Regis University

ePublications at Regis University

Regis University Student Publications (comprehensive collection)

Regis University Student Publications

Fall 2010

# Deep Packet Inspection and its Effects On Net Neutrality

Michael A. DeRose
*Regis University*

Follow this and additional works at: https://epublications.regis.edu/theses

Part of the Computer Sciences Commons

## Recommended Citation

DeRose, Michael A., "Deep Packet Inspection and its Effects On Net Neutrality" (2010). *Regis University Student Publications (comprehensive collection)*. 355.
https://epublications.regis.edu/theses/355

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

**Regis University**
College for Professional Studies Graduate Programs
**Final Project/Thesis**

# Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

**DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NEUTRALITY**

A THESIS

SUBMITTED ON TWENTY SECOND OF OCTOBER, 2010

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

INFORMATION TECHNOLOGY MANAGEMENT

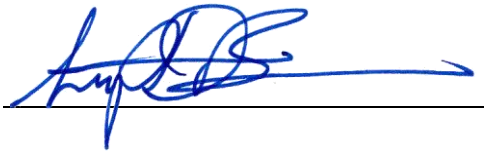
BY

Michael A. DeRose

APPROVALS

Ernest Eugster, Ph.D., Thesis Advisor

Shari Plantz-Masters



Stephen D. Barnes

**Abstract**

Deep packet inspection (DPI) is becoming increasingly important as a means to classify and control Internet traffic based on the content, applications, and users. Rather than just using packet header information, Internet Service Providers are using DPI for traffic management, routing and security. But by being able to control traffic by content, a growing number of public policy makers and users fear ISPs may discriminately charge more for faster delivery of their data, slow down applications or even deny access. They cite such practices as endangering the principle of net neutrality; the premise that all data on the Internet should be treated equally. The existing literature on DPI and net neutrality is sizeable, but little exists on the relationship between DPI and net neutrality. This study examines the literature, develops a research methodology and presents results from a study on the challenges of DPI in regards to privacy and net neutrality. The findings show that although most users are unaware of DPI technology, they feel strongly that it places their privacy at risk.

**Acknowledgements**

I would like to thank my fellow students, the faculty of Regis University and all those that have made this culmination of my education possible. I have been privileged to have had some great cohorts on this journey and I am thankful for the contributions, discussions, arguments and revelations that would not have been possible without your support. Additionally, I would like to thank my Thesis Advisor, Dr. Ernest Eugster whose tireless efforts kept me on target and track.

I would also like to thank my friends, family and coworkers that stepped up and supported me by participating in the longest survey ever composed. In particular, I would like to thank Timmy Harper for his tireless efforts in taking the survey. My sincere thanks also go out to my children, Sofia and Conner for putting up with Daddy being grumpy, busy and generally unavailable afterhours for the past six years. Well, Daddy is done and I promise that it was all worth it! Most importantly, I would like to thank my wife, Jodee, for her patience, her wisdom, her guidance and her never ending support on my journey to complete my education. Without her help and innumerable sacrifices, this would not have been remotely possible.

## Table of Contents

**Abstract** ..... **i**

**Acknowledgements** ..... **ii**

**Table of Contents** ..... **iii**

**List of Tables** ..... **v**

**Chapter 1 - Introduction** ..... **1**

1.1 Deep Packet Inspection, Technology and Net Neutrality ..... 1

1.2 Statement of Problem ..... 4

1.3 Statement of Goals and Objectives ..... 4

1.4 Project Description ..... 5

1.5 Summary ..... 6

**Chapter 2 - Literature Review** ..... **7**

2.1 Deep Packet Inspection ..... 7

2.2 Traffic Shaping ..... 9

2.3 Deep Packet Inspection Devices ..... 10

2.4 Benefits of Deep Packet Inspection ..... 11

2.5 Net Neutrality.....12

2.6 Summary.....14

**Chapter 3 - Methodology.....15**

3.1 Ontology…….....15

3.2 Questions and Survey.....16

3.3 Summary....…….....17

**Chapter 4 – Data Analysis and Findings.....18**

4.1 Background Information.....18

4.2 Privacy and Content.....22

4.3 Regulation.....26

4.4 Trust and Moral Obligations .....28

4.5 Privacy of Communications.....30

4.6 Summary.....31

**Chapter 5 – Discussion and Conclusions.....32**

**References .....34**

**Appendix A – Survey Questions .....36**

**Appendix B – Survey Results .....44**

## List of Tables

Table 1. Which Best Describes Your Background?..……..... 19

Table 2. Background Knowledge Questions (All Participants).....19

Table 3. Background Knowledge Questions (IT Field Only).....20

Table 4. Background Knowledge Questions (Non-IT Field Only).....22

Table 5. Examination of Network and Telephone Communications.....23

Table 6. ISPs Should Be Allowed to Deny or Delay Communications.....24

Table 7. Telephone Deny or Delay Communications.....24

Table 8. Premium Content, Premium Fees? .....25

Table 9. To Regulate or Not to Regulate? .....26

Table 10. Government Regulation? .....27

Table 11. Standards Agency Regulation? .....28

Table 12. Moral Obligations? .....29

Table 13. Trusted Providers. .....29

Table 14. Privacy of Communications.....30

# Chapter 1 – Introduction

For decades, ISPs have been managing and routing traffic based on packet header information. DPI, however, has emerged as a critical traffic management tool and is the subject of this research. By being able to control traffic based on content, in addition to header information, DPI offers ISPs improved traffic management and routing as well as security. But having ISPs controlling traffic content has lead to increasing public debate. The opposing sides of the net neutrality debate argue that without safeguards in place, ISPs would cut lucrative deals to prioritize some kinds of content and throttle others, turning themselves into the unofficial gatekeepers of the world's best leveling force. ISPs argue that practices such as tiered-pricing are needed to ensure continued investments in Internet infrastructure.

This chapter introduces DPI and the concept of net neutrality. It identifies how the technology works and the challenges it can present to net neutrality. The chapter also describes the goals of the research and the research methodology used.

## 1.1 Deep Packet Inspection Technology and Net Neutrality

Deep packet inspection takes the process of inspecting the origin and destination of packets and expands it to examine the actual data being sent. This technology allows Internet Service Providers (ISPs) and network administrators the ability to filter data transmissions by denying, delaying or giving precedence to certain types of data.

Historically, packet inspection occurred at the network layer which was dependant upon the header and footer information contained in packets to determine routing and filtering options. Deep packet inspection came about as a means to enhance the process to include the data that was once only accessible in the application and presentation layers of the OSI model. Access to the presentation and application layer information at the network layer, allows for packet filtering to be implemented based on the actual data, not header information. The ability to filter data at the lower layers allows ISPs to circumvent any header information and route packets based on what the payload contains.

As the type, contents, the destination and any digital signatures of the data can be identified, deep packet inspection can provide many benefits for ISP environments. Kumar (2006) identified three popular applications of DPI:

- Content-based traffic management and routing, where packets are classified and processed based upon content.
- Network intrusion detection systems (NIDS) generally scan the packet header and payload to identify a given set of signatures of well known security threats.
- Layer 7 switches and firewalls provide content-based filtering, load-balancing, authentication and monitoring.

By applying content-based traffic management, ISPs can give priority to traffic based on the type of content being sent, guaranteeing enhanced delivery for premium content providers. Network intrusion detection systems (NIDS) utilize DPI to examine the content of packets and compare the digital signatures to a database of known threats, discarding transmissions that pose security risks. DPI also enables layer 7 switches to become application aware. This awareness

gives application layer switches the ability to filter traffic based on the type of application. This provides ISPs with a scalable and efficient traffic management option.

Such applications and benefits can provide ISPs an important competitive advantage. Stallings (2007) observed that many opportunities exist for companies to use differentiation as a strategy to create competitive advantages. Today's networks can offer differing levels of quality of service (QoS), which include specifications for maximum delay and minimum throughput. They also provide a variety of customizable services in the network management and security arenas. Deep packet inspection can provide the differentiation that will help ISPs offer a wide array of services with guaranteed QoS levels. These services and guarantees are possible because DPI allows network traffic to be manipulated with intimate knowledge of the data being sent.

Net neutrality enters the picture as the movement to keep the flow of information free. Free access to content, the ability to connect with any device or run any application is what has made the Internet so popular and useful. This openness is the heart of innovation that has driven the rapid growth of the Internet and to deny any content, applications or devices would be stifling. Net neutrality is the process of keeping the Internet open and freely available to all users, devices and content.

Net neutrality began as an information revolution to help guide Internet policies as they were being formed. Since 1930, the United States communication networks have been governed by non-discrimination policies like net neutrality. Older regulations focusing on telephone communications still have their place, but updated regulation aimed at Internet communications should be addressed (Schahczenski, 2008).

Congressional debate on net neutrality heated up in 2005 and the debate still continues. Initially, Congress had focused on video franchising, attempting to revamp the laws to allow phone companies to compete in the video space. Once the legislation progressed, net neutrality as a whole was addressed and some minimal progress was achieved. Although a recent bill was withdrawn, Congress continues the debate.

By giving ISPs the ability to discriminate packets based on content or premium access, only ideas or services backed by a significant funding or offered by ISPs would flourish. Although the technology allows for safer, more scalable and more controllable networks, DPI raises serious concerns about privacy and net neutrality.

**1.2 Statement of Problem**

The problem under investigation in this study focuses on the threats that deep packet inspection can pose to net neutrality.

DPI gives ISPs the ability to manipulate and inspect every bit of data sent over their networks and this does not sit well with pundits for net neutrality. The ability to throttle services, divvy out bandwidth and even reject contents of information traversing the network goes against the philosophy of a Free Internet.

**1.3 Statement of Goals and Objectives**

Using data from a survey of Internet users, this study has three goals. The first objective of the study is to determine the risks that DPI poses to net neutrality. To reach this objective, a survey was conducted of Internet users. The results of the study revealed that most users are not aware their privacy may even be compromised and that IT industry insiders appear largely in the dark with regards to network monitoring capabilities. ISPs have always been able to challenge

the free flow of information, but deep packet inspection allows them to do so with frighteningly intrusive means.

A second and more general objective is to add to the body of knowledge. Considerable literature on DPI exists, but it is largely focused on technical issues and case studies. The existing literature on net neutrality is also sizable. But there exists little technical description on how ISPs use DPI for monitoring and control. The study has emerged from this researcher's belief that the coupling of DPI technology and its net neutrality context has not been well explored.

Third, this researcher hopes that this study will result in informed public debate. By discussing the technology behind deep packet inspection and mapping that to the affects it can have on privacy and a free Internet, this study attempts to educate the general user on challenges of DPI to network neutrality.

**1.4 Project Description**

To reach these goals, the research proceeded in three phases. In the first phase, this researcher reviewed the existing literature, both in DPI and in net neutrality. The literature is vast, yet weighs heavily to technical descriptions and public policy debate. This paper attempts to redress this imbalance by examining and integrating DPI's role in endangering net neutrality. The literature review also provided a better definition of guidelines for exploration, especially in phases of question generation and survey phases.

In the second phase, specific questions were generated. Should ISPs be allowed to examine the content of network communications? Should they be allowed to deny or delay communications based on the type of content being sent (e.g., music, text, video)? Should they be allowed to deny or delay communications if the content is business versus personal? To

answer these questions, a survey represented the most appropriate research method to verify the knowledge and attitudes of the general Internet population. These questions were grouped to determine specific types of information. The first group was participant background information, followed by Internet communication questions, phone communication questions and finally privacy questions.

In the third phase, the survey targeted general Internet users. The sole criterion was that the participant had to have a working Facebook profile. This tactic was selected for a few reasons. First, through the popularity of Facebook, the rate of response was hoped to be adequate for the study (67, or 33% out of 200 responded to the invitation posted to Facebook). Second, by only querying active Facebook users, the respondents were guaranteed to be Internet users. Lastly, Facebook provided a medium other than email to communicate the invitations to participate in the study. It is this researcher's belief that had email been employed, the rate of response would have been drastically reduced.

The researcher felt this approach would be more rewarding than interviewing ISPs. One of the fundamental questions in the net neutrality debate is how much ISPs should be allowed to discriminate packets traversing their networks. As the debate rages on, the argument gets sidetracked with semantics. ISPs argue that they have the right to manage traffic on their networks, users and content providers argue that while it is acceptable for ISPs to manage traffic, it is not within their rights to block or delay any traffic. By focusing the study on users, the researcher hoped to avoid the black hole of the semantic argument.

**1.5 Summary**

Deep packet inspection provides many benefits to ISPs. But it can also adversely affect privacy. After laying the foundation for the technology and its benefits, the problem of net

neutrality and a free Internet were discussed. Also, due to the lack of substantial literature on the specific impacts of DPI on privacy and net neutrality, it was necessary to generate a study surrounding the issue from the end user's point of view. It is these competing factors that combine to formulate the need for further research and education on the topic. Finally, the chapter concluded by showing research method used.

The next chapter presents a review of the literature on DPI and net neutrality.

## Chapter 2 –Literature Review

This chapter delves deeper into literature on deep packet inspection and net neutrality. There is considerable literature on DPI, but it is limited to engineering issues and case studies. The literature on net neutrality is also vast, but little exists on how DPI poses a threat to privacy. This research attempts to fill this gap.

### 2.1 Deep Packet Inspection

A number of researchers have examined DPI technology. Hills (2006), for example, stated that DPI devices can operate on layers two through seven of the Open Systems Interconnect (OSI) model.

Deep packet inspection is packet filtering that inspects the data payload of an IP packet. DPI devices take deep looks into the data of each packet and either allows or denies passage according to some set of predetermined rules. Smith (2008) noted that as networks incorporate increasingly sophisticated services into their infrastructure, DPI uses application-specific data found in packet payloads to make routing decisions, to block or rate-limit unwanted traffic, to perform intrusion detection, and to provide quality of service.

The DPI inspection engine parses each packet and compares the contents against its rule set. This rule set is comprised of known electronic signatures of content which allow

identification of the packet's data. In the past, network packets were classified by their headers, but DPI now allows them to be classified by the actual content of their payloads.

To perform this functionality, DPI devices rely on a database of application signatures that are crosschecked against to determine the nature of the packet traversing the network. The DPI device groups the packets by protocol and security levels then processes the packets by "performing application level checks as well as stateful inspection" (Ranum, 2005). DPI devices look for any anomalies in the packets based on their know application signatures. If any packet is deemed out of the ordinary, it is not allowed to pass. An example would be the order in which commands are given for a certain protocol. An application will always order commands in the same sequence, where as a human attempting to hack into a system might issue the commands in some random order. By inspecting the packet for its application signature, then comparing that signature against known parameters, DPI devices can thwart attacks that would have gotten past traditional packet inspection principles.

Normally, DPI is used to monitor and shape IP traffic. ISPs can use DPI to monitor the type of traffic on their networks and give priority to the protocols they deem more important. This type of traffic shaping can slow down less important protocols, while not entirely cutting of access to the particular service.

Deep packet inspection does come with a heavy cost on the processing and bandwidth sides of the equation. To perform such a thorough look at each individual packet traversing a network, while keeping the throughput speed at normal levels, is quite a challenge. Becchi (2007) and Kumar (2006) showed that advanced algorithms are needed to enhance DPI's ability to meet the challenge. They argued the processing bottleneck is a result of the speed in which comparisons between known electronic signatures and quickly moving data occurs. As the data

is moving at ever increasing speeds, it is necessary for the processing to increase at the same rate as the bandwidth. Not until recently have DPI device vendors been able to come close to real-time DPI for mass market consumption. Even then, the financial costs can be prohibitive. Anderson (2007) noted that "...top-of-the-line products can set you back several hundred thousand dollars, but some of them can inspect and shape every single packet—in real time—for nearly a million simultaneous connections while handling 10-gigabit Ethernet speeds and above." The processing power needed to make DPI successful at real time speeds has been the major roadblock to widespread adaptation of the technology.

Along with throughput concerns comes the fact that DPI devices depend upon software to match, categorize, interpret and finally decide which packets are allowed to pass. As with any software, there are bound to be some cases of vulnerability. According to Porter (2005), Remote Procedure Call (RPC) attacks, stack overflow attacks, buffer overflow attacks, VoIP command processing vulnerabilities and H.225 messages over TCP are all cases of known DPI vulnerabilities. Even though DPI provides a robust manner in which to monitor network communications, it is an evolving technology.

**2.2 Traffic Shaping**

Traffic shaping is defined as, "the appropriate allocation of bandwidth to support application requirements" (Goldman, 2004). This boils down to ISPs ranking network traffic and throttling bandwidth in accordance to the ranking. The rankings can be based on several different factors, such as service level agreements, types of traffic, application requirements and performance considerations.

Shaping network traffic is accomplished by either controlling the pace of the data or by queuing the data for a timed release. These two methodologies can also be combined to further control or shape the traffic as it travels over a network. Georgiadis (1996) stated that "Reshaping makes the traffic at each node more predictable and, therefore, simplifies the task of guaranteeing performance to individual connections; when used with a particular scheduling policy, it allows the specification of worst case delay bounds at each node. End-to-end delay bounds can then be computed as the sum of the worst case delay bounds at each node along the path." This is analogous to an interstate highway at rush hour. Traffic flows in the main lanes, while stop lights queue on ramp traffic to enter the interstate in a staggered fashion. All the while, the carpool lane is comfortably cruising at above average speeds.

**2.3 Deep Packet Inspection Devices**

DPI devices are a combination of previous filtering technology with deep packet inspection functionality. Stateful inspection, packet sniffing and firewall technology work in concert with the DPI database to perform network monitoring and traffic shaping on a level that has not previously been attainable. As speeds and functionality improve, deep packet inspection will become embedded within the network core.

Several flavors of deep packet inspection devices exist, but devices are mainly found in the form of hardware firewalls. The main consideration with DPI devices is the throughput in which they can operate. Deep inspection of packets is expensive in terms of processing and memory overhead. Porter (2005) stated that "searching through the payload for multiple string patterns within the data stream is a computationally expensive task. The requirement that these searches be performed at wire speed adds to the cost."

**2.4 Benefits of Deep Packet Inspection**

Deep packet inspection can provide many benefits for corporate and ISP environments. The addition of a DPI to a network monitoring portfolio can help to bolster the services and security provided by their respective networks. Increased service levels can be attained by utilizing content-based traffic management while increased understanding and control of their networks will help to cut operating and capital expenditures. Application aware switches can provide increased load balancing, authentication and monitoring capabilities. In addition to increased service levels and more control, DPI can help ISPs secure their networks by implementing network intrusion detection systems based on electronic signatures of well known threats.

Previous network monitoring devices only gave the network administrators an overview of bandwidth, services and the destination of network traffic. By adding DPI functionality, network monitoring takes a step up to the next level. Companies will be able to stop many network attacks in their tracks. Combining existing intrusion prevention technology with the additional filtering of DPI devices will allow for networks to identify and prevent many attacks that currently are able to bypass today's prevention measures. ISPs will be able to shape their bandwidth to better serve their customers most critical needs. DPI will allow them to throttle services at peak usage times to better accommodate the needs of their customers. While a DPI device is in use, ISPs and corporations will gain a deeper understanding of what their networks are actually being used for. This greater level of knowledge will allow them to focus on specific areas of need and not waste time or expense on areas that are performing up to par. As a result of a more controlled network, companies can focus on additional services and offerings that will help to generate additional opportunities for revenue generation. Hill (2006) wrote that "Once

ISPs have networks under better control, it is time to look into how to extract additional revenue streams, and DPI can be leveraged to create additional tiers of service."

**2.5 Net Neutrality**

The advent of inspecting the data payloads of packets traversing the network is a powerful tool which can help better manage traffic, increase security, and shape usage. The ability to inspect the data portion of IP packets, however, poses challenges to net neutrality.

What is net neutrality? Jordan (2009) defined net neutrality as, "the idea that Internet users are entitled to service that does not discriminate on the basis of source, destination, or ownership of Internet traffic." The implications of net neutrality are vast and it is getting attention. For example:

- Google and Verizon released their joint policy proposal aimed preserving the openness of the Web, but exempting net neutrality regulation to the mobile industry (Krigman, 2010).
- The FCC now requires ISPs to treat lawful content, applications, and services in a nondiscriminatory manner (Feldman, 2010).
- Congress was debating the Waxman Net Neutrality Bill, requiring ISPs to follow the basic principles of the "open internet" advocated by net neutrality supporters, including bans on the blocking of unreasonable interference with lawful content, applications, services and devices. The bill has since been dropped, but it is evidence that net neutrality continues to be a hot topic (Kennedy, 2010).

One of the main drivers for net neutrality was to prevent ISPs and backbone network providers to charge more for specific types of network traffic (Economides, 2008). This differentiation of network communications is greatly enhanced by devices that can peer deep into the payload of network communications and report the type and content of the data being

transmitted. Jordan (2009) wrote that advocates of net neutrality want to prohibit discrimination of Internet communication by ISPs based on dedicated bandwidth or improved QoS. He argues that these discriminations could result in outright blocking of sites or content types which could result in a decrease in innovation and development. Jordan contends that dedicated bandwidth and improved QoS as a result of priority access offerings should not be allowed due to the restrictive costs imposed by ISPs for these premium services.

Those against net neutrality argue that free market forces and competition will be sufficient regulation of ISPs, as any official regulation will hinder ISPs ability to fund infrastructure improvements (Jordan 2009). It is an age old argument, free market versus regulation, but in this case DPI devices provide the ability that oversteps the boundaries of network performance and encroaches on basic rights of free speech. As such, net neutrality is one of the main arguments against increased use of DPI.

When asked about how concerned he was about Internet companies using his bandwidth, AT&T CEO Ed Whitacre stated, “How do you think they’re going to get to customers? Through a broadband pipe. Cable companies have them. We have them. Now what they would like to do is use my pipes free, but I ain’t going to let them do that because we have spent this capital and we have to have a return on it. So there’s going to have to be some mechanism for these people who use these pipes to pay for the portion they’re using. Why should they be allowed to use my pipes? The Internet can’t be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts!” (Economedies 2008).

The ability of ISPs to track, monitor and thoroughly log the data being sent over their networks, raises important ethical questions. Is it even ethical to parse through data being sent

via network communications? Surely a private corporation is well within its rights to monitor data transmitted by its employees, but is it right for an ISP to log the data sent by its customers? Proponents of net neutrality also raise issues with ISPs throttling back services or charging extra for those that utilize higher bandwidth or services that are deemed less than critical. Deep packet inspection and subsequent logging of the mined data are tantamount to bugging your phone line, and in fact could be exactly that in the case of voice over IP (VoIP) communications (Renals, 2009). Throw in government monitoring of private citizens and DPI gives ISPs the technology to comply with government surveillance initiatives. "Although the technology isn't yet common knowledge among consumers, DPI already gives network neutrality backers nightmares and enables American ISPs to comply with Commission on Accreditation for Law Enforcement Agencies (CALEA) (government-ordered Internet wiretaps) reporting requirements" (Anderson, 2007).

**2.6 Summary**

This chapter focused on the technology of deep packet inspection, the devices that employ the technology and the different ways it is used. It also examined the principles behind net neutrality and how DPI is at odds with a free Internet. Deep packet inspection can come in many forms, and provide great functionality, but it also gives ISPs the means to threaten net neutrality.

# Chapter 3 – Methodology

This research proceeded in three phases. The first step was to gather the academic literature on net neutrality and deep packet inspection to identify any gaps in knowledge. The results of this phase formed the basis of Chapter 2. The second phase developed questions based on the identified gaps in the knowledgebase. In phase three, the survey was conducted to quantify the assertions made in the first two phases.

## 3.1 Ontology

While most of the technological facts about the benefits of deep packet inspection are empirical, or fact based, the main focus of the argument for restraining the technology came from personal perspectives with citations from non empirical sources. This maintained an overarching approach to the study which encompassed the technological facts along with affirming and deferring opinions, which were generated through a survey of general Internet users.

By employing qualitative ontology to the thesis, the goal was to discover how deep packet inspection technology impacts privacy and net neutrality. This qualitative approach allowed for the research to be measured against general principles of right and wrong and how those principles change based on the environment. Once the study was complete, it was apparent the privacy concerns due to monitoring of telephone service, were more clearly understood and

held in higher regard than the privacy concerns of monitoring Internet communications. This further proved that the perceived gap in the body of knowledge existed and needed to be accounted for.

**3.2 Questions and Survey**

As noted, Chapter 2 contains the results of the first phase of the research. Gaps in the literature were discovered and areas of improvement were apparent. The literature review also provided a foundation for the remaining two phases: question development and survey.

In phase two, questions were developed. The survey consisted of 33 questions divided into four sections: a) background information, such as field of work (IT vs. non-IT), knowledge of packet inspection and traffic shaping, b) details on Internet Service Providers with regards to how they treat network communications, regulation and pricing, c) descriptions of Telephone Service Providers such as phone tapping, conversation shaping and regulation, and d) privacy of communications. For a list of the survey questions, see Appendix A.

The participants were asked to rank each survey statement on a scale of 1 – 5, with an answer of 1 meaning strongly disagree with the statement and an answer of 5 meaning strongly agree with the statement. These rankings were combined to tally a final score for each survey question. For example, a score of 4.45 would mean that the majority of respondents strongly agree with the statement, while a score of .25 would indicate that most respondents strongly disagree with the statement. An average score of 3 would show that the average respondent fell somewhere in the middle (an average of 3 could also mean half strongly agreed and half strongly disagreed, but that scenario was not present in the result set).

In phase three, the researcher posted the survey to Facebook. The survey was available for two weeks, August 28 to September 11 2010. Once the allotted timeframe expired, the survey was closed and the results were tallied.

Of the 200 invitations extended, 68 (33%) responses were received. As expected, each respondent was a technology user with at least a passing knowledge of Internet usage (only those with Facebook accounts were surveyed). The general goal was to extract a theme or pattern to display the knowledge level and attitudes of Internet users with regards to the topics covered in this study.

**3.3 Summary**

Any endeavor worth attempting requires a plan. Through research of the academic literature involving deep packet inspection, net neutrality and their relationships, a gap in the knowledge base was ascertained. This study embraced the missing components and presented new research, accompanied by empirical data, to fill the void. The plan became a framework which allowed the research to be quantified. Once the research was in place, deliverables were created to support the study. These deliverables included the academic research and the survey of Internet users. The combination of deliverables formed the basis of what is hoped to be a solid contribution to the field by directly addressing the identified gaps in the body of knowledge. By specifically targeting an audience that stood to gain the most from the study, the methodology was doubly effective as it was able to educate while it collected data. This research framework allowed the study to uncover real concerns about privacy while detailing the relationship between deep packet inspection and net neutrality.

# Chapter 4 – Data Analysis and Findings

The survey suggested several findings that seem to support the investigation into how DPI threatens net neutrality. The results of the study revealed that most users are not aware of the dangers posed by DPI and that many IT insiders were only slightly more informed. The second finding showed that even though considerable literature on DPI exists, it is largely targeted to the engineering side of the technology. The last finding displayed that although literature on net neutrality is vast, little research has been documented on how damaging DPI technology can be to net neutrality.

## 4.1 Background Information

Table 1 provides an overview on the technical background of survey respondents. Of the 68 respondents, 14 or 21% work in the IT field, while 53 or 79% do not (1 abstained from answering). This question was posed to decipher the demographics of the audience and to provide a means to compare the results between IT and non-IT workers.

Table 1

*Which Best Describes Your Background?*

| 1. Which best describes your background? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Work in the IT field. | 20.9% | 14 |
| Not working in the IT field. | 79.1% | 53 |
| ***answered question*** | | **67** |
| ***skipped question*** | | **1** |

Table 2 shows the lack of awareness of DPI. The majority of respondents 46, or 68% were not aware of what packet inspection was. Even fewer know about deep packet inspection, 55 or 81% or traffic shaping 52 or 77%. These questions set the baseline for the group as a whole. When viewing the results, they begin to show that a gap exists in the general Internet user's knowledge of network monitoring and filtering.

Table 2

*Background Knowledge Questions (All Participants).*

| 2. Do you know what Packet Inspection is? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 32.4% | 22 |
| No | 67.6% | 46 |
| ***answered question*** | | **68** |
| ***skipped question*** | | **0** |

| 3. Do you know what Deep Packet Inspection is? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 19.1% | 13 |
| No | 80.9% | 55 |
| ***answered question*** | | **68** |
| ***skipped question*** | | **0** |

| 4. Do you know what Traffic Shaping is? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 23.5% | 16 |
| No | 76.5% | 52 |
| ***answered question*** | | **68** |
| ***skipped question*** | | **0** |

To explore these findings further, the researcher looked those working in the IT field. The data in Table 3 shows that all respondents knew what packet inspection was, while 9, or 64% knew about deep packet inspection and 10, or 71% were familiar with traffic shaping. It was no surprise that greater knowledge of network monitoring and filtering technologies was expected of those in the IT field.

Table 3

*Background Knowledge Questions (IT Field Only).*

| 2. Do you know what Packet Inspection is? (IT Field Only) | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 100.0% | 14 |
| No | 0.0% | 0 |
| ***answered question*** | | **14** |
| ***skipped question*** | | **0** |

| 3. Do you know what Deep Packet Inspection is? (IT Field Only) | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 64.3% | 9 |
| No | 35.7% | 5 |
| ***answered question*** | | **14** |
| ***skipped question*** | | **0** |

| 4. Do you know what Traffic Shaping is? (IT Field Only) | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 71.4% | 10 |
| No | 28.6% | 4 |
| ***answered question*** | | **14** |
| ***skipped question*** | | **0** |

Inversely, by looking at the same questions when asked only to non-IT workers, the results speak loudly. As shown in Table 4, only 8 respondents, or 15% knew what packet inspection was, while only 4 or 7% knew about deep packet inspection and only 6, or 11% were familiar with traffic shaping. When comparing IT workers against non-IT workers, there was a decrease in background knowledge of 85%, 57%, and 60% respectively. A decrease was expected, but this radical fall off provided solid evidence that serious gaps in network monitoring knowledge exists and a reminder that what may seem like common knowledge to industry insiders, could be foreign to laymen.

Table 4

*Background Knowledge Questions (Non-IT Field Only).*

| 2. Do you know what Packet Inspection is? (Non-IT Field Only) | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 14.8% | 8 |
| No | 85.2% | 46 |
| ***answered question*** | | **54** |
| ***skipped question*** | | **0** |

| 3. Do you know what Deep Packet Inspection is? (Non-IT Field Only) | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 7.4% | 4 |
| No | 92.6% | 50 |
| ***answered question*** | | **54** |
| ***skipped question*** | | **0** |

| 4. Do you know what Traffic Shaping is? (Non-IT Field Only) | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 11.1% | 6 |
| No | 88.9% | 48 |
| ***answered question*** | | **54** |
| ***skipped question*** | | **0** |

### 4.2 Privacy and Content

Once the background information was cataloged, the study moved to understand the attitudes of respondents towards privacy and content. As previously discussed, the format changed from yes or no responses to a rating scale, where a score of 0 meant the respondent strongly disagreed with the statement and a score of 5 meant they strongly agreed. The first segment focused on Internet Service Providers.

Should ISPs be allowed to monitor network communications? As Table 5 shows, answers to this question scored a .9 making it clear that the respondents did not think ISPs should be allowed to examine user network communications. This response was echoed when the subject switched to telephone communications as well. These queries were included to validate the necessity of privacy when communicating over any medium and the response overwhelmingly confirmed the need.

Table 5

*Examination of Network and Telephone Communications.*

**1. Internet Service Providers (ISP's) should be allowed to examine the content of your network communications.**

| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
|---|---|---|---|---|---|---|---|
| . | 38 | 12 | 7 | 2 | 0 | 0.90 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |

**1. Telephone service providers should be allowed to examine the content of your phone communications (Business, Personal_).**

| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
|---|---|---|---|---|---|---|---|
| . | 44 | 13 | 0 | 0 | 0 | 1.23 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

After establishing the need for privacy, the study continued and focused on ISPs ability to delay or deny communications based on the content being sent. Table 6 presents the scores of 1.46 in response to deny communications and 1.49 in response to delay communications. While not as lopsided as the answers in Table 5, the scores clearly illustrate disapproval of ISPs denying or delaying communications based on the content.

Table 6

*ISPs Should Be Allowed to Deny or Delay Communications.*

| 2. ISP's should be allowed to deny communications based on the type of content being sent (Music, Text, Video, Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 41 | 13 | 1 | 4 | 0 | 1.46 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |

| 3. ISP's should be allowed to delay communications based on the type of content being sent (Music, Text, Video, Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 39 | 15 | 1 | 4 | 0 | 1.49 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |

The same questions were posed regarding telephone communications. In response to service provider's ability to deny or delay communications, the subjects disagreed even more stringently. As shown in Table 7, the scores tallied 1.14 and 1.2, clearly laying out a disdain for any type of delaying or denying of communications based on content. This is a critical point that must be disseminated; Internet and telephone users do not want their communications disrupted based on the type of content they are utilizing.

Table 7

*Telephone Deny or Delay Communications.*

| 2. Telephone service providers should be allowed to deny communications based on the type of conversation (Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 49 | 8 | 0 | 0 | 0 | 1.14 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 3. Telephone service providers should be allowed to delay communications based on the type of conversation (Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 45 | 11 | 0 | 0 | 0 | 1.20 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

To cap off the content based questions, the survey turned to the respondent's attitudes towards content based fees. For both network and telephone communications, the subjects decreed a strong unwillingness to pay for service based on content. In this case, the scores for both network communications (1.75) and telephone communications (1.61) were squarely placed in the strongly disagree category. As evidenced in Table 8, the thought of paying a premium for specific types of communications did not sit well.

Table 8

*Premium Content, Premium Fees?*

| 15. ISP's should be allowed to charge more for specific types of network communications (Music, Text, Video, Business, Personal). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 34 | 11 | 9 | 5 | 0 | 1.75 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |

| 12. Telephone service providers should be allowed to charge more for specific types of phone calls (Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 34 | 13 | 8 | 2 | 0 | 1.61 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

### 4.3 Regulation

The content and privacy attitudes were clearly displayed as evidenced by reviewing the results in the previous segment, but the trend did not continue with the regulation results as they were a bit more ambiguous.

After reviewing the data for the network monitoring topics (packet inspection, deep packet inspection and traffic shaping), the majority of the answers were agreeable (final score of ~3) for regulation, but disagreeable (final score of ~2) for government regulation. The general regulation results are defined in Table 9, which showed the respondents were middle of the road when asked about general regulation of packet inspection, deep packet inspection and traffic shaping. Table 10 illustrated that the respondents did not feel government regulation was the answer. Following suite, the questions surrounding regulation by a standards agency scored roughly on par with general regulation as shown in Table 11. These results detail the overall uneasiness felt around government regulation, but still supported that some regulation would be beneficial.

Table 9

*To Regulate or Not To Regulate?*

| 4. Packet Inspection should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 15 | 3 | 21 | 8 | 10 | 2.91 | 57 |
| | | | | | | ***answered question*** | **57** |
| | | | | | | ***skipped question*** | **11** |

| 7. Deep Packet Inspection should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 13 | 4 | 25 | 6 | 9 | 2.89 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 10. Traffic Shaping should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 12 | 6 | 27 | 4 | 7 | 2.79 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

Table 10

*Government Regulation?*

| 5. Packet Inspection should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 26 | 9 | 19 | 2 | 1 | 2.00 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 8. Deep Packet Inspection should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 24 | 6 | 23 | 2 | 2 | 2.16 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 11. Traffic Shaping should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 22 | 9 | 23 | 0 | 1 | 2.07 | 55 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

Table 11

*Standards Agency Regulation?*

| 6. Packet Inspection should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 12 | 6 | 26 | 9 | 4 | 2.77 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 9. Deep Packet Inspection should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 13 | 5 | 29 | 6 | 4 | 2.70 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 12. Traffic Shaping should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 9 | 6 | 30 | 5 | 5 | 2.84 | 55 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

### 4.4 Trust and Moral Obligations

As deep packet inspection gives ISPs the ability to peer into the content of network communications, the threat of abuse is present. The study attempted to gauge the respondent's feelings about whether or not service providers had moral obligations when utilizing network monitoring technology. Table 12 shows that while the ratings were agreeable, with scores of 3.34 for ISPs and 3.47 for telephone service providers. This shows that even though the respondents were lukewarm towards regulation, they felt that there still was a moral obligation for service providers when examining communications.

Table 12

*Moral Obligations?*

| 13. There are moral obligations with regard to ISP's examining the content of network communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 10 | 9 | 10 | 9 | 20 | 3.34 | 58 |
| | | | | | | ***answered question*** | **58** |
| | | | | | | ***skipped question*** | **10** |

| 10. There are moral obligations with regard to Telephone service providers examining the content of phone communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 10 | 4 | 12 | 11 | 20 | 3.47 | 57 |
| | | | | | | ***answered question*** | **57** |
| | | | | | | ***skipped question*** | **11** |

Continuing the theme of the previous statements, the next two survey questions dealt with trust. As illustrated in Table 13, Internet users felt they could somewhat trust service providers to examine only the content and not the information of their communications. It should be noted, that the highest tallies were present in the strongly disagree (no trust) options on both statements and the lowest tallies were in the strongly agree (trust) columns.

Table 13

*Trusted Providers.*

| 14. ISP's can be trusted to only examine the type of content and not the information contained in the content of network communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 18 | 9 | 18 | 7 | 7 | 2.59 | 59 |
| | | | | | | ***answered question*** | **59** |
| | | | | | | ***skipped question*** | **9** |

| 11. Telephone service providers can be trusted to only examine the type of conversation and not the information discussed. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 24 | 10 | 12 | 6 | 4 | 2.21 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

**4.5 Privacy of Communications**

The loudest declaration from the respondents was far and away their privacy concerns. These last two questions were included to put a statement on the survey, and the results came through. Table 14 shows the direct privacy questions scored the highest of all questions. When asked if Internet and telephone communications should be private, the audience resoundingly agreed, with scores of 4.44 and 4.55. These final questions were further evidence that privacy is a concern that is of utmost importance to general Internet users.

Table 14

*Privacy of Communications.*

| 1. Internet communications should be private. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 0 | 1 | 3 | 23 | 30 | 4.44 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

| 2. Phone communications should be private. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 0 | 1 | 1 | 20 | 34 | 4.55 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

### 4.6 Summary

Clearly the results provided a deeper understanding of the technical knowledge and attitudes of general Internet population. This understanding validated that the identified gap in the literature would directly address the concerns of the public.

Once the demographics of the study were established, the results between IT and non-IT workers showed a vast difference in network monitoring knowledge. This delta in the knowledge adds to the evidence that more research and communication is needed to ensure the general population is educated about threats to their privacy. When queried about regulation, the audience felt it was a good idea, but they felt strongly that government regulation was not the answer. That privacy was worth worrying about was validated as the respondents made it clear they want their communications to remain private and they want service providers to stay away from the information they are sharing.

## Chapter 5 – Discussion and Conclusions

This researcher believes this study contributes to the literature still dominated by engineering issues and public policy debate. The findings help explain how a gap in the literature can have far reaching consequences and the need for more education and awareness of the general public with regards to privacy of communications is needed. Analyzing the results clearly illustrated a desire for privacy, yet the knowledge of network monitoring technologies was scant at best. Without raising the awareness of technologies like deep packet inspection and communicating the dangers it carries, net neutrality will be difficult to achieve.

In designing the research, a three phase methodology was adopted. The first phase was to gather existing literature on deep packet inspection and net neutrality and how they related to privacy of communications. The gap in the literature became evident. Once the empirical data was garnered, the second phase focused on generating questions to help gauge the attitudes and knowledge of Internet users. Once the questions were in hand, they were presented via survey to help quantify the aforementioned literature gap.

The methodology used may limit the use and interpretation of the data. First, by relying on qualitative means to demonstrate the missing links, the study will always be open to interpretation. As the nature of qualitative research is to generate and quantify opinions, it can only be as strong as the opinions and the analysis of them. This is especially difficult when the

subject matter is as controversial as net neutrality. Second, the number of respondents was small. But this researcher believes that even with a greater number of respondents, the overall trends would remain largely unchanged. The focus of the study was to fill a gap in the literature. The validity of the gap was proven as the drastic differences in knowledge between IT and non-IT workers was displayed in the results. The study's ability to fill that gap will be judged as time passes. This study should be considered an early attempt to investigate the linkages between deep packet inspection and net neutrality. The literature could benefit from other studies; notably - a survey of ISPs. Further research is necessary to ensure that while technology advances, so does the ability to keep a balance between progress and privacy. This research generally supports the belief that DPI endangers net neutrality and privacy. But more research would, in the long run, produce a more complete picture of the challenges that DPI poses to net neutrality.

**References**

Anderson, N. (2007). Deep packet inspection meets 'Net Neutrality, CALEA'. *Arstechnica*. Retrieved from http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars

Becchi, M., Crowley, P. (2007). An improved algorithm to accelerate regular expression evaluation. *Proceedings of the 3rd ACM/IEEE Symposium on Architecture for networking and communications systems*.

Economedies, N. (2008). "Net Neutrality," Non-Discrimination and digital distribution of content through the Internet. *I/S: A Journal of Law and Policy.* 4 (2) 209-233.

Feldman, P. J. (2010). FCC releases net neutrality NPRM - Let the jousting begin. *CommLawBlog.* Retrieved from http://www.commlawblog.com/2009/10/articles/wireline-telephony/fcc-releases-net-neutrality-nprm-let-the-jousting-begin/

Georgiadis, L. Guérin, R. Peris, V. & Sivarajan, K. N. (1996). Efficient network QoS provisioning based on per node traffic shaping. *IEEE/ACM Transactions on Networking (TON)*, 4-n.(4), 482-501.

Goldman, J. E. & Rawls, P. T. (2004). *Applied data communications* (4th ed.). Hoboken, NJ: Wiley.

Hills, T. (2006). Deep packet inspection. *Lightreading*. Retrieved from http://www.lightreading.com/document.asp?doc_id=111404

Jordan, S. (2009). Implications of Internet architecture on net neutrality, ACM Transactions on Internet Technology, *9*, 1-28.

Kennedy, J. (2010). Draft net neutrality bill to go before US Congress. *Silicon Republic*. Retrieved from http://www.siliconrepublic.com/comms/item/18046-draft-net-neutrality-bill

Kirgman, E. (2010). Net neutrality bill might be more about message than action. *National Journal*. Retrieved from http://techdailydose.nationaljournal.com/2010/09/net-neutrality-bill-might-be-m.php

Kumar, S., Turner, J., & Williams, J. (2006). Advanced algorithms for fast and scalable deep packet inspection. *Proceedings of the 2006 ACM/IEEE Symposium on Architecture for Networking and Communications Systems*.

Porter, T. (2005). The perils of deep packet inspection. *Security Focus*. Retrieved from http://www.securityfocus.com/infocus/1817

Ranum, M. (2005). What is "Deep Inspection"?". *Ranum*. Retrieved from http://www.ranum.com/security/computer_security/editorials/deepinspect/index.html

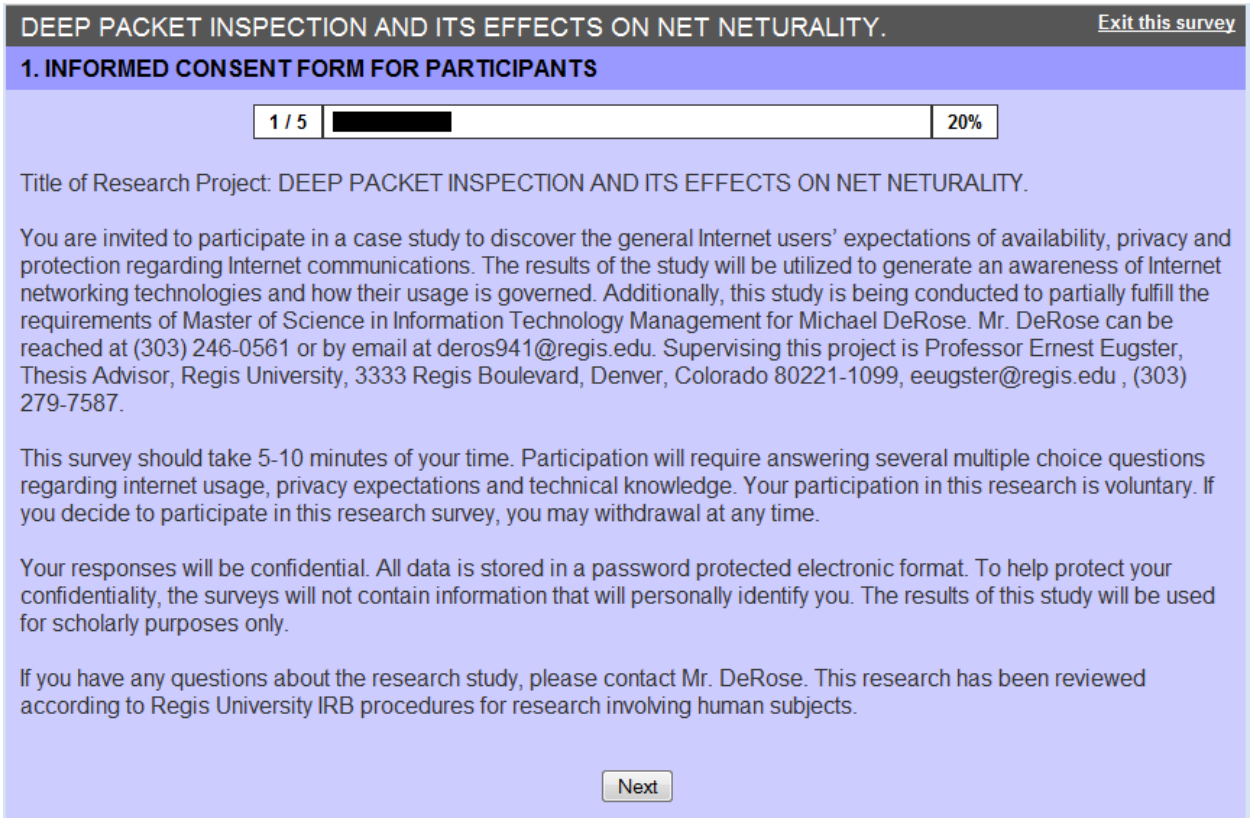
Renals, J. (2009). Blocking skype through deep packet inspection**.** *Proceedings of the 42nd Hawaii International Conference on System Sciences.*

Schahczenski, C. (2008). Net neutrality, computing and social change. *SIGCAS Computers and Society*, *38-2*. http://www.ranum.com/security/computer_security/editorials/deepinspect/index.html

Smith, R., Estan, C., Jha, S., & Kong,S. (2008) Deflating the big bang: fast and scalable deep packet inspection with extended finite automata. *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*.

Stallings, William. (2007). *Data and computer communications* (8th ed.). Upper Saddle River, NJ: Pearson Education, Inc.

# Appendix A – Survey Questions



DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NETURALITY. Exit this survey

**1. INFORMED CONSENT FORM FOR PARTICIPANTS**

1 / 5 20%

Title of Research Project: DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NETURALITY.

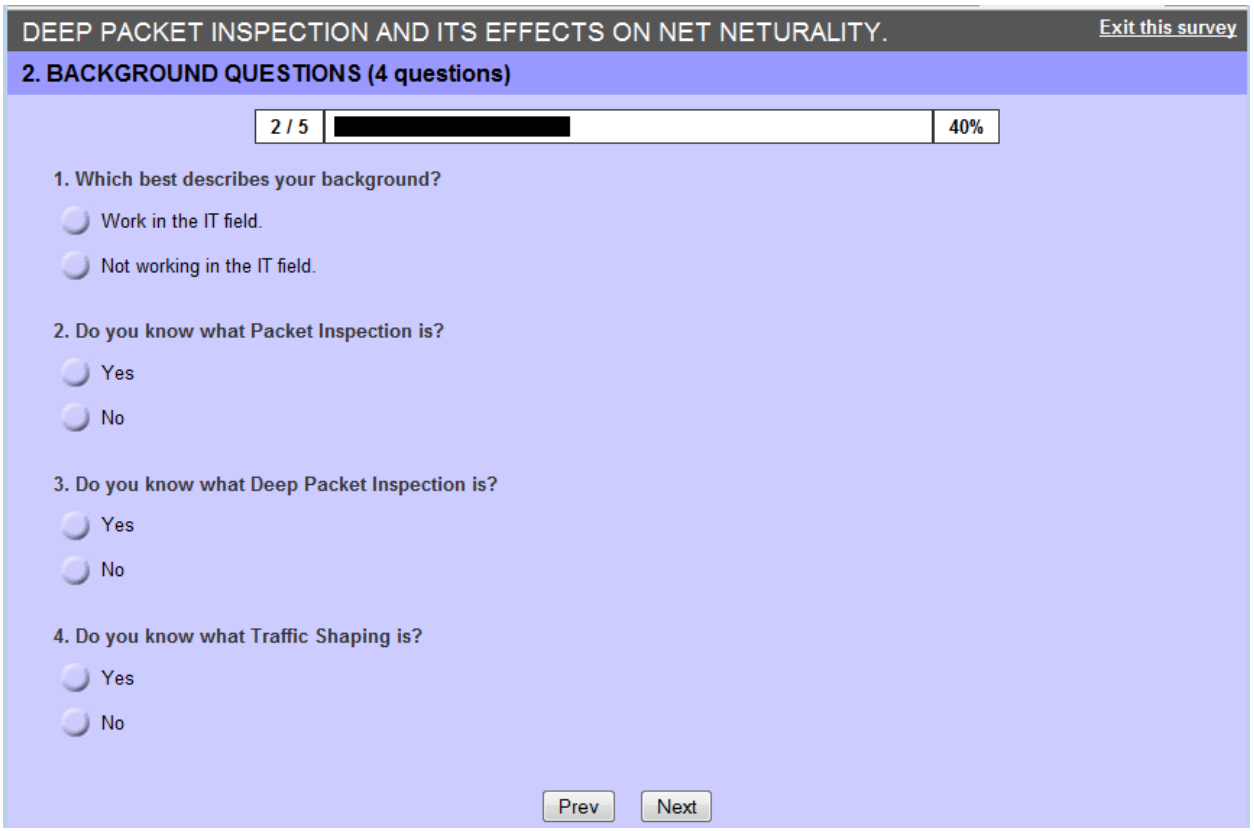
You are invited to participate in a case study to discover the general Internet users' expectations of availability, privacy and protection regarding Internet communications. The results of the study will be utilized to generate an awareness of Internet networking technologies and how their usage is governed. Additionally, this study is being conducted to partially fulfill the requirements of Master of Science in Information Technology Management for Michael DeRose. Mr. DeRose can be reached at (303) 246-0561 or by email at deros941@regis.edu. Supervising this project is Professor Ernest Eugster, Thesis Advisor, Regis University, 3333 Regis Boulevard, Denver, Colorado 80221-1099, eeugster@regis.edu , (303) 279-7587.

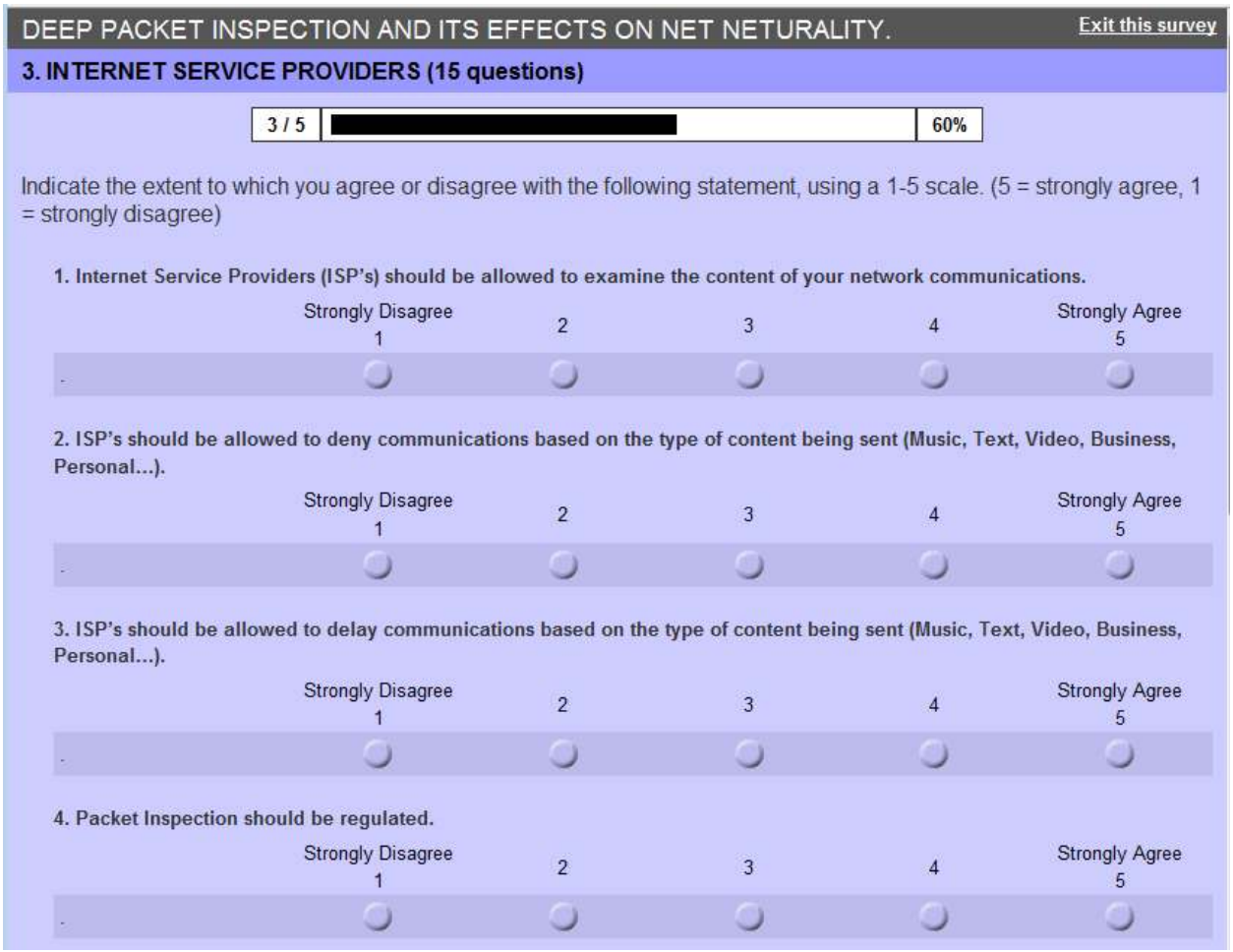
This survey should take 5-10 minutes of your time. Participation will require answering several multiple choice questions regarding internet usage, privacy expectations and technical knowledge. Your participation in this research is voluntary. If you decide to participate in this research survey, you may withdrawal at any time.

Your responses will be confidential. All data is stored in a password protected electronic format. To help protect your confidentiality, the surveys will not contain information that will personally identify you. The results of this study will be used for scholarly purposes only.

If you have any questions about the research study, please contact Mr. DeRose. This research has been reviewed according to Regis University IRB procedures for research involving human subjects.

Next


DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NETURALITY.
Exit this survey
2. BACKGROUND QUESTIONS (4 questions)
2 / 5
40%
1. Which best describes your background?
Work in the IT field.
Not working in the IT field.
2. Do you know what Packet Inspection is?
Yes
No
3. Do you know what Deep Packet Inspection is?
Yes
No
4. Do you know what Traffic Shaping is?
Yes
No
Prev
Next



DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NETURALITY. Exit this survey

**3. INTERNET SERVICE PROVIDERS (15 questions)**

3 / 5 60%

Indicate the extent to which you agree or disagree with the following statement, using a 1-5 scale. (5 = strongly agree, 1 = strongly disagree)

**1. Internet Service Providers (ISP's) should be allowed to examine the content of your network communications.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**2. ISP's should be allowed to deny communications based on the type of content being sent (Music, Text, Video, Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**3. ISP's should be allowed to delay communications based on the type of content being sent (Music, Text, Video, Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**4. Packet Inspection should be regulated.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

5. Packet Inspection should be regulated by the government.

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

6. Packet Inspection should be regulated by a non-government agency (Standards group).

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

7. Deep Packet Inspection should be regulated.

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

8. Deep Packet Inspection should be regulated by the government.

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

9. Deep Packet Inspection should be regulated by a non-government agency (Standards group).

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

10. Traffic Shaping should be regulated.

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**11. Traffic Shaping should be regulated by the government.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**12. Traffic Shaping should be regulated by a non-government agency (Standards group).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**13. There are moral obligations with regard to ISP's examining the content of network communications.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**14. ISP's can be trusted to only examine the type of content and not the information contained in the content of network communications.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**15. ISP's should be allowed to charge more for specific types of network communications (Music, Text, Video, Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

Prev Next

DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NETURALITY. Exit this survey

**4. TELEPHONE SERVICE PROVIDERS (12 Questions)**

4 / 5 80%

Indicate the extent to which you agree or disagree with the following statement, using a 1-5 scale. (5 = strongly agree, 1 = strongly disagree)

**1. Telephone service providers should be allowed to examine the content of your phone communications (Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**2. Telephone service providers should be allowed to deny communications based on the type of conversation (Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**3. Telephone service providers should be allowed to delay communications based on the type of conversation (Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**4. Phone Tapping should be regulated.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**5. Phone Tapping should be regulated by the government.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**6. Phone Tapping should be regulated by a non-government agency (Standards group).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**7. Conversation Shaping should be regulated.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**8. Conversation Shaping should be regulated by the government.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**9. Conversation Shaping should be regulated by a non-government agency (Standards group).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**10. There are moral obligations with regard to Telephone service providers examining the content of phone communications.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

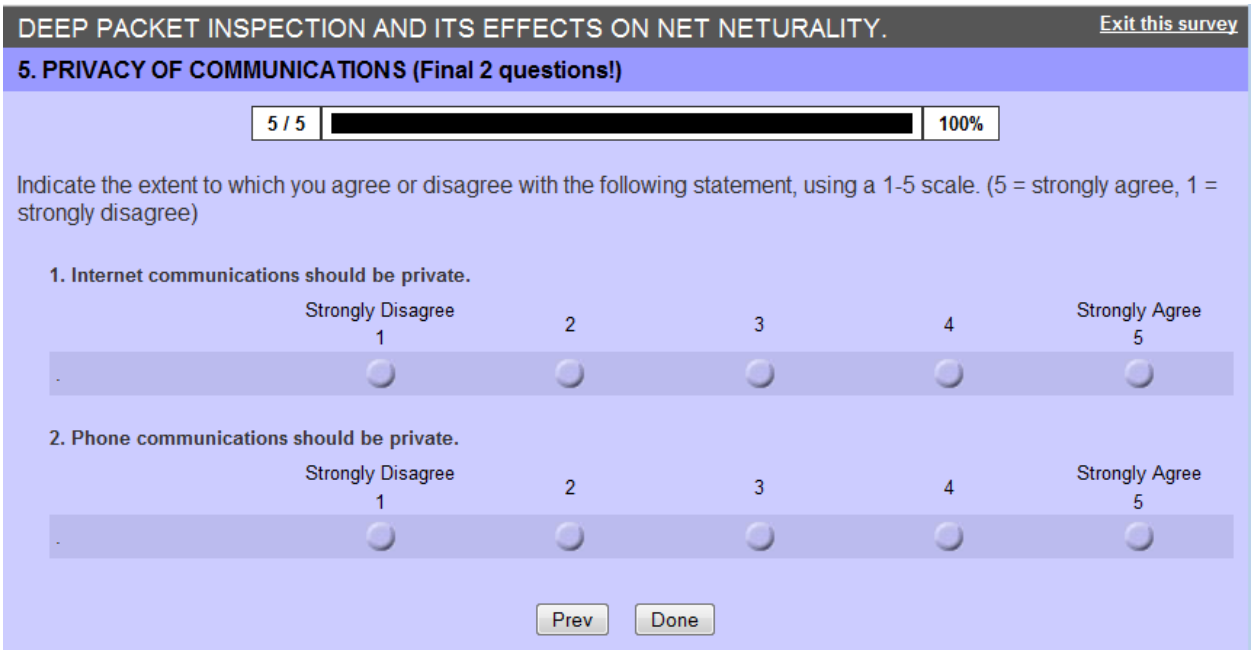
**11. Telephone service providers can be trusted to only examine the type of conversation and not the information discussed.**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

**12. Telephone service providers should be allowed to charge more for specific types of phone calls (Business, Personal...).**

| | Strongly Disagree 1 | 2 | 3 | 4 | Strongly Agree 5 |
|---|---|---|---|---|---|
| . | ○ | ○ | ○ | ○ | ○ |

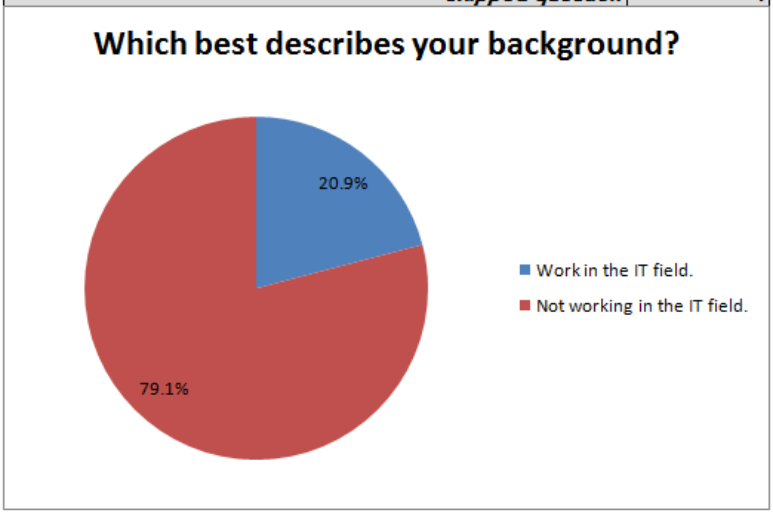
Prev Next


DEEP PACKET INSPECTION AND ITS EFFECTS ON NET NETURALITY.
Exit this survey
5. PRIVACY OF COMMUNICATIONS (Final 2 questions!)
5 / 5
100%
Indicate the extent to which you agree or disagree with the following statement, using a 1-5 scale. (5 = strongly agree, 1 = strongly disagree)
1. Internet communications should be private.
Strongly Disagree 1
2
3
4
Strongly Agree 5
2. Phone communications should be private.
Strongly Disagree 1
2
3
4
Strongly Agree 5
Prev
Done

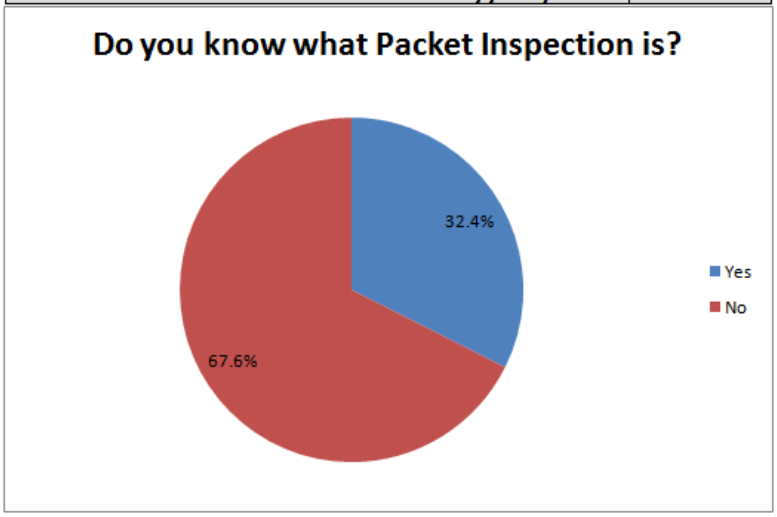
## Appendix B - Survey Results

Section 1 - BACKGROUND QUESTIONS (4 questions)

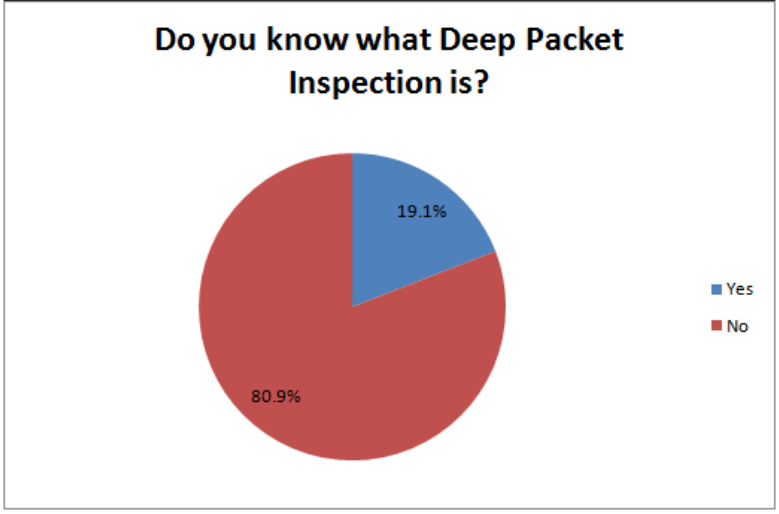
| 1. Which best describes your background? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Work in the IT field. | 20.9% | 14 |
| Not working in the IT field. | 79.1% | 53 |
| *answered question* | | 67 |
| *skipped question* | | 1 |



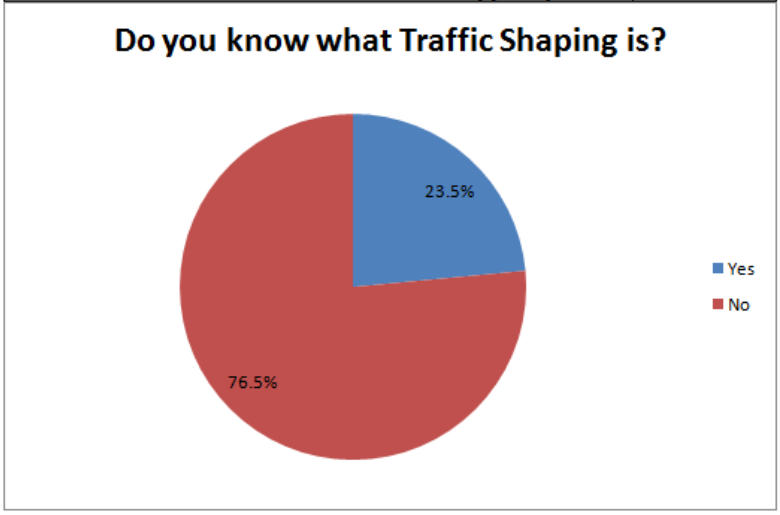

| 2. Do you know what Packet Inspection is? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 32.4% | 22 |
| No | 67.6% | 46 |
| *answered question* | | 68 |
| *skipped question* | | 0 |



| 3. Do you know what Deep Packet Inspection is? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 19.1% | 13 |
| No | 80.9% | 55 |
| *answered question* | | 68 |
| *skipped question* | | 0 |

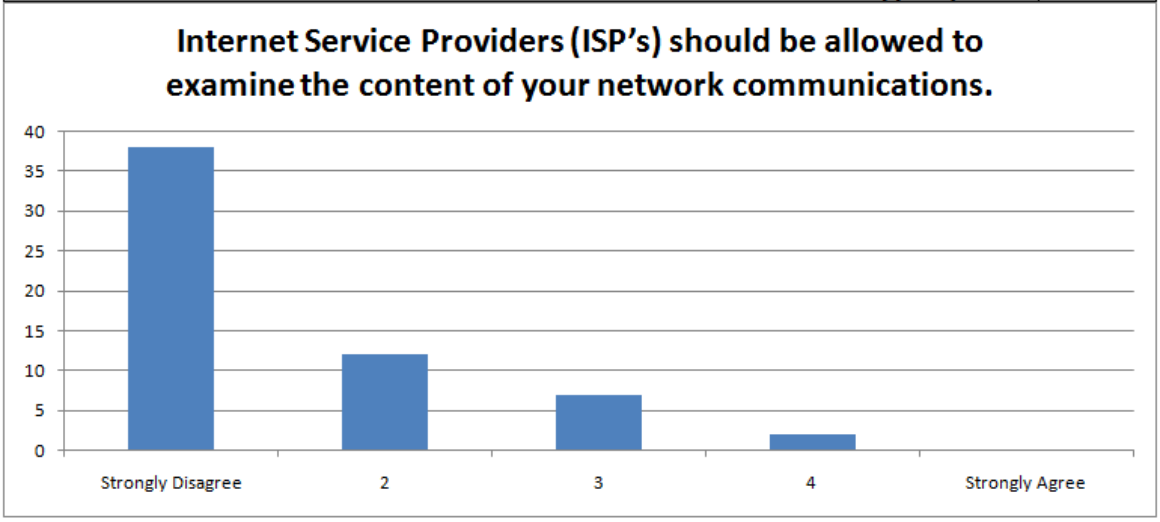



| 4. Do you know what Traffic Shaping is? | | |
|---|---|---|
| **Answer Options** | **Response Percent** | **Response Count** |
| Yes | 23.5% | 16 |
| No | 76.5% | 52 |
| *answered question* | | 68 |
| *skipped question* | | 0 |

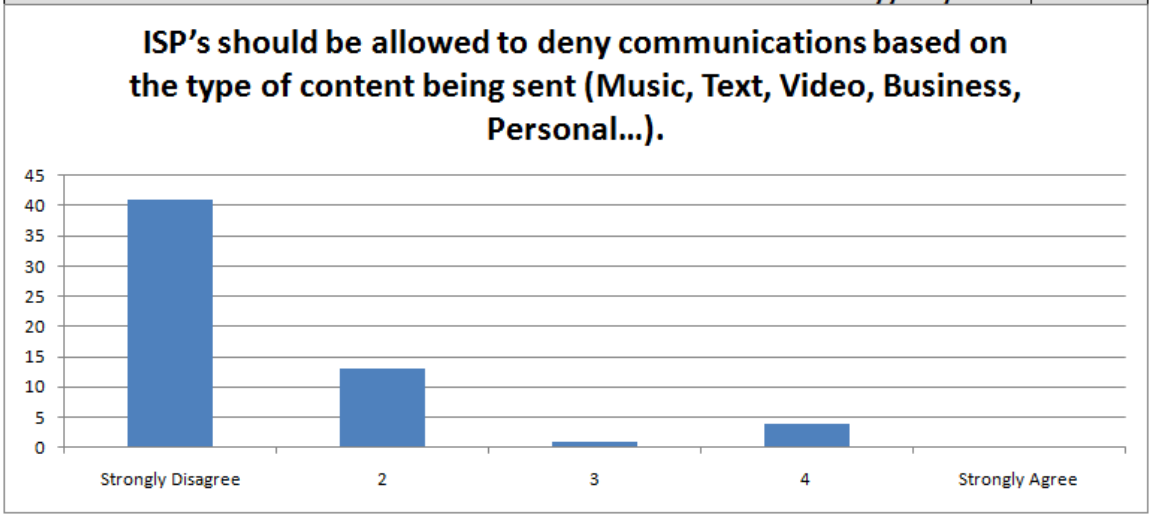



Section 2 - INTERNET SERVICE PROVIDERS (15 questions)

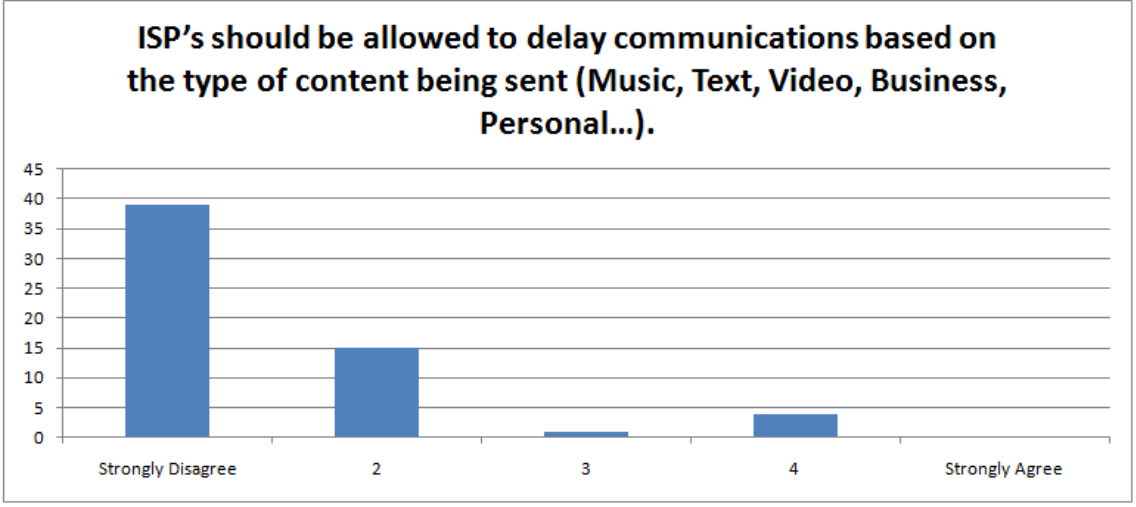
| 1. Internet Service Providers (ISP's) should be allowed to examine the content of your network communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 38 | 12 | 7 | 2 | 0 | 0.90 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |



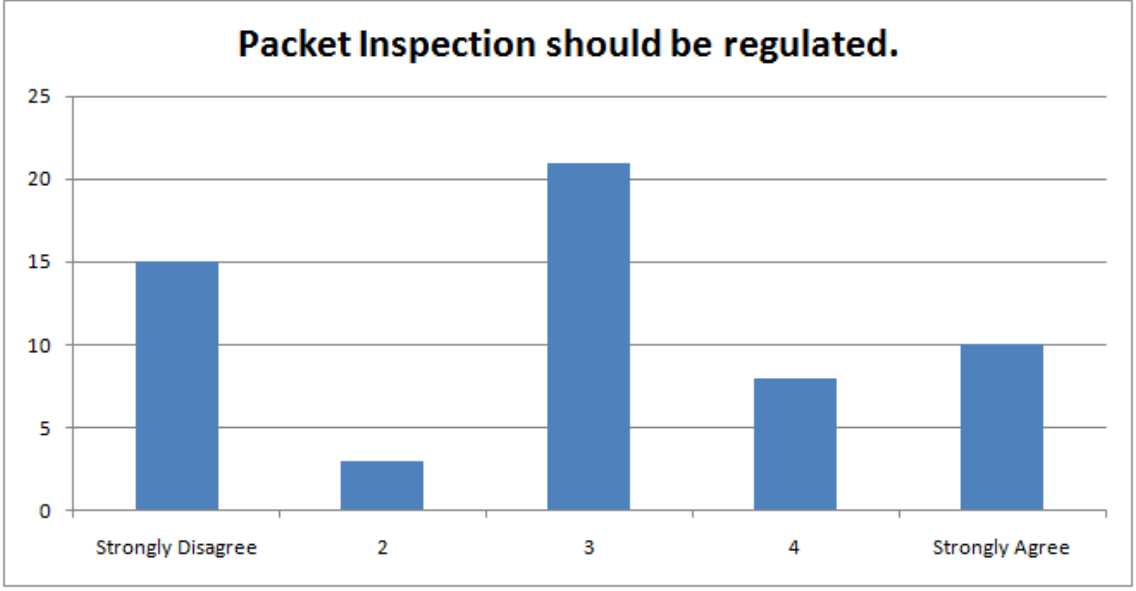

| 2. ISP's should be allowed to deny communications based on the type of content being sent (Music, Text, Video, Business, Personal...). | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 41 | 13 | 1 | 4 | 0 | 1.46 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |



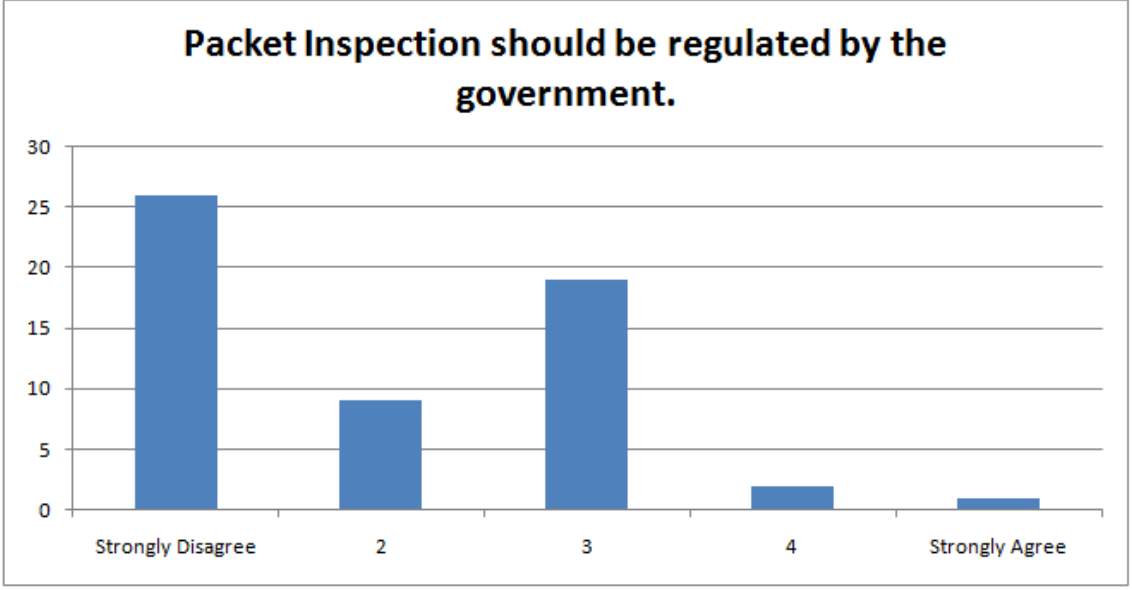
| 3. ISP's should be allowed to delay communications based on the type of content being sent (Music, Text, Video, Business, Personal...). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 39 | 15 | 1 | 4 | 0 | 1.49 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |



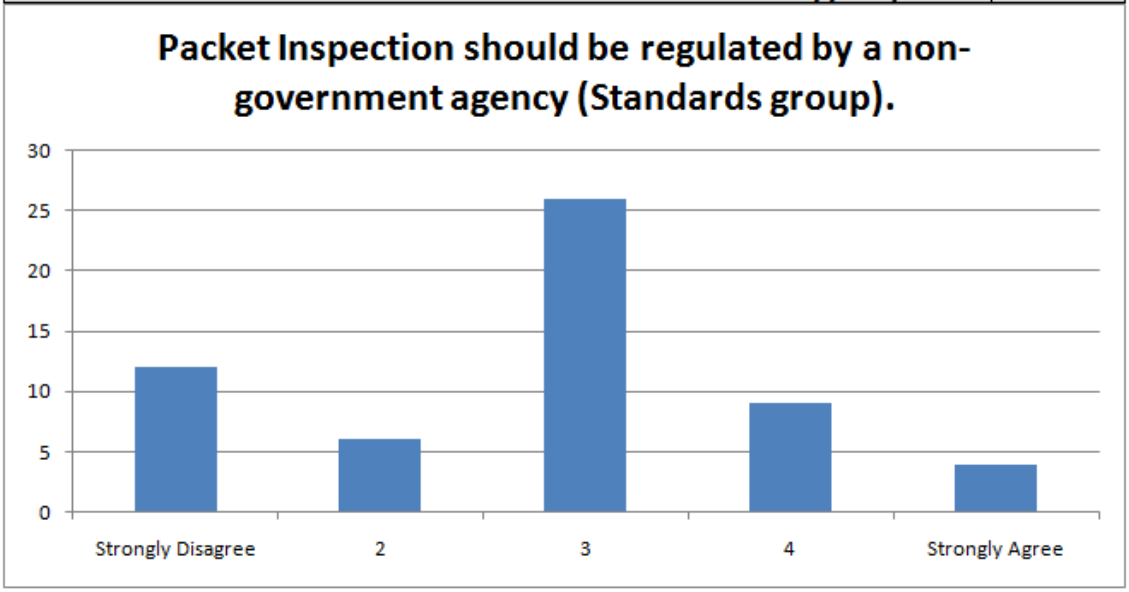

| 4. Packet Inspection should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 15 | 3 | 21 | 8 | 10 | 2.91 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



| 5. Packet Inspection should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 26 | 9 | 19 | 2 | 1 | 2.00 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

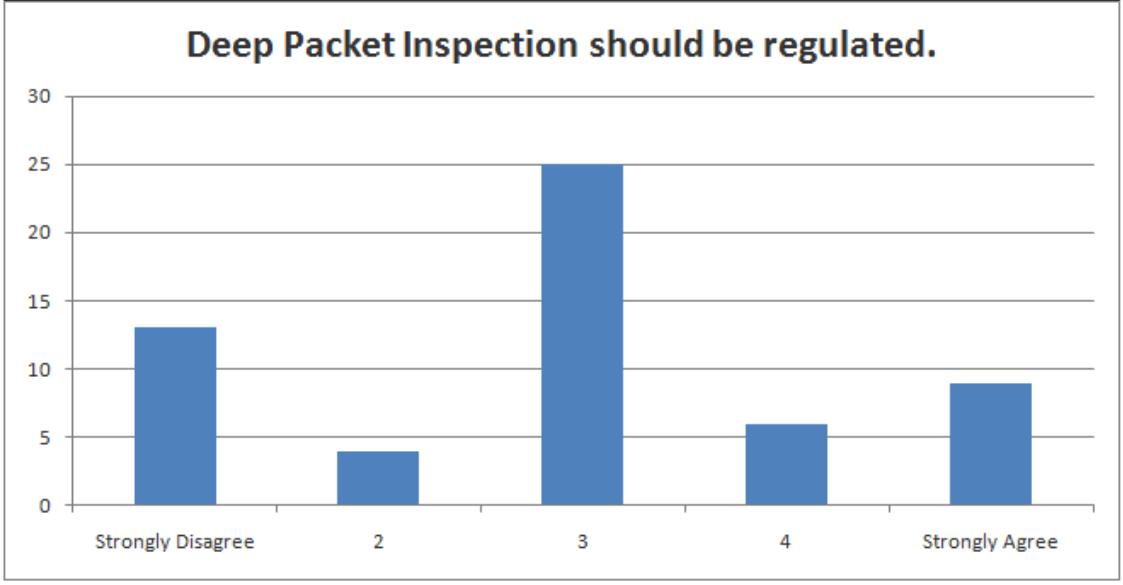



| 6. Packet Inspection should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 12 | 6 | 26 | 9 | 4 | 2.77 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



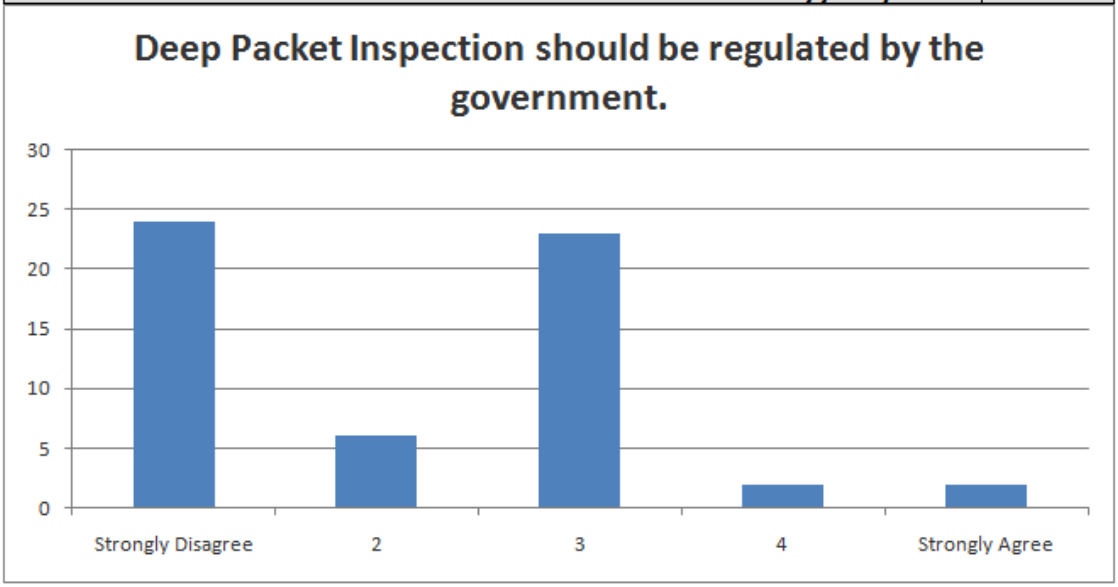
**7. Deep Packet Inspection should be regulated.**

| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
|---|---|---|---|---|---|---|---|
| . | 13 | 4 | 25 | 6 | 9 | 2.89 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |

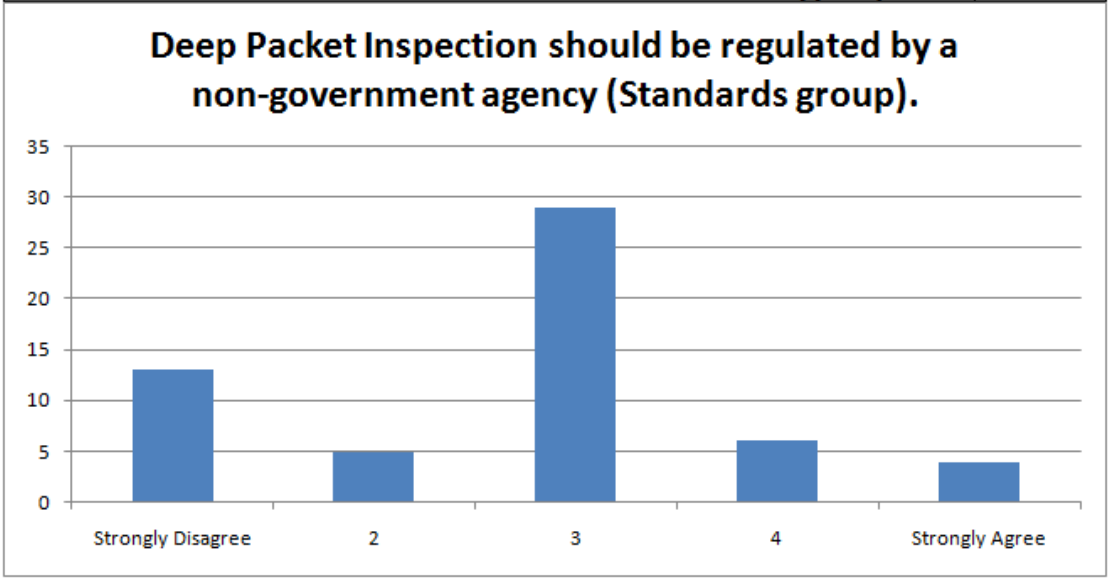



**8. Deep Packet Inspection should be regulated by the government.**

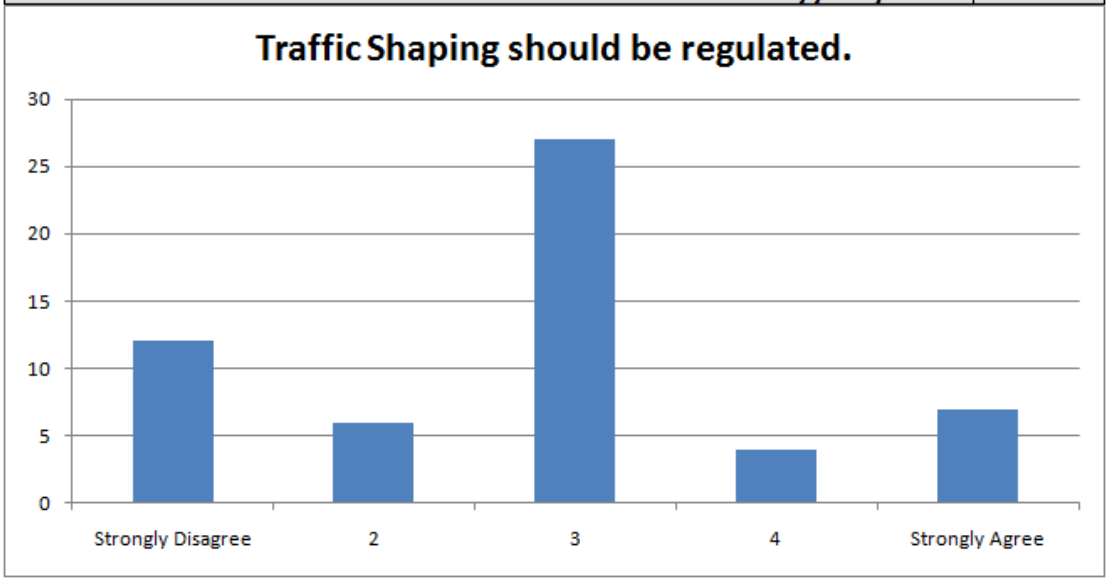
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
|---|---|---|---|---|---|---|---|
| . | 24 | 6 | 23 | 2 | 2 | 2.16 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



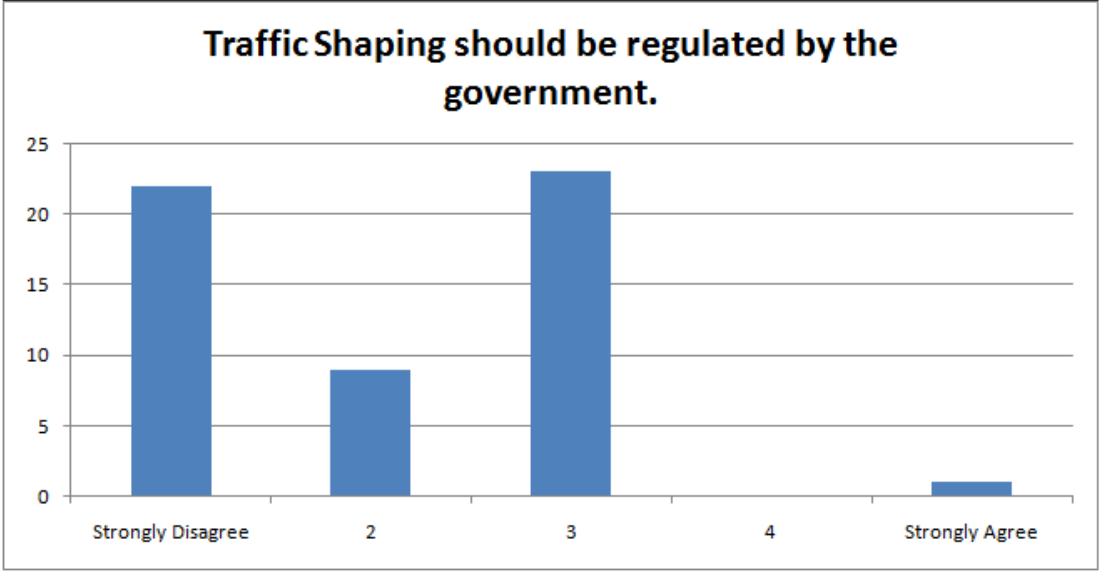
| 9. Deep Packet Inspection should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 13 | 5 | 29 | 6 | 4 | 2.70 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



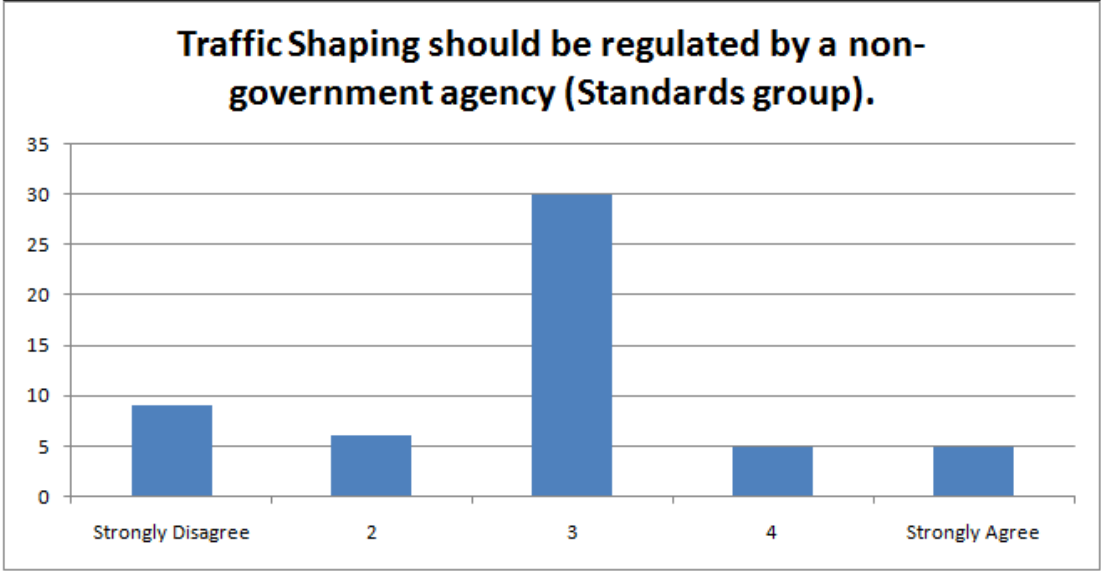

| 10. Traffic Shaping should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 12 | 6 | 27 | 4 | 7 | 2.79 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |



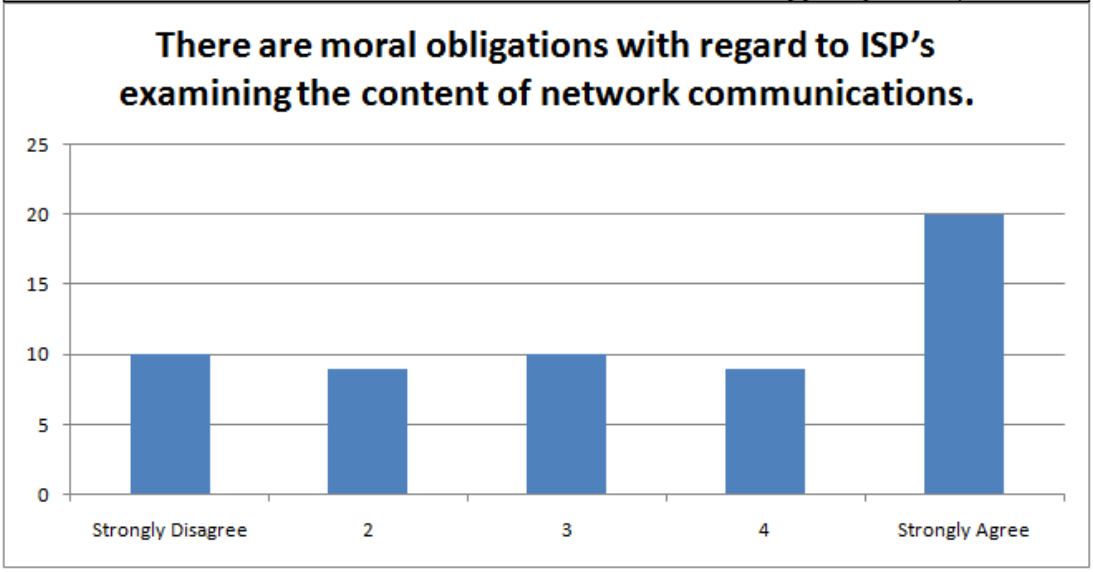
| 11. Traffic Shaping should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 22 | 9 | 23 | 0 | 1 | 2.07 | 55 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |



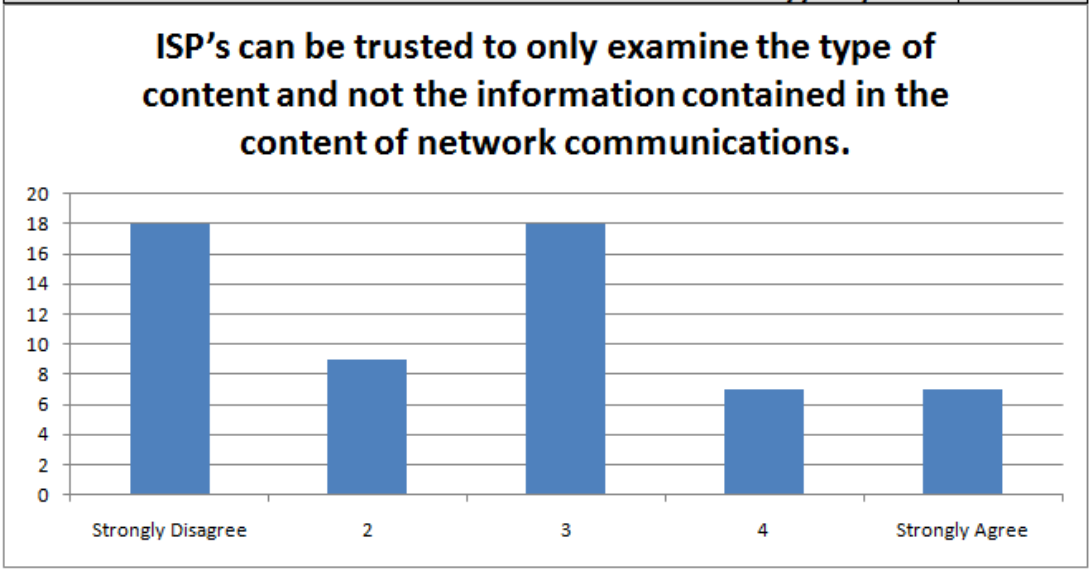

| 12. Traffic Shaping should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 9 | 6 | 30 | 5 | 5 | 2.84 | 55 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |



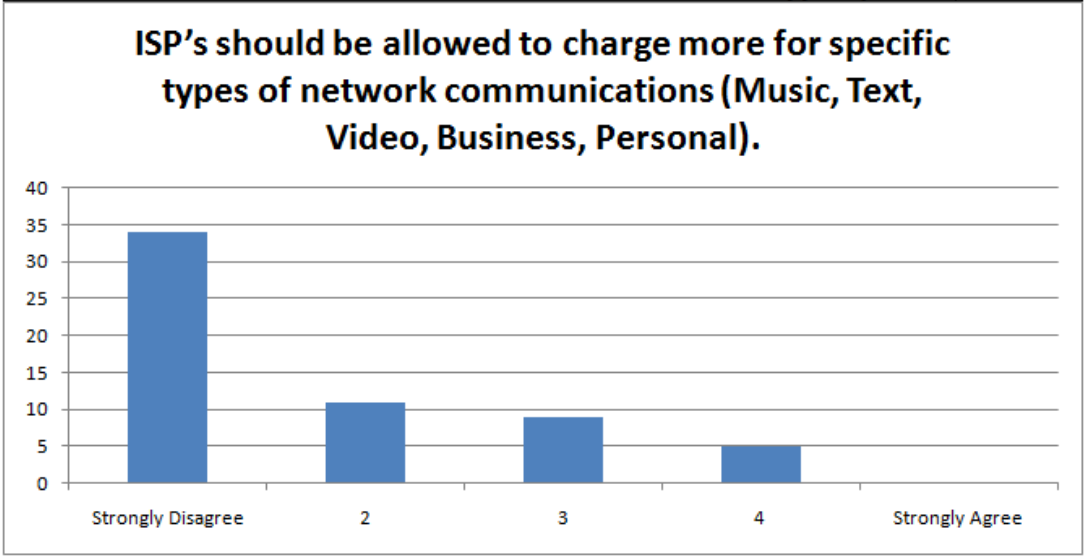
| 13. There are moral obligations with regard to ISP's examining the content of network communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 10 | 9 | 10 | 9 | 20 | 3.34 | 58 |
| | | | | | | *answered question* | 58 |
| | | | | | | *skipped question* | 10 |




| 14. ISP's can be trusted to only examine the type of content and not the information contained in the content of network communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 18 | 9 | 18 | 7 | 7 | 2.59 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |

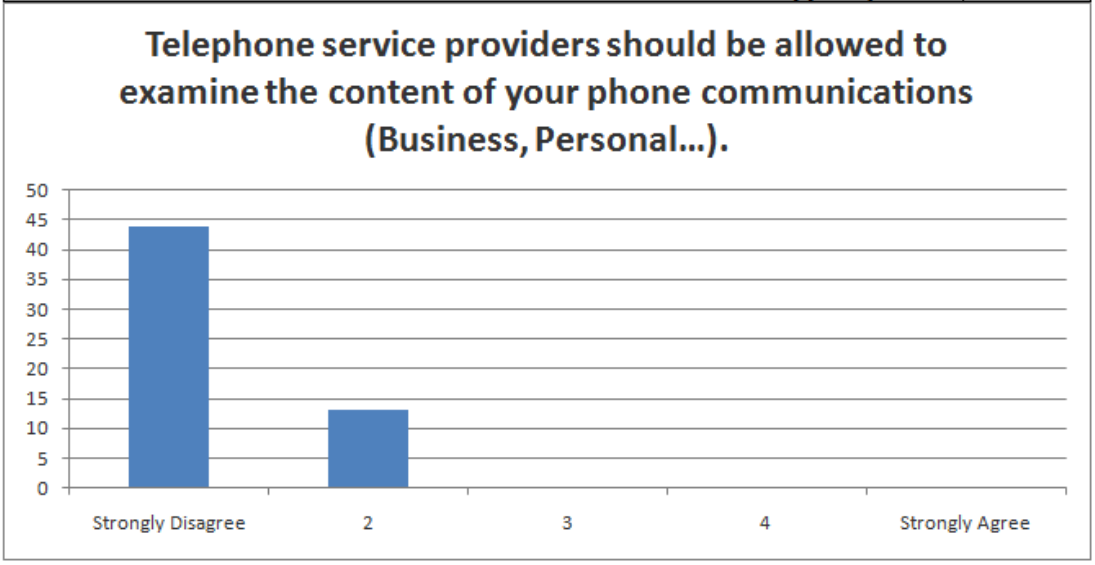


| 15. ISP's should be allowed to charge more for specific types of network communications (Music, Text, Video, Business, Personal). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 34 | 11 | 9 | 5 | 0 | 1.75 | 59 |
| | | | | | | *answered question* | 59 |
| | | | | | | *skipped question* | 9 |

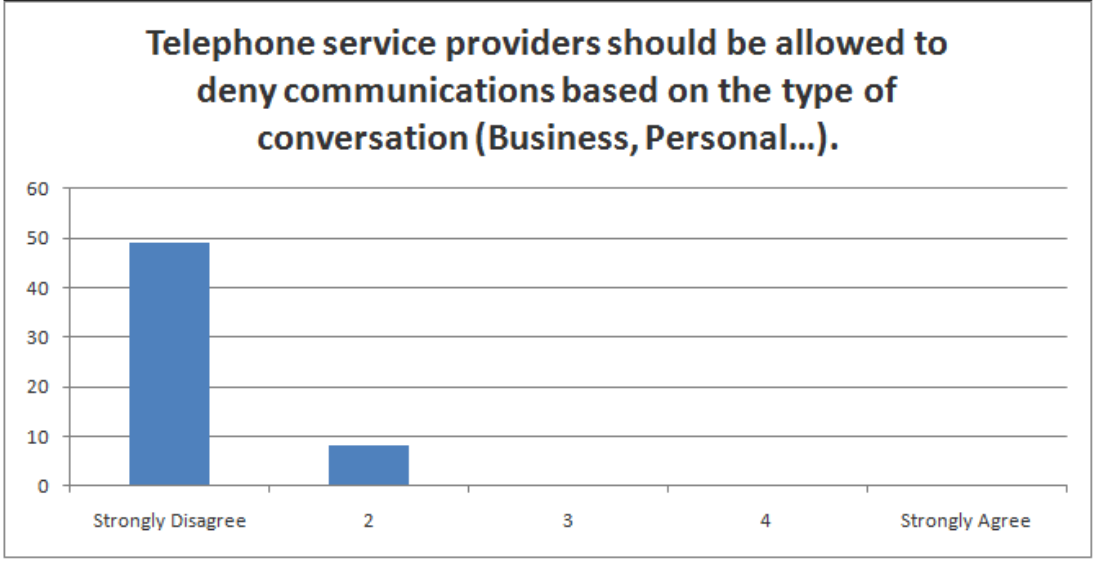



Section 3 - TELEPHONE SERVICE PROVIDERS (12 Questions)

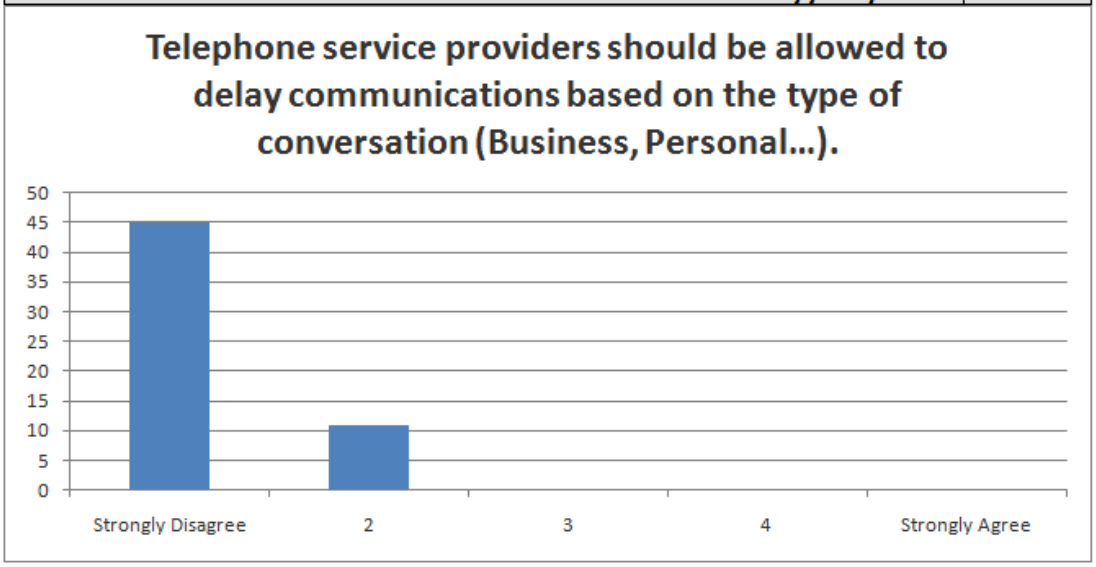
| 1. Telephone service providers should be allowed to examine the content of your phone communications (Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 44 | 13 | 0 | 0 | 0 | 1.23 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



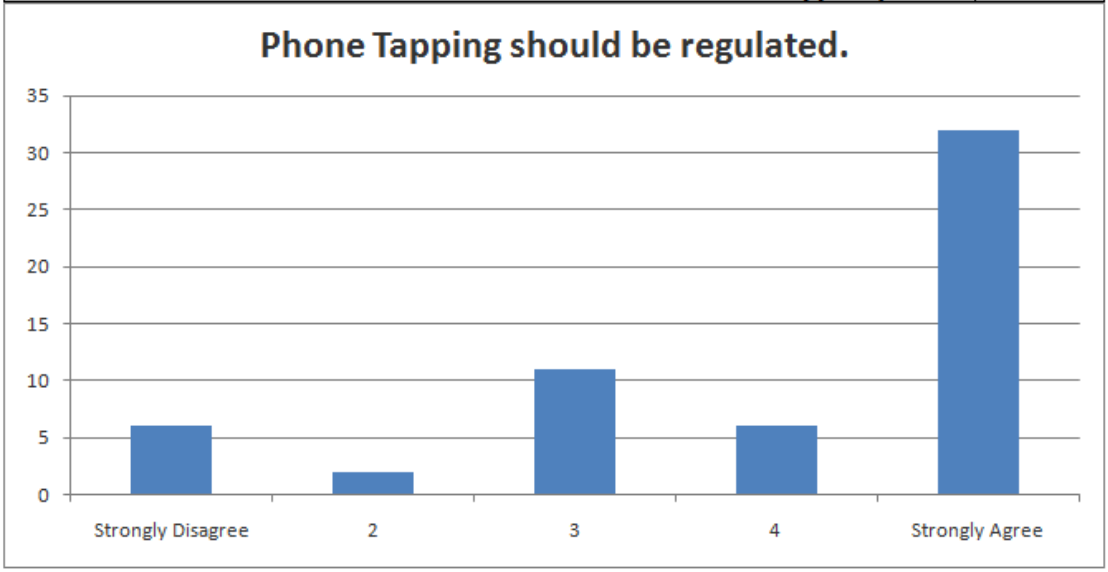
| 2. Telephone service providers should be allowed to deny communications based on the type of conversation (Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 49 | 8 | 0 | 0 | 0 | 1.14 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



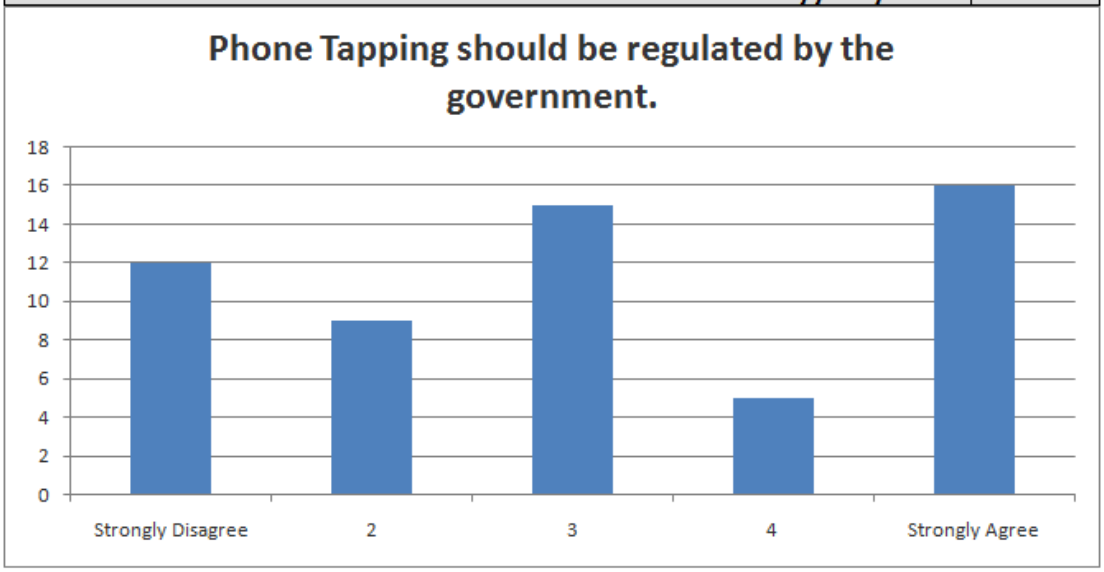

| 3. Telephone service providers should be allowed to delay communications based on the type of conversation (Business, Personal_). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 45 | 11 | 0 | 0 | 0 | 1.20 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |



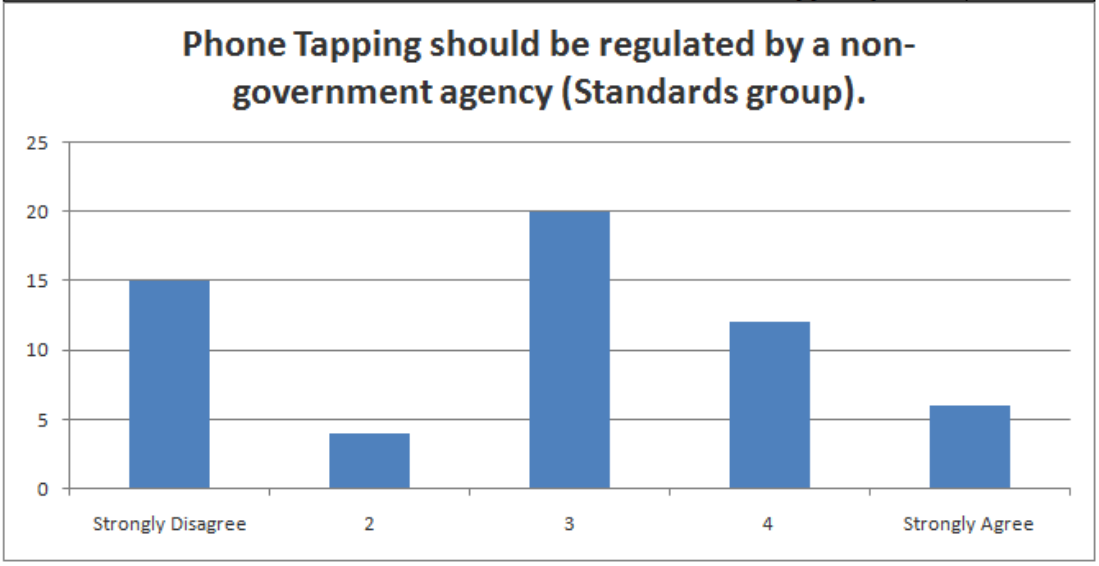
| 4. Phone Tapping should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 6 | 2 | 11 | 6 | 32 | 3.98 | 57 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |



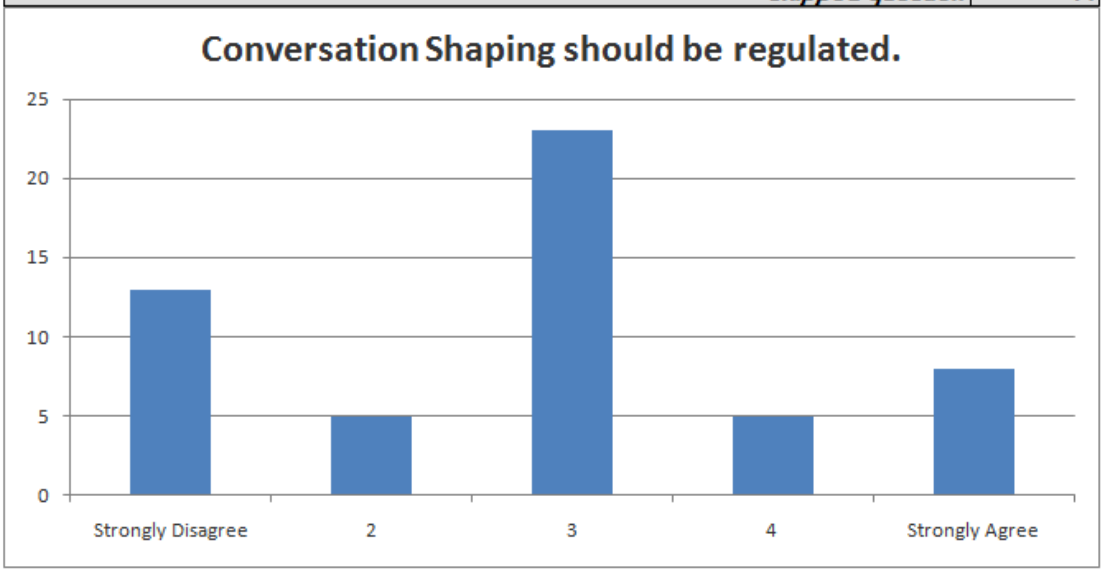

| 5. Phone Tapping should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 12 | 9 | 15 | 5 | 16 | 3.07 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



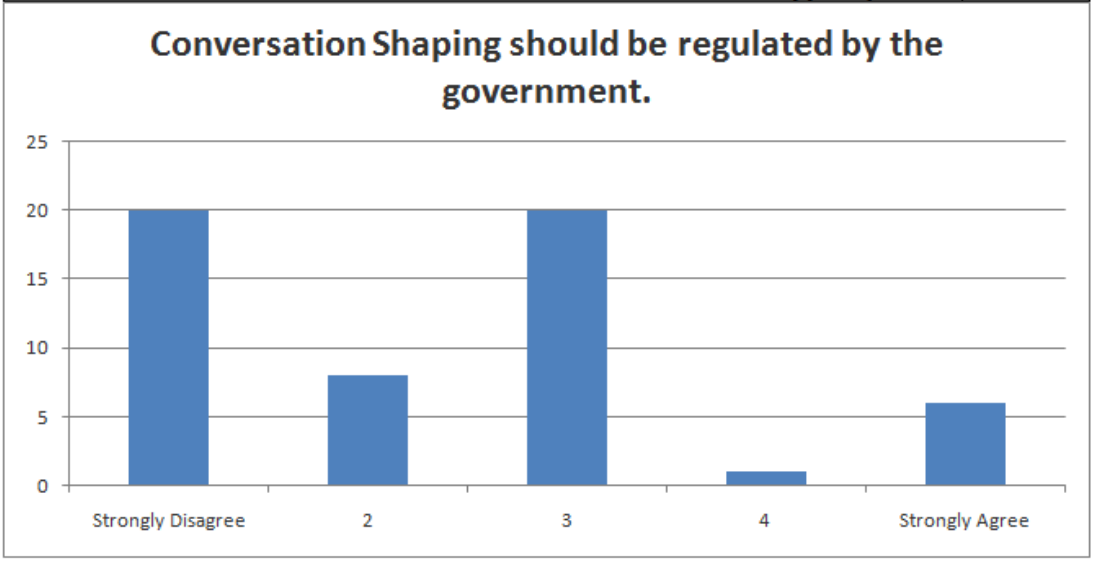
| 6. Phone Tapping should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 15 | 4 | 20 | 12 | 6 | 2.82 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



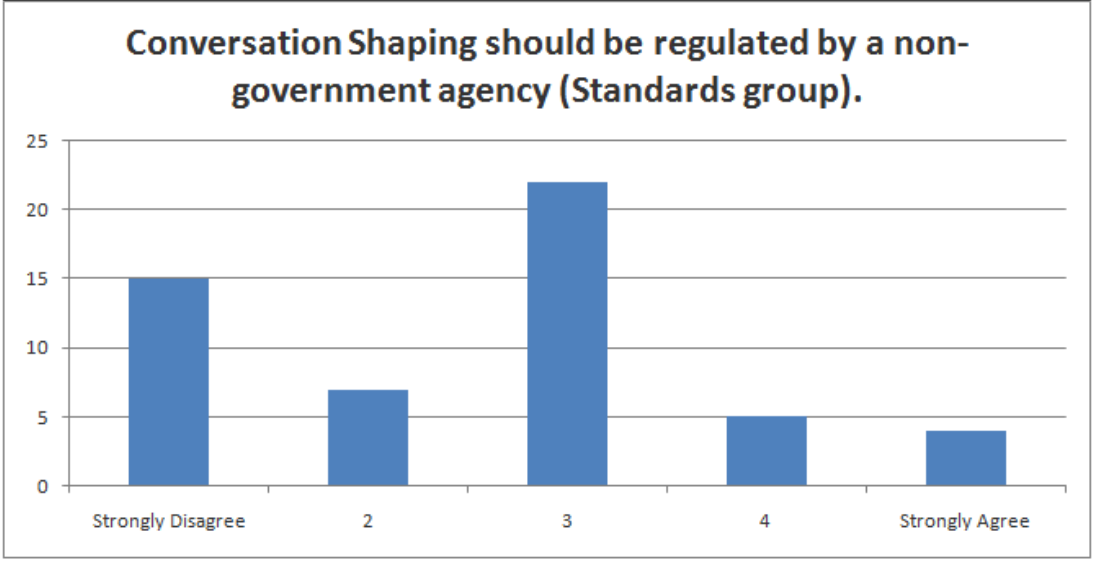

| 7. Conversation Shaping should be regulated. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 13 | 5 | 23 | 5 | 8 | 2.81 | 54 |
| | | | | | | *answered question* | 54 |
| | | | | | | *skipped question* | 14 |



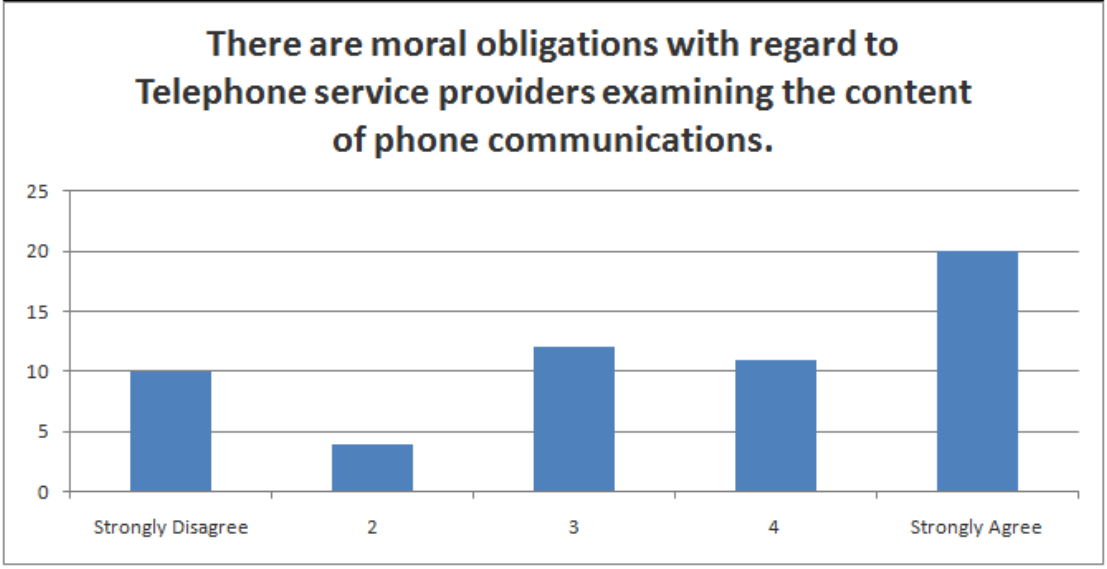
| 8. Conversation Shaping should be regulated by the government. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 20 | 8 | 20 | 1 | 6 | 2.36 | 55 |
| | | | | | | *answered question* | 55 |
| | | | | | | *skipped question* | 13 |



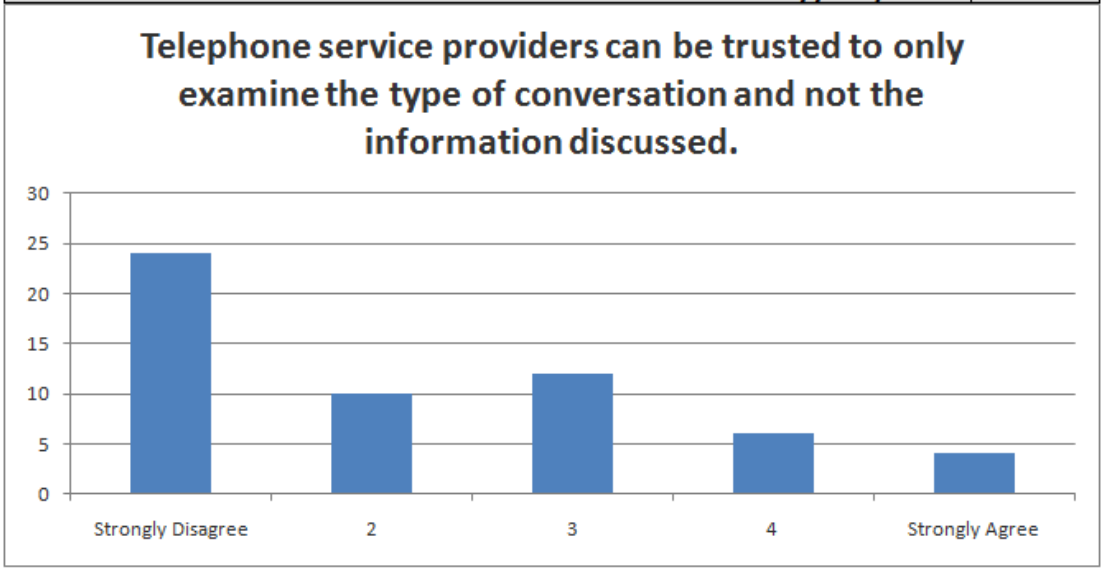

| 9. Conversation Shaping should be regulated by a non-government agency (Standards group). | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 15 | 7 | 22 | 5 | 4 | 2.55 | 53 |
| | | | | | | *answered question* | 53 |
| | | | | | | *skipped question* | 15 |



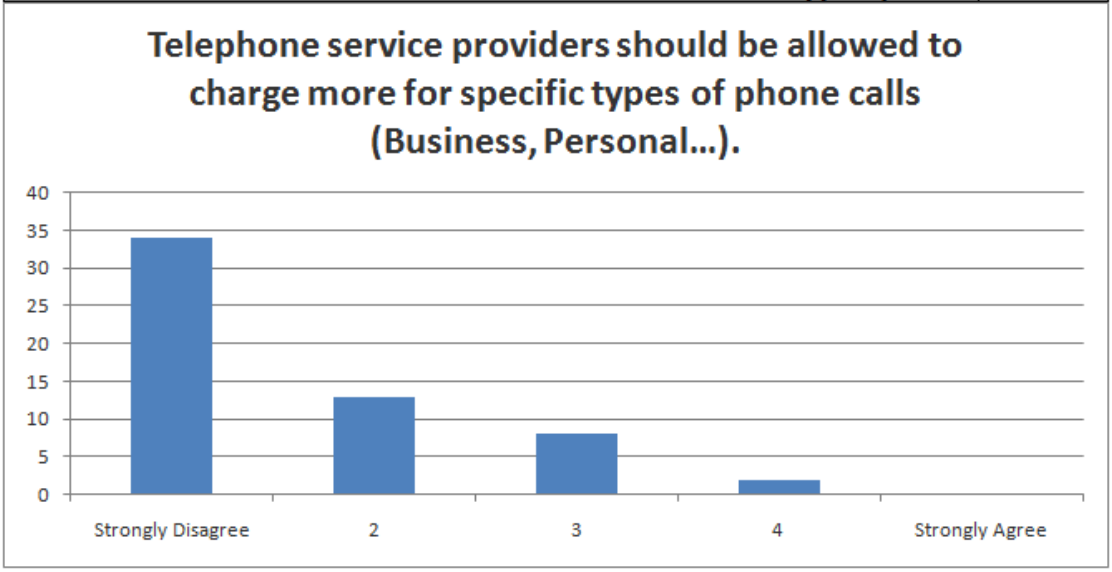
| 10. There are moral obligations with regard to Telephone service providers examining the content of phone communications. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 10 | 4 | 12 | 11 | 20 | 3.47 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |




| 11. Telephone service providers can be trusted to only examine the type of conversation and not the information discussed. | | | | | | | |
|---|---|---|---|---|---|---|---|
| Answer Options | Strongly Disagree | 2 | 3 | 4 | Strongly Agree | Rating Average | Response Count |
| . | 24 | 10 | 12 | 6 | 4 | 2.21 | 56 |
| | | | | | | *answered question* | 56 |
| | | | | | | *skipped question* | 12 |

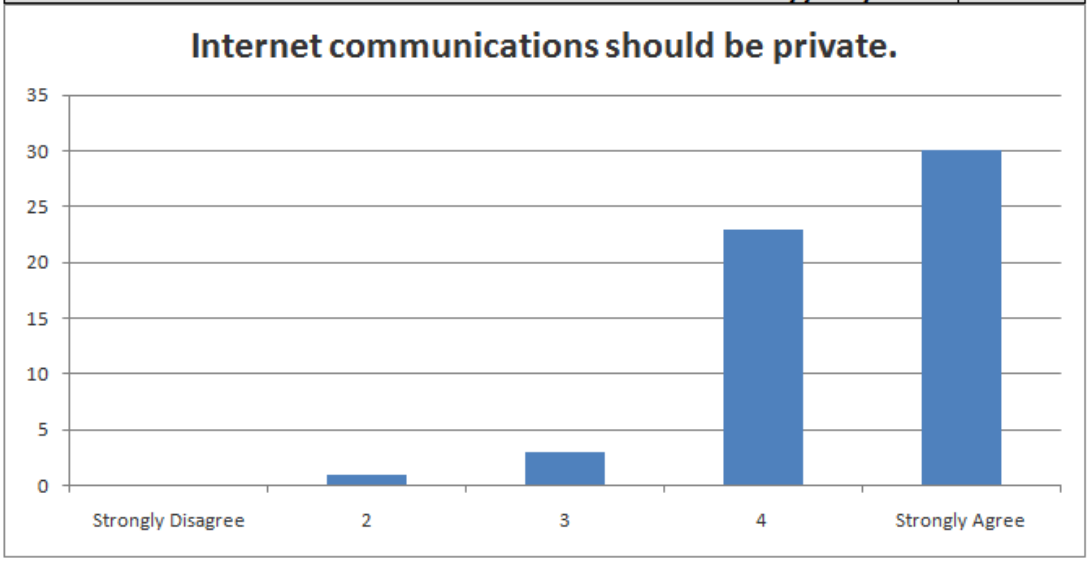
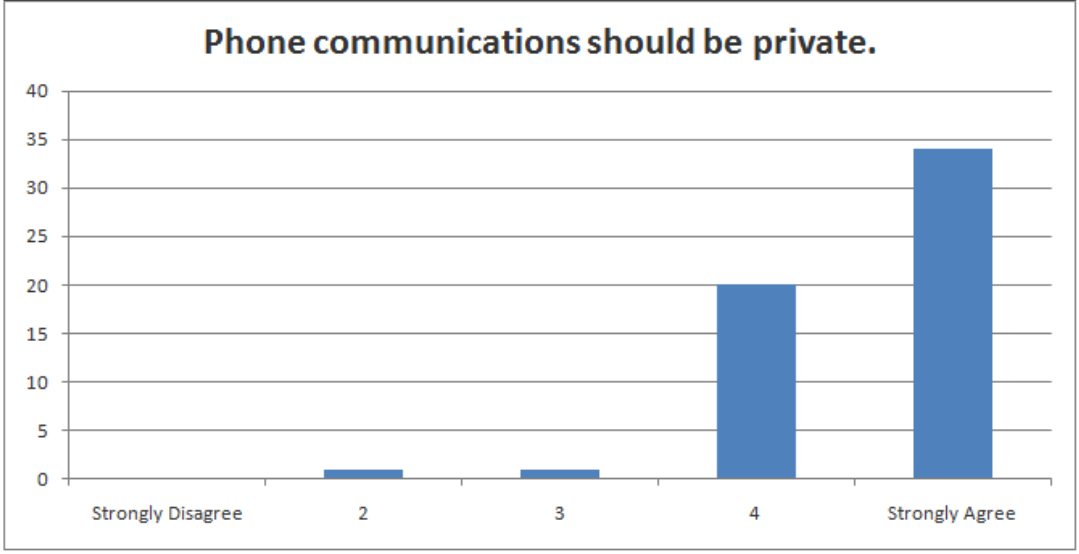


| 12. Telephone service providers should be allowed to charge more for specific types of phone calls (Business, Personal...). | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 34 | 13 | 8 | 2 | 0 | 1.61 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |




Section 4 - PRIVACY OF COMMUNICATIONS (2 questions)

| 1. Internet communications should be private. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 0 | 1 | 3 | 23 | 30 | 4.44 | 57 |
| | | | | | | *answered question* | 57 |
| | | | | | | *skipped question* | 11 |



| 2. Phone communications should be private. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Answer Options** | **Strongly Disagree** | **2** | **3** | **4** | **Strongly Agree** | **Rating Average** | **Response Count** |
| . | 0 | 1 | 1 | 20 | 34 | 4.55 | 56 |
| | | | | | | ***answered question*** | **56** |
| | | | | | | ***skipped question*** | **12** |