Code, control, and choice: why East is East and West is West', *Legal studies*, 25(1), 1-21.
- ❖ Brughna, R. and Z. Varvasovszky (2000), 'Stakeholder analysis: a review', *Health policy and planning*, 15(3) pp. 239-246.

- ❖ BuddeComm (2016), <http://www.budde.com.au/Research/Netherlands-Mobile-Infrastructure-Broadband-Operators-Statistics-and-Analyses.html>; last consulted July 20, 2016.
- ❖ Consumentenbond (2016), <https://www.consumentenbond.nl/veilig-internetten/veiliger-internetten-met-een-vpn> , last consulted: November 24, 2016.
- ❖ CPB Netherlands Bureau for Economic Policy Analysis (2003), *Equal Rules or Equal Opportunities? Demystifying Level Playing Field*, <https://www.cpb.nl/sites/default/files/publicaties/download/equal-rules-or-equal-opportunities-demystifying-level-playing-field.pdf> , last consulted: November 4, 2016.
- ❖ Deibert, R.J. (2009), 'The geopolitics of internet control, Censorship, sovereignty, and cyberspace' *Chapter 23 Handbook of Internet Politics*, http://www.handbook-of-internet-politics.com/pdfs/chapter_23.pdf , last consulted: April 30, 2016.
- ❖ European Union (2016a), *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031>, last consulted: May 22, 2016.
- ❖ European Union (2016b), *Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1479733938340&from=NL> , last consulted: November 21, 2016.
- ❖ European Commission (2016), "State of the Union 2016: Commission paves the way for more and better internet connectivity for all citizens and businesses", <http://europa.eu/rapid/press-release-IP-16-3008-en.htm>, September 14, last consulted: September 28, 2016.
- ❖ Fahad, A.A., H. Gaspar-Modelo, B. Saurabh (2012), 'To cloud or not to cloud: A study of trade-offs between in-house and outsourced virtual private network', *The 2012 20th IEEE International Conference Network Protocols (ICNP): IEEE*, <http://ieeexplore.ieee.org/document/6459949/> , last consulted: October 24, 2016.
- ❖ F-Secure (2014), *The dangers of public wifi – and crazy things people do to use it*, <http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/> , September 29, last consulted: April 30, 2016.
- ❖ Gfk (2013), *Rapportage Cyber security*, October 24, <https://www.alertonline.nl/toolkit> , last consulted: October 8, 2016.
- ❖ Gfk (2014), *Cyber security; awareness, gedrag en informatiebehoefte*, October 15, <https://www.alertonline.nl/toolkit> , last consulted: October 8, 2016.
- ❖ GfK (2015), *Cybersecurity 2015 Awareness, gedrag & digitaal verantwoord ondernemen*, <https://www.alertonline.nl/toolkit>, September 25, last consulted: October 8, 2016.
- ❖ Goldsmith, J. and T. Wu (2006), *Who controls the internet? Illusions of a borderless world*: Oxford University Press.
- ❖ Jager, J. de (2016), 'Wat is VPN?' , <http://computertotaal.nl/internet-thuis/wat-is-vpn-67587>, February 21, last consulted: May 25, 2016.
- ❖ KPN (2016a), KPN Wifi <https://www.kpn.com/mobiel/bundels/kpn-wifi.htm>, last consulted: September 30, 2016.
- ❖ KPN (2016b), KPN Fon <https://www.kpn.com/internet/wifihotspots.htm>, last consulted: September 30, 2016.
- ❖ KRO Brandpunt (2014), *Episode of April 13, 2014 on the security of wifispots*, <https://www.youtube.com/watch?v=I7BBeocq9Fo> , until 11:30 minutes, last consulted: April 30, 2016.

- ❖ Leenes, R. (2011), 'Framing techno-regulation: an exploration of state and non-state regulation by technology', *Legisprudence*, 5(2), 143-169.
- ❖ Lessig, L. (2006), *Code: version 2.0*, 2nd ed. New York: Basic Books.
- ❖ Let's Connect (2016), <https://letsconnect-vpn.org/>, last consulted: November 24, 2016.
- ❖ Lodge, M. and K. Wegrich (2012), *Managing regulation, regulatory analysis, politics and policy*, Basingstoke: Palgrave Macmillan.
- ❖ Mayer-Schonberger, V. (2008), 'Demystifying Lessig', *Wisconsin law review*, 2008(4), 713-746.
- ❖ Microsoft (2016), "Windows 8: Explore new and improved security features", <https://www.microsoft.com/en-us/safety/pc-security/windows8.aspx>, last consulted: September 30, 2016.
- ❖ Ministry of Economic Affairs (2013), *Middellangetermijn visie op telecommunicatie, media en internet*, December 23, <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2013/12/23/kamerbrief-over-middellangetermijn-visie-op-telecommunicatie-media-en-internet/kamerbrief-over-middellangetermijn-visie-op-telecommunicatie-media-en-internet.pdf>; last consulted July 20, 2016.
- ❖ Ministry of Interior and Kingdom Relations (2013), *Identiteit in cijfers*, December 12, <https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/rapporten/2013/12/12/identiteit-in-cijfers>, last consulted: November 24, 2016.
- ❖ Ministry of Security and Justice (2013), *National Cyber Security Strategy 2, from awareness to capability*, October 29, <https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html>; last consulted, July 20, 2016).
- ❖ Ministry of Security and Justice and Ministry of Economic Affairs (2016), *Kabinetsstandpunt encryptie*, January 4, <https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie>, last consulted: November 18, 2016.
- ❖ Motivaction (2012), *Cyber Security Awareness, een onderzoek naar kennis, bewustzijn en gedrag ten aanzien van cyber security*, November, <https://www.alertonline.nl/toolkit>, last consulted: October 8, 2016.
- ❖ NCSC, National Cyber Security Center (2015), *Wifi onderweg: gebruik een VPN*, Factsheet FS-2008-01 version 2.0, August 6, <https://www.ncsc.nl/actueel/factsheets/wifi-onderweg-gebruik-een-vpn.html>, last consulted: April 30, 2016.
- ❖ NCSC, National Cyber Security Center (2016), *Cyber Security Assessment Netherlands 2016*, <https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html>, last consulted: November 5, 2016.
- ❖ Neelen, G.H.J.M., M.R. Rutgers, M.E. Tuurenhout (ed.) (2003), *De bestuurlijke kaart van Nederland*, Bussum: Coutinho, 2nd edition.
- ❖ Nu.nl (2016), *Ziggo en Vodafone Nederland verder als één bedrijf*, <http://www.nu.nl/internet/4215362/ziggo-en-vodafone-nederland-verder-als-bedrijf.html>, February 16, last consulted: November 25, 2016.
- ❖ Overheid.nl (2016), *Telecommunicatiewet*, <http://wetten.overheid.nl/BWBR0009950/2016-07-01>; last consulted, November 21, 2016.
- ❖ Oosthuizen (1998), 'Security issues related to E-commerce', *Network Security*, 1998(5), pp.10-11.
- ❖ Opera (2016), *Free VPN integrated in Opera for better online privacy*, <http://www.opera.com/blogs/desktop/2016/04/free-vpn-integrated-opera-for-windows-mac/>, April 20, last consulted: November 24, 2016.

- ❖ Paulissen, L. and J.A. van Wilsem (2015), *Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland*, Amsterdam: Reed Business,
<http://www.politieenwetenschap.nl/download/wrud2HFKQ9JCKoy8dHkjV3Ou52YeQfdUbsvZcFw/EclGEHYOyxHY4RVMExJim7rHqwgDIIFuQVTvEWQd/>.
- ❖ Pcworld.com (2013), *How (and why) to set up a VPN today*,
<http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html> , last consulted: April 30, 2016.
- ❖ Rijksoverheid (2016), “Overheid als marktpartij”,
<https://www.rijksoverheid.nl/onderwerpen/mededinging/inhoud/markt-en-overheid>, last consulted: September 28, 2016.
- ❖ Scott, C., P Wolfe and M. Erwin (1999), *Virtual Private Networks, Turning the Internet into your private network* (2nd ed), Sebastopol, CA: O’Reilly. Retrieved from
<https://books.google.nl/books?hl=nl&lr=&id=OuFQ3t7eF4IC&oi=fnd&pg=PR9&dq=virtual+private+network+consumer&ots=hepWzAyL5z&sig=S9AjQkfSCwIVdHN5pDFo6xalG0k#v=onepage&q&f=false> , last consulted: October 24, 2016.
- ❖ Security.nl (2014), *Europol: VPN noodzakelijk bij open wifi-netwerken*,
<https://www.security.nl/posting/403599>, September 29, last consulted: May 21, 2016.
- ❖ Security.nl (2016), *Poll: Maak jij gebruik van een VPN op je smartphone?*,
<https://www.security.nl/posting/470158/Maak+jij+gebruik+van+een+VPN+op+je+smartphone+percent3E>, May 9, last consulted: May 21, 2016.
- ❖ Statistics Netherlands and Ministry of Security and Justice (2016), *Veiligheidsmonitor 2015*, March 1, <https://www.rijksoverheid.nl/documenten/rapporten/2016/03/01/tk-bijlage-veiligheidsmonitor-2015>: last consulted September 28, 2016.
- ❖ Tele2 (2013), *Market Overview, Bob Bunnik*,
<http://www.tele2.com/Documents/documents/Analyst-Journalist-Meeting-Tele2-5-9-2013-Bob.pdf>; last consulted: July 20, 2016.
- ❖ Telecompaper (2013), *OTT markt monitor januari 2013 Rapport voor OPTA*, January 10,
<https://www.acm.nl/nl/publicaties/publicatie/11717/Overzicht-markt-voor-over-the-top-diensten---Nederland---januari-2013-Telecompaper/> , last consulted: October 22, 2016.
- ❖ Telecompaper (2016), *Dutch Mobile Virtual Operators 2016 Q1 - All Profiles* (the publicly available sections), <http://www.telecompaper.com/research/dutch-mobile-virtual-operators-2016-q1-all-profiles--1153924>; last consulted: July 20, 2016.
- ❖ Thaler, R.H. and C.R. Sunstein (2008), *Nudge: Improving decisions about health, wealth, and happiness* New Haven: Yale University Press. Retrieved from:
https://books.google.nl/books?id=mzZV9jFLltwC&printsec=frontcover&dq=Nudge:+Improving+decisions+about+health,+wealth+and+happiness&hl=nl&sa=X&redir_esc=y#v=onepage&q&f=false , last consulted: October 24, 2016.
- ❖ That One Privacy Guy (2016), <https://thatoneprivacysite.net/vpn-comparison-chart/> , version of November 20, 2016, last consulted: November 20, 2016.
- ❖ TNS NIPO (2016), *Cyber Security awareness en skills in Nederland*, September,
<https://www.alertonline.nl/toolkit> , last consulted: October 8, 2016.
- ❖ Top10vpn.com (2016), <https://www.top10vpn.com/about/>, last consulted: November 24, 2016.
- ❖ Tweakers (2016a), *Opera brengt gratis VPN-app voor iOS uit*,
<https://tweakers.net/nieuws/111117/opera-brengt-gratis-vpn-app-voor-ios-uit.html>, May 9, 2016, last consulted: November 24, 2016.

- ❖ Tweakers (2016b), *LinkedIn bevestigt dat logins van 117 miljoen leden in 2012 werden buitgemaakt*, <https://tweakers.net/nieuws/111475/linkedin-bevestigt-dat-logins-van-117-miljoen-leden-in-2012-werden-buitgemaakt.html>, May 19, last consulted: September 28, 2016.
- ❖ Van den Berg, B. and R.E. Leenes (2013), 'Abort, retry, fail: scoping techno-regulation and other techno-effects'. In: Hildebrandt, M., Gaakeer, J. (eds.) *Human Law and Computer Law Comparative Perspectives. Perspectives on Law and Justice* 25, pp. 67–88, London: Springer.
- ❖ Van Eeten, M. and J. Bauer (2013), 'Enhancing incentives for Internet security', in: I. Brown (ed.). *Research Handbook on Governance of the Internet*, Cheltenham: Edgar Elgar, pp. 445-484.
- ❖ Veiliginternetten.nl (2016a), <https://veiliginternetten.nl/uitleg/>; last consulted, July 20, 2016.
- ❖ Veiliginternetten.nl (2016b) <https://veiliginternetten.nl/themes/zakelijk/draadloos-onderweg/>; last consulted, July 20, 2016.
- ❖ Vpncomparison.org (2016), <http://www.vpncomparison.org/country/netherlands/>, last consulted: November 24, 2016.
- ❖ Vpnpick.com (2016), <http://vpnpick.com/best-vpn-netherlands-holland/>, last consulted: November 24, 2016.
- ❖ Yahoo (2016), "Yahoo Data Breach: Stolen Passwords Were Encrypted, but That Doesn't Mean Users Are Safe", September 23, <https://www.yahoo.com/tech/yahoo-data-breach-stolen-passwords-191113081.html>, last consulted: September 28, 2016.
- ❖ Yeung, K. (2012), 'Nudge and fudge', *The modern law review*, 75(1), pp 122-148.
- ❖ Ziggo (2016), Ziggo Wifispots <https://www.ziggo.nl/internet/wifispots/>, last consulted: September 30, 2016.

Interviews

- ❖ ACM, S. Woutersen, Directorate Consumers, Team manager, The Hague, October 12, 2016.
- ❖ Bits of Freedom, R. Zenger, Amsterdam, November 3, 2016.
- ❖ ECP, M. Bonthuis, deputy director, The Hague, October 25b, 2016.
- ❖ Ministry of Economic Affairs, Directorate Telecom Market, R. van der Luit, Head of Policy division, The Hague, October 10, 2016.
- ❖ Ministry of Security and Justice, Directorate Cyber Security, M. van Leeuwen, Head of the Policy division, The Hague, October 19, 2016.
- ❖ Ministry of Security and Justice, National Cyber Security Center, P. Rogaar, Senior Advisor Expertise and Advice, The Hague, May 25, 2016.
- ❖ KPN, O. Koeroo, CISO-office, Senior Policy Advisor, The Hague, September 26, 2016.
- ❖ KPN, O. Zeijpveld, Internet Value Added Services, Commercial Productmanager, The Hague, October 26, 2016.
- ❖ Nederland ICT, R. Corbijn, Advisor public policy and public affairs, The Hague, October 20, 2016.
- ❖ Surfnet, S. Veeke, Project manager Let's Connect / edu VPN, Utrecht, November 1, 2016.
- ❖ VNO-NCW, N. Mallens, Advisor safety and security, critical infrastructure, cybersecurity and sports, The Hague, October 25a, 2016.

Appendix 1: Comparison of costs of mobile subscriptions in the Netherlands

Date of comparison: July 20, 2016

Smartphone for comparison: iPhone 6s space grey 16GB

Subscription form: 2-year subscription, unlimited minutes and SMS, 5GB mobile data (the 'recommended' package by the telecom providers, T-mobile offered 6GB instead of 5GB).

Results: (see screenshots below)

T-Mobile: €53, 50 a month

Vodafone: €54, 00 a month

KPN: €59, 00 a month

https://shop.t-mobile.nl/eca/RAPRD/Apple-iPhone-6s-16GB-Grijs/map6s16gs.html?ab_agid=1

Prive Zakelijk Favonet

Shop Klantenservice Netwerk Telefonisch bestellen 0800 7123 (gratis)

Stel Samen & Stel Bij

Startabonnement

- ✓ Online met een basissnelheid tot 64 Kbps
- ✓ Nooit onverwachte kosten voor mobiel internet
- ✓ Gratis gebeld worden in de EU
- ✓ Onbeperkt SMS in NL en EU

12 mnd **24 mnd**

€ 10,00 /mnd

1 Apple iPhone 6s 16GB Grijs

★★★★★ 57 reviews

DELEN

Kies zelf hoe je voor je telefoon betaalt

Per/mnd	€ 25,00	€ 17,50	€ 7,50	€ 0,00
Enmalig	€ 0,00	€ 164,95	€ 389,95	€ 539,95
Jouw toestelprijs	€ 600,00	€ 584,95	€ 569,95	€ 539,95
Korting	€ 0,00	€ 15,05	€ 30,05	€ 60,05

Of kies een Sim Only >

Direct leverbaar Specificaties Ander toestel >

JOUW BESTELLING

Maandelijkse kosten

Abonnement: Stel Samen & Stel Bij

- Startabonnement 24 mnd € 10,00
- + 6 GB L € 20,00
- + Onbeperkt NL & 120 EU € 10,00
- 24 mnd korting -€ 11,50
- Toestelbetaling /mnd € 25,00

Totaal per maand € 53,50

Enmalig bij bestelling

- Apple iPhone 6s 16GB Grijs t.w.v. € 729,95
- Toestel (i.c.m. abonnement) € 600,00
- 24 x € 25,00 /mnd -€ 600,00
- Enmalige bijbetaling toestel € 0,00
- Thuiskopieheffing € 4,24

Totaal enmalig € 4,24

Enmalige aansluitkosten (op eerste factuur) € 29,95

Naar bestellen

Of bewaar als favoriet >

105% 16:14 20-7-2016

T-Mobile

https://shop.t-mobile.nl/eca/RAPRD/Apple-iPhone-6s-16GB-Grijs/map6s16gs.html?ab_agid=1

https://www.vodafone.nl/shop/mobiel/pakket/?package_id=null

Vodafone Libertel B.V. [NL]

Jouw pakket ✓ iPhone 6s 16GB Space Grey

Red ✓ en bekijk daarna je pakket

Bekijk je pakket en kies hoe je wil betalen

Verlengen? Verleng nu en krijg 3 maanden TV Anywhere, Netflix of Napster cadeau

Verleng via My Vodafone

Overzicht

Stap 1: Kies hoe je voor je telefoon wilt betalen

iPhone 6s 16GB Space Grey € 24 p.mnd. looptijd 2 jaar

Op voorraad [Bekijk de details](#) >

eenmalige betaling: € 0,00
totale kosten toestel: € 576,00

Toestelprijs icm Red van € 576
Jouw voordeel t.o.v. losse toestelprijs € 183

	Eenmalige betaling	Toestel per maand
<input checked="" type="checkbox"/>	€ 0,00	€ 24,00
<input type="checkbox"/>	€ 96,00	€ 20,00
<input type="checkbox"/>	€ 192,00	€ 16,00
<input type="checkbox"/>	€ 288,00	€ 12,00
<input type="checkbox"/>	€ 384,00	€ 8,00
<input type="checkbox"/>	€ 504,00	€ 3,00
<input type="checkbox"/>	€ 576,00	€ 0,00

Overzicht

iPhone 6s 16GB Space Grey
In combinatie met:
Red 2 jaar

Maandelijkse kosten

Kosten abonnement € 30,00
Kosten telefoon € 24,00

Eenmalige kosten

iPhone 6s 16GB € 0,00
Thuiskopieheffing [Meer over](#) € 4,24
[Thuiskopieheffing](#)
Aansluitkosten
De aansluitkosten betaal je via je eerste telefoonrekening € 25,00

Totale kosten

Per maand € 54,00
Eenmalig nu € 4,24
Eenmalig via je eerste rekening € 25,00

[Naar winkelwagen](#)

Stap 2: Je gekozen abonnement

Red 5 GB internetten
Onbeperkt bellen en sms'en
[Kies voor een Sim Only](#) >

1 jaar 2 Jaar
€ 30 p.mnd. looptijd 2 jaar

95%

NL 16:18 20-7-2016

Vodafone

https://www.vodafone.nl/shop/mobiel/pakket/?package_id=null

https://mobiel.kpn.com/nieuwe-klant/bestellen/jouw-gegevens/handset/apple-iphone-6s-16gb-space-gray/zorgeloos-standaard

Jouw gegevens

E-mailadres

Herhaal e-mailadres

Nummerbehoud ?
Je kan nummerbehoud aanvragen vanaf 60 dagen voor het einde van je huidige contract. Na je bestelling kun je heel makkelijk online je gegevens voor nummerbehoud achterlaten. Zoals de gewenste startdatum van je abonnement. KPN zorgt er verder voor dat je nummer succesvol wordt overgenomen.

Ik wil mijn nummer behouden Ik wil een nieuw nummer

Belangrijk
Neem je voorletter(s) en achternaam exact zo over zoals die in je legitimatiebewijs staan vermeld.

Aanhef
 De heer Mevrouw

Voorletter(s) Tussenvoegsel


Achternaam

Geboortedatum
DD-MM-JJJJ (bijv. 25-06-1988)
 - -

Postcode

Huisnummer Toevoegen

Overzicht van je bestelling

Toestel
 **Apple iPhone 6s 16GB Space Gray**

Maandelijkse kosten

Zorgeloos Standaard € 64,00

- Onbeperkt bellen en smsen
- 5 GB mobiel internet
- 2-jarig contract

Korting zolang je abonnement loopt **- € 5,00**

Totaal per maand € 59,00


Aansluitkosten eenmalig via 1e factuur **€ 30,00**
Thuiskopieheffing eenmalig via 1e factuur **€ 4,23**

Eenmalige kosten bij bestelling

Apple iPhone 6s 16GB Space Gray € 29,00
t.w.v. € 732,00

Totaal eenmalig € 29,00

Prijzen zijn incl. BTW

 Hulp nodig bij bestellen?
24 uur / 7 dagen per week
Bel gratis 0800 2626253

Feedback

100% 16:47 20-7-2016

KPN

<https://mobiel.kpn.com/nieuwe-klant/bestellen/jouw-gegevens/handset/apple-iphone-6s-16gb-space-gray/zorgeloos-standaard>

Appendix 2: Search for information on VPN on sites telecom providers

Date of search: October 26, 2016

Providers: T-Mobile, Vodafone and KPN

Method used: search on homepage of providers for 'VPN'. If specific article on VPN for consumers was found: analysis of the article. If no specific article on VPN for consumers was found: analysis of the type of search results with consultation of at least three of the search results. See the screenshots below. If an analysis was conducted on search results, then a screenshot is included of only the first page of the search results.

Results of the search:

T-Mobile:

No specific articles on VPN for consumers. With one exception all search results led to forum posts of users asking connectivity questions about various devices and in various situations. The search result not related to a forum post was a press statement from February 2016 that T-Mobile is supplying the service for the business application of VPN for the employees of the TU Eindhoven and TU Twente for remote access to the business network.

Vodafone:

No specific articles on VPN for consumers. Most search results led to articles on business services that Vodafone offers in which VPN is a feature. The second type of search results led to installation manuals of a number of modems.

KPN:

A specific article was found containing VPN for consumers. Information on VPN was part of an article on protective cybersecurity measures consumers can take. A specific VPN-provider was mentioned.

Zoeken op T-Mobile

https://www.t-mobile.nl/zoeken?q=vpn§ion=Particulier&p=1

Privé Zakelijk

Shop Klantenservice Netwerk

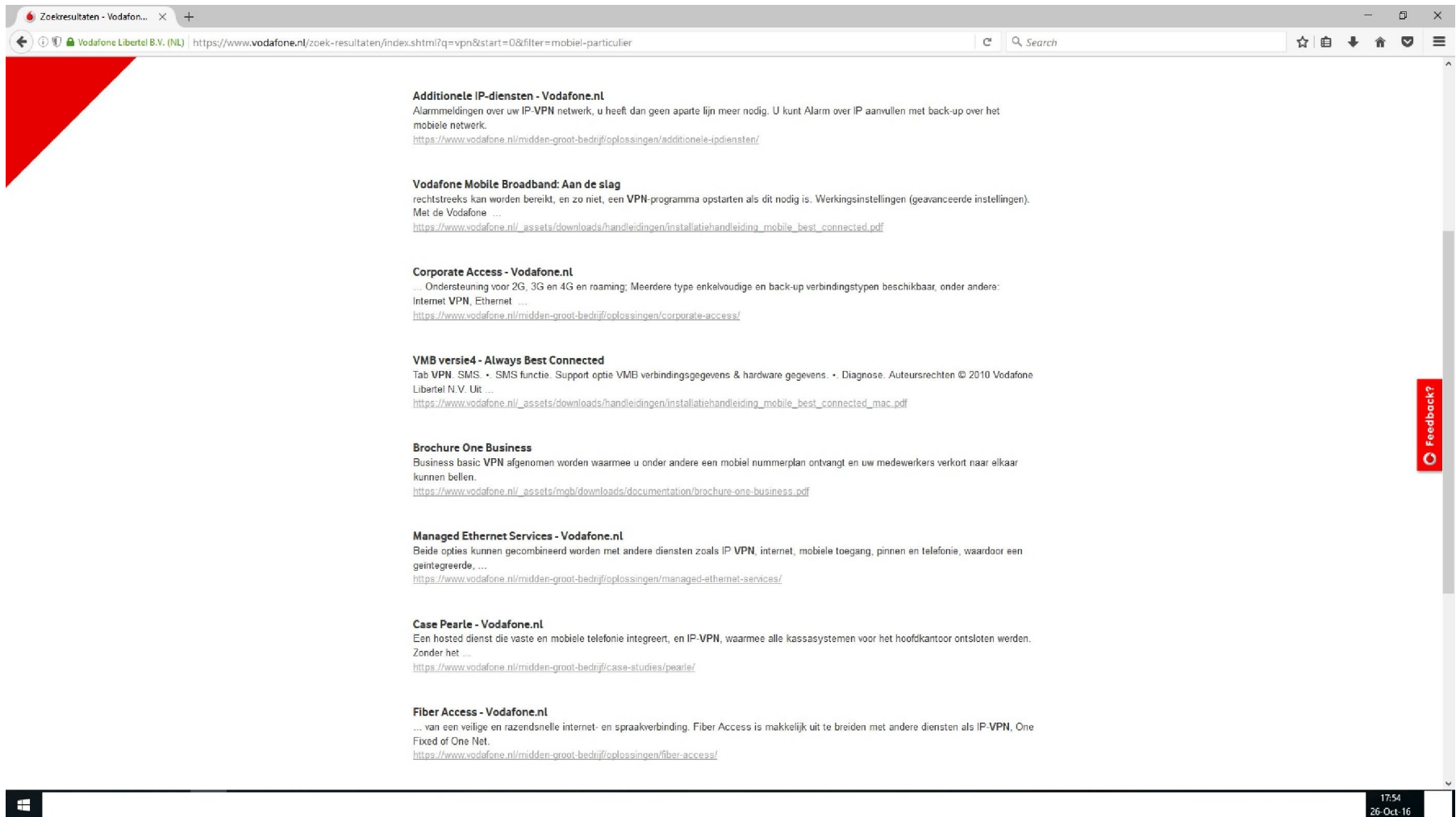
vpn My T-Mobile

- Samsung s5 VPN e-mail verzenden**
Sinds enkele dagen werk ik met een VPN van privateinternetaccess. ... of Een vraag stellen. Beantwoord: Samsung s5 VPN e-mail verzenden. ...
Forum
- Navigon verdwenen na ios-update**
... Ik had eerder VPN Hotspot Shield en toen werkte het goed. ... Vandaag heb ik VPN helemaal uitgeschakeld en Navigon opgestart zonder Wifi. ...
Forum
- Datavrije Muziek**
... tablet. Werkt Datavrije Muziek in combinatie met VPN? Nee, met een VPN-verbinding werkt Datavrije Muziek niet. Aanvullende ...
Shop
- TU Eindhoven en Universiteit Twente kiezen voor T-Mobile ...**
... Medewerkers (3500 gebruikers van UT en 3000 gebruikers van TU/e) hoeven dan geen aparte VPN-verbinding op te zetten of opnieuw op het wifi ...
Persberichten
- BB boid 9780 internet probleem**
... wand ik wil alles doen via WIFI maar dat werkt ook niet kunt u mij helpen mail dan [email]@hetstartpunt.com/email] of reageer PS VPN apn dat ...
Forum
- Wifi in de trein**
... Dat laatste is niet voldoende om een betrouwbare VPN verbinding met het netwerk van mijn werkgever op te kunnen zetten. ...
Forum
- Vragen/problemen iPhone (deel 2)**
... 2 dataroaming staat uit 3 WIFI staat uit 4 VPN heeft geen verbinding. ... 2 dataroaming staat uit 3 WIFI staat uit 4 VPN heeft geen verbinding. ...
Forum
- na een update wel wifi maar geen 3g meer htc wildlife**
goede middag, ik heb een update gehad/ uitgevoerd op mijn htc wildlife, nu heb ik wel wifi maar geen 3g meer, mijn apn lijst en vpn lijst zijn door. ...

17:49
26-Oct-16

T-Mobile

<https://www.t-mobile.nl/zoeken?q=vpn§ion=Particulier>



Vodafone

<https://www.vodafone.nl/zoek-resultaten/index.shtml?q=vpn>

Instellen internetbeveiliging

kpn-customer.custhelp.com/app/answers/detail/a_id/17197/~/instellen-internetbeveiliging

kpn Mobiel TV, Internet & Bellen Speciaal voor klanten

Zoeken naar... Webmail

- Installeer alleen apps via de officiële appstores.

Instellen internetbeveiliging draadloos netwerk

Maak je gebruik van een draadloos netwerk dan is het belangrijk dat je deze verbinding goed beveiligd. Zo voorkom je dat anderen gebruik kunnen maken van jouw internettoegang of via deze verbinding kunnen inbreken in je computer.

Wat kun je zelf doen om een draadloos netwerk veilig te gebruiken:

- Beveilig de KPN Experia Box (de modem) met een ander wachtwoord dan het wachtwoord dat je standaard bij aanschaf van je draadloze modem hebt ontvangen (fabriekswachtwoord). Raadpleeg de [handleiding](#) van je modem voor het wijzigen van het wachtwoord.
- Beveilig je draadloze netwerk door de draadloze netwerknaam (SSID) en je beveiligingsleutel (WPA/WPA2) in te stellen. Volg de [instructievideo](#) voor het instellen van de netwerknaam en beveiligingsleutel.

Instellen internetbeveiliging open KPN WiFi HotSpot

Wat kun je zelf doen om KPN WiFi Hotspot veilig te gebruiken:

- Gebruik voor het internetten op [KPN WiFi Hotspots](#) de KPN WiFi app op je smartphone of tablet. Zo ben je ervan verzekerd dat je met het juiste netwerk verbonden bent. Download de app voor iOS, Android of Windows Phone door op 'KPN WiFi' te zoeken in de appstore.
- Zorg dat je altijd de laatste updates van je besturingssysteem en apps hebt geïnstalleerd op je laptop, tablet of smartphone. Dan zijn de beveiligingsinstellingen ook altijd up to date.
- Internetbankieren en webmail verlopen via een beveiligde verbinding. Controleer altijd of er 'https' in de adresbalk staat voor de website.
- Gebruik een goede firewall en virusscanner op je laptop, tablet of smartphone. Bijvoorbeeld het [KPN Veilig pakket](#).
- Maak je gebruik van KPN mail via de Hotspots van KPN WiFi, pas dan je [instellingen](#) aan zodat je e-mail altijd via een beveiligde verbinding gebruikt.
- Maak gebruik van [VPN software](#) om veilig te internetten, zeker als je vertrouwelijke zaken wilt uitvoeren op openbare WiFi netwerken. Om gebruik te maken van een VPN verbinding kun je apps gebruiken, zoals [F-Secure freedom VPN](#).

Uitkomst

- Je weet wat je zelf kunt doen om je internetverbinding van je PC, Mac, tablet of smartphone te beveiligen.
- Je weet hoe je de internetverbinding van je draadloos netwerk kunt beveiligen.
- Je weet hoe je veilig kunt internetten via een open KPN WiFi Hotspot.

Gerelateerde informatie

- [Productinformatie: KPN Veilig pakket](#)
- [Wat doet het KPN Abuse team](#)
- [Handleidingen en software die bij jouw producten en/of diensten van KPN horen](#)

17:39
25-Oct-16

KPN

http://kpn-customer.custhelp.com/app/answers/detail/a_id/17197/~/instellen-internetbeveiliging

Appendix 3: overview of empirical research through interviews

For the semi-structured interviews with policy stakeholders the list of questions underneath was used as a guideline. Some interviews had additional questions concerning the specific perspective or role of the organization. For instance, the ministry of Economic Affairs was asked for their view on the telecom market in order to confirm the desk research. Nederland ICT was asked about their view on the market for VPN-providers to confirm the desk research. The interview with the technical expert of the NCSC was an unstructured interview to confirm the technical working of VPN found through desk research and to find additional relevant technical aspects of VPN. The interview with the business unit of KPN focused primarily on the question what the elements would be of a business case of VPN for consumers and how important certain elements are for a business decision. The interview with Surfnet focused on gaining more insight into the Let's Connect initiative, what the initiative contains, which organizations participate/fund the initiative and with which organizations the initiative cooperates and how.

Interview questions for policy stakeholders:

General questions

1. Has this organization previously considered the topic/service VPN for consumers? Yes/no and why?
2. How does the organization look at the current and hypothetical situation of VPN as a standard service for consumers?

Industry self-regulation

3. What do you think of the proportionality of this government strategy?
4. To what extent do you think this government strategy will achieve the goal of the hypothetical end-state as VPN as a standard service for all consumers?
5. How do you look at the impact on the level-playing field in the market with this government strategy?
6. What level of buy-in do you think that stakeholders will have for this government strategy?
7. What do you think the amount of time this strategy will take?
8. How do you think the costs and benefits are divided and who will pay?

Legislation

9. What do you think of the proportionality of this government strategy?
10. To what extent do you think this government strategy will achieve the goal of the hypothetical end-state as VPN as a standard service for all consumers?
11. How do you look at the impact on the level-playing field in the market with this government strategy?
12. What level of buy-in do you think that stakeholders will have for this government strategy?
13. What do you think the amount of time this strategy will take?
14. How do you think the costs and benefits are divided and who will pay?

Co-regulation

15. How do you think co-regulation would look in this case?
16. Would it fall under a legal norm such as the duty of care?
17. How do you think this strategy would be different from the two previous strategies?

(If applicable and different from any of the previous strategies)

18. What do you think of the proportionality of this government strategy?
19. To what extent do you think this government strategy will achieve the goal of the hypothetical end-state as VPN as a standard service for all consumers?
20. How do you look at the impact on the level-playing field in the market with this government strategy?
21. What level of buy-in do you think that stakeholders will have for this government strategy?
22. What do you think the amount of time this strategy will take?
23. How do you think the costs and benefits are divided and who will pay?