



Norwegian University of
Science and Technology

Analyzing the Privacy Policy: Responses and Challenges.

A survey research about the experiences from common users and
service providers?

Murtaza Hussain Shaikh

Master in Information Systems

Submission date: May 2011

Supervisor: Torbjørn Skramstad, IDI

Problem Description

A privacy policy is a legal document intended to tell the user which personal information is obtained, the later use of this and with whom this information is shared. There are many personal data acts and legislations that are responsible to protect privacy, personal information and integrity and ensure adequate quality of this personal information. Many countries /states have these laws but the content is varying. The goal of this thesis is to answer whether the common users are aware of the contents of the policy that is accepted and if it at all is read. What are the known issues, and generally there are too long privacy policies issued by service providers and the policies and the language makes the reading difficult for a common user. In this thesis we have given different prospective of a common users and service providers that are offering their services.

Assignment given on: 20th - January -2011

Supervisor: Prof. Torbjørn Skramstad, IDI – NTNU.

Abstract

The main purpose of this thesis is to investigate how different age categories of users and the service provider's point of view about understandability, technicality, importance and awareness of privacy policy. The emerging ambiguity in information security has raised many privacy and trust issues that are context dependent. Therefore there are several uncertainties and risks seen today concerning the privacy policy & subscriber trust. It is a responsibility of services providers before amending their policy to notify their subscribers. Because if they do not take this initiative then it creates trust deficit for their subscribers and this affects their business and goodwill.

In this work we have adopted the online survey questionnaire technique to perform a research based on the user's ideas and thoughts about the privacy policy and security issues. We have used the same technique with different questions based on the organization's own perspectives on the privacy policy. This would highlight to what extent an organization thinks the policy fulfills the user's confidence. We have decided to target Norwegian service providers and people as participants for this survey, to better understand the theme of research. It took about four months to collect the responses from the organizations and from the participants. This report discusses the importance of privacy policy for a common user / subscriber. Generally observed in this work is that, before accepting privacy policy, it is hard to read these policies and understood by end-user, and taking this prospect ahead, many privacy policies and regulations have a difficult context to understand.

This survey methodology was selected to ensure the originality of the user's state of mind, and it was also vital for the service providers to show their responses and opinion on privacy policy. We have noticed that a majority of the users are not interested in reading the contents of the privacy, and they simply provide their sensitive information without ensuring the authenticity and regulations inside the privacy policy. Furthermore, we observed that users think privacy policy just saves them from viruses and threats, and there is a chance of phishing if it is not mentioned on the service provider website. Most of the service providers have recently introduced the privacy protection seals for secure data transmission on their website in order to build a strong subscriber's trust.

Finally, it is important to continue researching to get better tools and more mechanisms for a good security policy, and to establish guidelines for better understanding as we learn more.

Keywords: *Privacy; Personal information; Service providers; Subscriber's; Policy; Issues; Survey design; Legislation; Settings; Practices.*

Preface

This report is a documentation of a master's work assigned by the mandatory TDT4900: Information Systems Engineering, master's thesis, executed during the spring of 2011 at Department of Computer and Information Science (IDI), Norwegian University of Science and Technology (NTNU).

This work is carried out in the last semester of two years International master program in Information Systems Engineering at IDI. The scope of the master's thesis amounts to 30 units.

The work is submitted in fulfillment of the requirement for master's degree program in Information Systems Engineering at Norwegian University of Science and Technology, Trondheim- Norway.

This work has been defined in consultation with Professor Torbjørn Skramstad at Department of Computer and Information Science. The author wishes to thank for his valuable guidelines, feedbacks, and interesting meetings for the thesis during the period.

Murtaza Hussain Shaikh,
Trondheim, Norway, June 16th of 2011

Acknowledgement

Firstly, I would like to thank Almighty Allah for His protection, guidance and direction throughout my life and for my entire 2-year Master of Science program in Information Systems Engineering at the Norwegian University of Science and Technology (NTNU) Norway.

I would like to express my deepest gratitude and loyalty to my supervisor, Professor Torbjørn Skramstad of Department of Computer & Information Sciences (IDI) NTNU, for invaluable advice, feedbacks and guidance throughout the entire period for this master's thesis work.

Lastly, I would specially like to thank my beloved mother Mrs. Naseem Ahsan Shaikh who always encouraged and imbued me throughout my life; her blessings inspired me for all the achievements of my life and may Allah always keeps her shadow on me (*Amen*).

Murtaza Hussain Shaikh,
Trondheim – Norwegian University of Science & Technology,
June, 16th of 2011 .

Acronyms

APPEL - A P3P Preference Exchange Language. (*P3P defined below*)

AAA - Authentication, Authorization and Accounting.

BBB - Better Business Bureau.

COPPA – The Children’s Online Privacy Protection Act of 1999.

EPAL - Enterprise Privacy Authorization Language created by IBM.

FIP – Fair Information Practice Principles.

FTC – Federal Trade Commission .

GLBA – Gramm Leach Bliley Act.

HIPPA – Health Insurance Portability and Accountability Act.

IDS – Intrusion detection systems.

NCJA- National Criminal Justice Association.

P3P - Platform for Privacy Preference Project.

POL- The Norwegian Personal Data Act 2000.

W3C - The World Wide Web Consortium.

Contents

Abstract	<i>i</i>
Preface	<i>ii</i>
Acknowledgement	<i>iii</i>
Acronyms	<i>iv</i>
List of Figures	<i>v</i>
List of Tables	<i>vi</i>

1. Introduction

1.1. Background and Motivation.....	1
1.2. Problem definition.....	2
1.3. Research objectives.....	3
1.4. Meetings with supervisor.....	3
1.5. Report outline.....	4

2. Background Realities

2.1. What is a privacy policy?.....	5
2.2. What are privacy policy and security trust issues?.....	6
2.2.1. Is a policy context difficult with typical legal jargon?.....	6
2.2.2. Policy context is too long to read and understand.....	7
2.2.3. Standardization of policy context.....	8
2.2.4. Accessibility of policy contents.....	8
2.2.5. Policy structure and presentation of policy context.....	9
2.3. Other related issues.....	9
2.3.1. Wasting time on reading the policy.....	10
2.3.2. No difference among security policies.....	10
2.3.3. Users believe they don't have choice.....	10
2.3.4. Policy does not address the user's concerns.....	10

2.4.	What is a personal information?.....	11
2.5.	What are the main privacy concerns?.....	12
2.5.1.	The phenomena of trust.....	13
2.5.2.	Subscriber`s trust on security policies.....	14
2.5.3.	Traditionalist group versus non Traditionalist group.....	15
2.5.4.	Common user behaviour on privacy context.....	16
2.6	Other related work on privacy policy.....	17
2.7	Summing up.....	19

3. Privacy Legislations and Privacy Principles

3.1.	The privacy principles and guidelines.....	20
3.1.1.	Fairness and lawfulness.....	21
3.1.2.	Limitations on collection.....	21
3.1.3.	Purpose binding.....	21
3.1.4.	Quality of the information.....	22
3.1.5.	The co-determination.....	22
3.1.6.	Security safeguards.....	22
3.1.7.	Sensitivity of data.....	22
3.2.	OECD Guidelines on protection of privacy & Trans-border flow of personal data [2010].....	23
3.3.	The Norwegian personal data act (POL) [2000].....	24
3.4.	Privacy practicing of personal data.....	25
3.5.	EU data protection directive (EUDPD) [1995].....	26
3.6.	EU Convention for protection identification with regards of automatic data processing [1981].....	27
3.7.	United States privacy act of [1974].....	27
3.8.	Other legislations and sector specific laws for privacy.....	29
3.8.1.	The health data filing system act.....	29

3.8.2. The U.S Federal Trade Commission and self regulation.....	29
3.8.3. The U.S children’s online privacy protection act of [1999].....	31
3.8.4. The EU and U.S safe harbor privacy framework of [2000].....	31
3.9. Comparison of privacy acts with common instruments.....	31

4. Research Approach

4.1. Research Questions.....	35
4.2. Methodology.....	36
4.3. Survey research.....	37
4.3.1 What actually is a survey research?.....	37
4.3.2 Elaboration.....	38
4.3.3 Generality in survey & Target audience.....	39
4.3.4 Measurement and data gathering approach.....	40
4.3.5 Accuracy and Relevancy in survey research.....	41
4.4. Survey response.....	42
4.4.1 Survey response calculations.....	43
4.4.2 Maximizing the rate of survey response.....	43
4.5. Questionnaires.....	44
4.6. Types of Questionnaire.....	45
4.7. Advantages and Disadvantages of web based survey.....	46
4.8. Limitations in a survey	47
4.9. Adopting the privacy practices in online surveys.....	47

5. Evaluations, Results and Discussions

5.1. User Survey.....	49
5.1.1 Evaluating results of user survey.....	49
5.1.2 Participants in terms of gender.....	50
5.1.3 Participants in terms of age category.....	50
5.1.4 Participants in terms of education.....	51

5.1.5	Participants in terms occupation level.....	52
5.1.6	Level of Internet usage of participants.....	53
5.1.7	Participants familiarity with the term “ <i>privacy policy</i> ”.....	54
5.1.8	Participants perception of “ <i>privacy policy</i> ”.....	54
5.1.9	Advantages of having a “ <i>privacy policy</i> ”.....	55
5.1.10	Disadvantages of having a “ <i>privacy policy</i> ”.....	56
5.1.11	Reading policy contents before registering.....	57
5.1.12	Degree of difficulty in understanding policy contents.....	57
5.1.13	Relevance of privacy contents as a subscriber.....	58
5.1.14	Level of confidentiality to give personal information.....	59
5.1.15	Amendment of privacy policy contents from service provider.....	59
5.1.16	Request/Review of personal information from service provider...	60
5.2.	Service provider`s Survey.....	62
5.2.1	Evaluating results of service provider`s survey.....	62
5.2.2	Categories of participated organization in survey.....	62
5.2.3	Service provider`s location.....	63
5.2.4	Number of registered subscribers.....	64
5.2.5	Service provider`s importance on “ <i>privacy policy</i> ”.....	65
5.2.6	Standards of privacy regulations and laws.....	66
5.2.7	Response of reading privacy policy from subscribers.....	67
5.2.8	Level of understanding privacy contents for subscriber.....	67
5.2.9	Any review body on setting up “ <i>privacy policy</i> ”.....	68
5.2.10	Retention regulation in service provider privacy policy.....	69
5.2.11	Disclosure of subscriber`s personal information.....	69
5.2.12	Request from subscribers to review personal information.....	70
5.2.13	Level of building confidence & trust for subscriber.....	71
5.2.14	Response of handling privacy violation reports from subscriber...	72
5.3.	Discussion.....	73
5.4.	Trends.....	74
5.4.1	Age category from 20-30 years.....	74
5.4.2	Age category from 30-40 years.....	76
5.4.3	Age category from 40-50 years.....	78

5.4.4	Age category from 50-60 years.....	80
5.4.5	Age category from 60-70 years and above.....	82
5.4.6	Response from the Internet sector.....	83
5.4.7	Response from the telecommunication sector.....	84
5.4.8	Response from the scientific/research/academia sector.....	85
5.4.9	Response from the financial sector.....	86
5.5.	Answering of research questions.....	87

6. Conclusion and Further work

6.1.	Executive summary.....	97
6.2.	Validity and Limitations.....	98
6.3.	The road ahead.....	99
6.4.	Potential research questions for further work.....	99

Appendix A (OECD privacy principles)

Appendix B (Statement of purpose)

Appendix C (Questionnaire format for users)

Appendix D (Questionnaire format for service provider)

Glossary

Bibliography

List of figures

4.3.1	General survey structure.....	38
4.3.2	Spiral link survey achievements.....	38
4.3.3	Generality in survey research process.....	39
4.3.5	Mathematical accuracy and relevancy in survey research.....	41
4.4.2	Maximizing the rate of Survey response.....	43
4.5	Technique of design and write questionnaires.....	45
5.1.1	Number of user participants in the survey.....	50
5.1.2	Response level of gender in survey.....	50
5.1.3	Number of Participants in survey according to age category.....	51
5.1.4	Responses to Level of Education in survey.....	52
5.1.5	Response level of participants on occupation.....	52
5.1.6	Response level of participants on internet usage.....	53
5.1.7	Response of participants over privacy policy.....	54
5.1.8	Response of terminology of privacy policy.....	55
5.1.9	Responses to advantages of privacy policy.....	55
5.1.10	Responses to disadvantages of privacy policy.....	56
5.1.11	Response of reading the policy contents.....	57
5.1.12	Level of difficulty in policy contents.....	58
5.1.13	Response of relevancy of privacy contents.....	58
5.1.14	Level of confidentiality of personal information.....	59
5.1.15	Response of amendment of policy contents.....	60
5.1.16	Response level of review of personal information.....	61
5.2.2	Categories of participated organization.....	63
5.2.3	Response of service provider's location and operations.....	64
5.2.4	Level of registered subscribers of service provider.....	64
5.2.5	Level of importance on privacy policy.....	65
5.2.6	Response of following privacy standards & regulations.....	66
5.2.7	Response reading the policy contents from subscribers.....	67
5.2.8	Level of understanding privacy contents.....	68
5.2.9	Response of having review body on Privacy policy.....	68
5.2.10	Response of following retention regulation.....	69
5.2.11	Response of disclosure of personal information.....	70
5.2.12	Level of request to review personal information.....	71
5.2.13	Level of confidence and trust for a subscriber.....	71
5.2.14	Response of handling policy violation reports.....	72
5.4.6	Response from the Internet sector.....	84
5.4.7	Response from the telecommunication sector.....	84
5.4.8	Response from the scientific / research / academia sector.....	85
5.4.9	Response from the financial sector.....	86
5.5.1	Level of relevancy of Privacy Policy.....	89
5.5.2	Advantages of Privacy Policy.....	89
5.5.3	Disadvantages of Privacy Policy.....	90
5.5.4	Reading and Understanding of Privacy Policy.....	91
5.5.5	Importance on Privacy Policy.....	92
5.5.6	Amendment of Privacy Policy.....	93
5.5.7	Retention regulation in service provider policy.....	93
5.5.8	Disclosure of personal information from service provider.....	94
5.5.9	Level of confidence from users.....	95
5.5.10	Privacy violation reports from subscribers.....	95
5.5.11	Confidentiality of user personal data.....	96

List of Tables

3.9 Analysis of different Privacy Laws of different countries.....	32
5.4.1 Analysis in tabulated form in terms of percentage(20 To 30 years).....	75
5.4.2 Analysis in tabulated form in terms of percentage(30 To 40 years).....	77
5.4.3 Analysis in tabulated form in terms of percentage(40 To 50 years).....	79
5.4.4 Analysis in tabulated form in terms of percentage(50 To 60 years).....	81
5.4.5 Analysis in tabulated form in terms of percentage(60 To 70 years).....	83

Chapter 1

Introduction

This first chapter describes the overall situation of privacy and security policies and defines the research objectives for the work. It outlines the development that has taken place in past decades, making users more aware about the notion of privacy and privacy policy.

1.1. Background and Motivation

More than a century ago, Warren & Brandeis have defined privacy as *"the right to let alone"* and *their concern about privacy was quite prompted* [1]. The emerging ambiguity in information society has raised many privacy and trust issues that are context dependent. These issues will pose many challenges for policy-makers and stakeholders because people's notion of privacy and trust are different and shifting [2]. Policies are considered as a fundamental factor to provide security and privacy in applications such as, file sharing, Web browsing, Web publishing, networking, and mobile computing. Such applications demand highly accurate policies to ensure that resources remain available to authorized access but not prone to compromise. The policies of the past are not suited to deal with new challenges and we are probably entering into new era that would require developing more effective policies. There are lots of uncertainties & risks today concerning our privacy & trust. It is also seen that people are sometimes compelled in circumstances to surrender their personal data to gain something [2]. Two non-expert groups of policy authors are on the rise. First are the non-technical enterprise policy authors, typically lawyers or business executives, who have the responsibility to write policies governing an enterprise's handling of personal information [4]. Second are end-users, such as that wish to set up their own spam filters, share photographs, videos or important files with friends but wants to protect them from unwanted access [5]. It is important to continue researching better mechanisms for security & privacy policies authoring and to establishing good guidelines; because to achieve the best security goals it's crucial to obtain high quality to ensure the intended policy. This work shows the current role of privacy policy in policy management, but it is still

immature in making security analysis and assessments [6]. Furthermore with this research, the interest to make the organizations flexible with respect to privacy matters, consistent over the design of policy language that could be enforceable. It may be fruitful for users if policy decisions with a higher impact were presented in a different manner. In last this would be helpful for the upcoming policy authors to understand the users` concerns and experiences in terms of privacy.

1.2. Problem definition

In privacy policies, what information is collected and how does the user experience this? A privacy policy is a legal document that it intends to tell the user which personal information is collected, the later use of it and with whom this important information is shared. The focus within this work is of acquiring complementary knowledge from the literature and other authentic sources of information. As the result, this thesis will mainly focus on elaborating the state of the art technology and drive insides on the core topic. In this work we have outlined our direction only on the following overarching aspects;

More concretely we want to look at;

- ✓ How important of a privacy policy for a users to accept them.
- ✓ How the contents of privacy policies are read and understood by common users.
- ✓ From the common users` perspective the policies, do they have a language that makes them difficult to read and understand.

And from the perspective of organization or service provider;

- ✓ What role they play in framing the trust and confidence of their registered subscribers.
- ✓ In what way the policies presented by service provider addresses the users` concern.
- ✓ How frequent a user requests for his/her personal details under the personal data protection act, regulation or some legislation?

Many developed countries have laws to protect privacy and have privacy & personal data acts & regulations. Most websites that allow users to register as members have such a privacy policy. These can often vary in content and how they are presented to the common users. So the scope is that user aware of contents of the policy that is accepted. Known issues that policy contents are often too long and the policies have a language that make them difficult and confusing to read and understand.

1.3. Research objective

Following are the main research objectives for this research project;

- To review the current status of the privacy policy offered by different organizations.
- To study whether the privacy policy is a crucial phenomenon in security management.
- To identify whether the policy language creates ambiguity in terms of understanding from the user's side.
- To trace the simplest method to prevent the conflicts for setting up the privacy policy.

1.4. Meetings with supervisor

The meetings with the supervisor are not generally planned, if require an urgent meeting the email would be sent to the supervisor (torbjorn@idi.ntnu.no). All meetings are mostly being held inside the supervisor's office in IDI –NTNU. During the meetings the supervisor approves and checks the status of the project and the report structure. Meetings were mostly setup for feedback and guidelines. The supervisor helped a great deal with the report.

1.5. Report outline

Below is a brief outline of the different chapters of the report.

- **Chapter 2: Background Realities:** This chapter describes the related / pre-study conducted under this thesis. The chapter focuses on some general information regarding the work.

- **Chapter3: Privacy Legislations and Principles:** In third chapter we would underlying the complexity of privacy legislations and principles that forms that basis of contents and structure in today's era. We will also describe different guidelines and set regulations adopted by different regions, organizations and states.

- **Chapter4: Research approach:** This chapter states the research questions that we seek to be answered in this study. It also describes the research methodology adopted for this work.

- **Chapter5: Evaluations, Results and Discussions:** This important chapter highlights the information gathered via adopting the above research methodology and gives the analysis over the facts and information gathered.

- **Chapter 6: Conclusion and Further work:** The last chapter will finally give the conclusion and observation that were concluded. Additionally there is an executive summary about over all results especially the further work. It also discusses whether the work with this project has provided sufficient results in order to answer the research questions and achieve the research objectives. The chapter will propose the further work on the topic along with validations and limitation on this research.

Chapter 2

Background Realities

This chapter includes a literature review, privacy & trust concerns and other related aspects and also a discussion of different studies done on this topic. This review is done to get a good basis for specifying the ground of this area and creates a sense about the level of the users' concerns on privacy policy.

2.1 What is a privacy policy?

In today's technological world, millions of individuals are subject to privacy threats. There are many companies that are hired not only to be a watch-dog but also keep a check and observe what you visit online. People set up accounts for facebook ,twitter, linkedIn and enter bank a credit card information to various websites [14]. A privacy interim of policy is a document which provides guidelines to users on the processing, storage and transmission of sensitive information. The primary goal is to ensure that information is appropriately protected from modification or disclosure [20]. A definition of security policy can be highly formal or informal. Security policies are enforced by organizational policies or security mechanisms. A technical implementation defines whether a computer system is secure or insecure. These formal policy models can be categorized into the core security principles: confidentiality, integrity and availability [19]. This simply reflects that a privacy policy is a higher level context of secure behavior; it has no meaning to claim an entity is secure without actually knowing what secure means [19]. *“It is also foolish and senseless to make any significant efforts to address security issue without tracing the effort to a security policy”* [21]. If it is important to be secure, then it's compulsory to be confident that the privacy policy is enforced by procedures that are quite reliable and strong enough. There are some systematic methodologies and risk calculation strategies to assure completeness of security policies and assure that they are completely enforced [21]. In a complex real time computer system, such as information & communication

systems, policies can be easily be decomposed into sub-policies to facilitate the allocation of security mechanisms [21]. The examples for this could be satellite systems or a media broadcast efficient systems etc that easily facilitate the allocation of security mechanism for enforcing detailed sub policies to properly guide a user.

2.2 What are privacy policy and security trust issues?

Privacy policies are meant to protect the privacy of the user: they need to reflect current regulations and possibly promises made to the customers. *“A privacy policy is a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer's data. The exact contents of a privacy policy will depend upon the applicable law and may need to address the requirements of multiple countries or jurisdictions”* [13]. While there is no exact universal guidance or recommendations for the content or text of specific privacy policies, a number of organizations provide example forms, templates or online consultant for this purpose [13]. Privacy policies arise further issues in comparison to access control policies, as they require a more sophisticated treatment of deny rules and conditions on context information; moreover privacy policy languages have to take into account the notion of “purpose”, which is essential to privacy legislation [89]. *“A subset of privacy policies are enterprise privacy policies which furthermore have to provide support to more restrictive enterprise-internal practices and may need to handle customer preferences”* [89]. This means that an enterprise level privacy policies plays a vital role to increase the loyalty with the users. A good reason for supporting enterprise privacy policies that it not only regulates access to data, but can impose some (i.e. obligations like to delete a data set within two weeks or simply notify the customers of the business firm) [89].

2.2.1 Is a policy context difficult with typical legal jargon?

Many researchers and experts of system security are asking the question; why do few people read the privacy policies? [52]. One common fact is simply that policies are often written in a hard and complicated language which a common user or subscriber cannot understand [52, 3].

In privacy notice research conducted by [53] the research is conducted in 2001 and in that research, 29 percent of the respondents expresses their feelings that policy contents are very difficult to read and 45 percent of respondents said that it was difficult to understand them. Another good reason subscribers have given for not understanding the policy is that they contain a lot of legal and lawful jargon [53]. In the survey by Milne [54], about 53 percent of the respondents agreed, or strongly agreed to, that privacy notices often use legal language which is very hard to understand or is confusing for most people. Same as described in [55] those policies use certain statement and distinct vocabularies which made them very hard to understand, even for the experienced reader.

2.2.2 Policy context is too long to read and understand

An interesting reason why subscribers find policies hard to understand has been found to be its length. As discussed in [53] 21 percent of the 29 percent which answered that they did not read security policies because they are too hard to understand, gave policy length as the reason for this. In the same study, 77 percent responded that they *“prefer a short privacy policy because a longer privacy policy makes it too confusing to understand how user personal information would be collected and used”*. Similarly, 68 percent of the respondents agreed when asked if they often found privacy/security policies too long to be useful in the survey [54].

A recent study conducted by [56] found that the policies in general were very legally framed and were too long to be expected to be read by most users and about 12 famous websites had policies longer than *3000 words*. Length of policies has also been measured in the times it takes to read it and as we mentioned in [31] that it took about ten to twelve minutes to read the privacy statements on the most popular websites. The evidence for lengthy privacy policies has also been discussed in [55] which highlights that common users often would not read the statements and they did not find any meaningful relation between the privacy policy and a common user or subscriber. This concept is also claimed by [57] that there is no linear correlation between the length of a policy and its complexity when designing privacy policies.

2.2.3 Standardization of policy context

Lack of standardization of privacy policy contents is also a problem. Different websites use different ways for structuring the information in their policies. Many service operators claim that their security statement first explains what particular information they are collecting and then how they will use those details [58]. Other service operators tell where on the website they would collect personal information, and then explain what they will do to protect this information [58]. Some service operators post on their website F.A.Q (*Frequently Asked Questions*) format focusing on answering the most common questions that mostly asked by the users regarding their privacy [58]. There is no particular standardization adopted across the organizations / companies for comparison [55]. The ability to compare policies could be helpful in many situations (e.g. where users have a chance to select a company /organization to fulfill its requirements on privacy and security).

2.2.4 Accessibility of policy contents

Recent studies have found that there are accessibility issues with privacy policy [56]. A study conducted in 2009, says that in forty five different social networking sites just fifteen sites opened their privacy policies in a new window which could be blocked, interrupted or inaccessible from the mobile devices [56]. It was also found issues where a JavaScript was a requirement to access the policy in those sites the policy contents could not be saved, printed or zoomed. It was also found that only 2 pages scored perfect on a mobility access test. Location and format of the policy has also been found to be a critical issue [55]. In their problem formulation, [58] the author claimed that the link to a privacy document is often difficult to spot, often hidden at the bottom of the website in very small font. This claim is, however, not supported in a more recent study by [7], where it was found that the privacy policies examined generally had good accessibility, with a consistent location of the privacy policy at the bottom of the homepage (around 86 percent of the privacy policies). It was found that despite the unglamorous location, the consistency provided the user with a location clue of where to find the policy [7]. A survey conducted in 2001 found that 48 percent of the respondents agreed strongly

that privacy notices were easy to find [54] and only 22 percent of the users disagree to the same concept. The author of [7] did, however, find that some pages (about 8 percent) used a formatting on the link, removing the typical link underlining, and other pages (about 27 percent) used a reduced font on the policy link which could explain why some users had troubles locating it.

2.2.5 Policy structure and presentation of policy context

Other major problems including the presentation and privacy policy structure and navigation in it has also been taken into an account. As a monolithic structure, security policy navigation is context independent, meaning that the policy always tells the same story in the same order [58]. For example, if a common user is looking for certain information in the policy, he/she still has to look through a lot of irrelevant information to get the exact point. This could lead the user to avoid the hurdle of finding the information they are interested in and to avoid the confusion or hurdles of finding the relevant information they are searching [58]. As policies can vary in length, how much information the user has to go through varies from policy- to-policy. Some websites choose to separate their security statements into several html pages with a main policy page with links to additional definitions [7]. Further it was found that while this practice may make policies less intimidating to users, it has the potential to be obscure. This practice has great potential for hiding facts from the subscribers. This indicates that just splitting the policy across several pages might help common users and subscribers more easily trace what they are looking for, but at the same time introducing a new problem of hiding important details. In a 2001 survey, only 3 percent of the users respond that they did not read the service provider security policies because the print was too small or difficult to read and understand [53].

2.3 Other related issues

We have noticed and discussed in the previous section that the language used and the policies accessibility together with various user expectations is the main reasons for why the users don't read the security policies. However, several other reasons have been found as well.

2.3.1 Wasting time on reading the policy

Here we would like to mention that "*Time is money*" said by Benjamin Franklin of USA in 1788 [88]. The issue with lack or waste of time can also be seen from an economical viewpoint, where time serves as a potential cost, and the time it takes to read the privacy policy may be a serious barrier [63]. It has been found that if the cost for reading privacy policies is too high, people are unlikely to read policies [63]. The cost of reading them would outweigh the potential benefit for reading the policies.

2.3.2 No difference among security policies

A very common prospective of a policy is that a common user or a common subscriber believe they all are the same and the content resemble with every privacy policy, and there is no big difference [7]. We have mentioned this before in other sections that in 2001, a survey was conducted and in that survey 12 percent responded that they did not read privacy policy because they felt they all say the same words, and 25 percent believe that they do not have time to view because of the length of policy contents [53].

2.3.3 Users believe they don't have choice

It is a strong belief that a common user does not actually have a choice, when it comes to their personal information. Based on expectations, they believe there are no options available for limiting or may be controlling an organization for using their personal information and other personal details [62]. This important fact is also supported by [7].

2.3.4 Policy does not address the users' concerns

Among other reasons for why users do not read the privacy policy it has been found that they do not address the users' concerns [59,60], that there exists a mismatch between what privacy policy documents express and what a common user wants these documents to express [61], and that they lack clarity for users to find them useful [55].

2.4 What is a personal information?

The definition of personal data is given as “*any information concerning the personal or material circumstances of an identified or identifiable person*” [39]. Another definition says that “*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors that are specific to his or her physical, physiological, mental, economic or social identity*” [42].

This definition implies that whether or not data is considered personal depends on whether or not the person who the data concern is identified or identifiable. The data is considered non-identifiable if the nature of the indirectly identifying data are such that identification of the individual is only possible with the application of disproportional effort, or if assistance by a 3rd party or 3rd vendor outside the power and authority of the individual responsible is necessary [46]. We have noticed that the concept of identification is rather ambiguous, and no clear definition of when data is identifiable is provided yet. [47] defines the concept like “*a raw data are numbers, characters, images or other outputs from devices to convert physical quantities into symbols, in a very broad sense*”. This concept is clearly elaborated that such representations or values do not make any sense without context. (E.g. a number 12345-6789-112 does not make any sense or gives any particular information about a person, unless we know the name), when personal details are put into context our understanding, then it can be easily traced and tracked [38].

- How to process the personal data / identifications?

It is specially defined in Norwegian personal data act 2000 about the terms processing of personal data as any use of personal data, such as collecting, storing, deleting, and disclosing or a combination of these [41]. The law applies to all processing of digital personal data even if only a part of the process is done digitally in Norway.

- What is Data Subject in process of personal data?

The data subject is the identified or identifiable individual whom the personal data is concerned. Personal data can concern more than one data subject [38].

- What is a Data Controller in process of personal data?

“The data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data” [46]. It is clearly explained and mentioned that processing means every form of usage of personal data [41]. It must be kept in mind that the data controller can be one or more persons, or an entire organization/institution. The data controller also determines which technological facilities that will be used in the process [38].

- What is a Data Processor in process of personal data?

The data processor is a natural or legal person, public authority; agency or any other which process personal data on behalf of the data controller [41, 42, 46] and that can be the same organization or person as the data controller, or a different organization processing the data on behalf of the data controller. The data controller is still responsible for actions done by the data processor on the data controller’s behalf [38].

2.5 What are the main privacy concerns?

The privacy threats of which people are concerned include;

- Visit to the websites will be tracked secretly without informing the user [19].
- E-mail ID and other confidential & personal information will be stored and used for marketing, publicity and other similar purpose without permission of the user [19].
- Personal information will be sold to third parties/vendors without getting permission from user [19].
- The credit card details are often stolen [19].

The advances of internet & database technologies increase information privacy threats. Data entered into forms or contained in existing databases, can be combined almost effortlessly with banking transaction records, and records of a user's every click of a mouse on internet. Privacy

concerns increase further as data mining tools and services become more widely available [10]. There is a potential for fraudulent activities on the internet, as few regulatory standards exist [16]. The security of banking card information for online purchase is also incorporated with the privacy concerns. Amazon.com admitted that hackers undetected over four months have stolen about 98,000 bank card numbers. Hackers from time to time publish a list of stolen card numbers and related information over the internet [16]. The information without permission may lead to a fraud, which has very serious consequences [10]. Although personal information may not be used after collecting them, it must be noticed that keeping information is a liability for a website when it meets some good consumers or some old users that take the safeguard of their privacy seriously. The Internet based businesses should take good care of the privacy concerns because the common consumer does not really care about going through every line of policy context. Surveys show that people are more comfortable if they see privacy statement has been approved by a third party, such as Trust-E [17, 18]. To boost the e-commerce environment, information privacy concerns should be treated seriously as they are discouraging users from using the internet in shopping and services [10].

2.5.1 The phenomena of trust

The phenomena of trust has been described as *“the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trust or, irrespective of the ability to monitor or control that other party”* [64]. Electronic commerce research has found trust to be strongly related to information disclosure because trust is like a faith for a user and if it is lost, then user would not try to buy any item from that particular organization and it will impact directly organization’s business [65]. Several models have been proposed to measure a subscriber trust, where most of them emphasize to have a strong vital role in forming a good trust with subscriber. Among all, individual differences found to influence trust is gender [66] amount of internet experience [67] and cultural background [68]. These individual differences are also likely to be influenced by *“consumers’ awareness of Internet fraud and their past experiences regarding both the Internet and other situations involving risk”* [69] and their tendency to be risk averse or they may be risk seeking [69].

A fundamental aspect here is also the type of information requested. The risk associated with sharing information online has been associated with the type of information required [69]. A common user might share information even if the level of trust is very low and conversely if the perceived level of risk is very high, they might sustain from sharing unless there is a high level of trust. Therefore, the level of willingness to share information is not only depending on the level of trust but also on the level on potential risk associated with the type of personal details required [67]. There is enormous variability in the types of information requested by service provider websites. While some websites only require basic information such as name or address, others might request sensitive data such as social security number, passport number, and taxation number. Online shopping has gained significance in recent years, requiring information such as credit card numbers and bank accounts to complete transactions. In the study done by [69] it was interestingly found that users were more willing to provide contact (e.g.: address, telephone number, country code etc) than biographical information and, likewise biographical information rather financial information.

2.5.2 Subscriber`s trust on security policies

Just like other studies have discussed on users` trust on privacy statements, a study conducted by [69] also discovered that respondents were most willing to provide information with a strong privacy statement. Based on the responses for providing personal information, it appeared that many Internet users would be unwilling to provide personal information online, except when offered a strong policy statement. In this context, the importance of the privacy / security policy becomes apparent. It is the only way a website can communicate privacy issues with the users. The article [69] concludes by showing strong concern for the low percentage of policy readers, given the impact that such statements would purportedly have on consumer trust. It has however been found that consumer trust relies on other aspects than the privacy policy. Studies have found that users tend to not read the whole privacy policy because they gained trust to the company through previous experience [75]. Almost half of the respondents in the study by [54] agreed or strongly agreed; when asked if they did not read the privacy policy because of pervious offline experience with a company and just 25 % disagreed. Similarly in the same study 45%

agreed that they do not read the policy contents if it belongs to a well known organization or by a well repudiated service provider. Other studies have found that previous experience is not the only factor for having trust in a site, but also just the presence of a privacy policy. In a 2000 survey, about 66% responded that they got increased confidence in a site if a privacy policy was present [76].

In other words, by just seeing a privacy policy posted some users may believe that the sites they are visiting are safe in terms of privacy. They may also naively believe that *“a security policy exposes a website to potential legal action; a website will always adhere to its policy”* [76]. These findings can be related to that some users believe policies are all the same, look like and have same context and that just by seeing it posted could make them believe its content is similar to other policies. It has also been found that just the quality and professionalism in the website itself is enough to build a strong trust. If the website looks mature and well maintained it is more effective in establishing trust than the existence of a privacy policy [76].

2.5.3 Traditionalist group versus non Traditionalist group

If we go deeper in privacy and security issues we would also find different user groups and believers on privacy. Users are classified in to 3(*three*) main categories; the traditionalist privacy concerns group, the pragmatic user group, and the non-traditionalist group [63]. The first group which is traditionalist privacy group is characterized as “extremely concerned” about their privacy and any use of their personal data, information and generally they are unwilling to provide their data to a service provider website [77]. It has been estimated that around 17% of users belong into this category [78]. The users in this category are less likely to join any social networking sites and events and are seen on as less valuable customers because of their importance on privacy ; unwillingness to provide personal details and they *“actively investigate service provider website and they would complain if they feel dissatisfaction”* [56].

Probably in this group users might be journalist, bloggers, parents and government officials who all disproportionate influence over other comments / opinions [79] and they have also been found

to be twice as frequent as the two other groups to report having been a victim of an invasion of privacy on the Internet.

The second group and the majority of users are pragmatists, and also considered to be concerned about their use of personal information, but less than the fundamentalists. As opposed to fundamentalists, the concerns of the pragmatists are often significantly reduced by the presence of privacy protection measures such as a security law or some authentic statement on service operator`s website [77]. It has also been found that pragmatic users claim to be concerned about their privacy when asked, but tend to forget about the privacy when offered efficient and attractive services [78].

The third and last groups of the subscriber /user are most likely to provide personal data and are thus much less concerned about the security and privacy issue. It was however, found that they under some situations value their personal data and express little concern about privacy [77]. One interesting finding about this and the pragmatist group is that providing them with more assurance of privacy can actually make them less comfortable than simply ignoring privacy [56]. In other words, just mentioning privacy issues to non-fundamentalists might raise their privacy concern. The author of [56] has described the term privacy salience in his article and it has been shown that even promoting positive privacy practices might have a negative impact on users initially not concerned about their privacy. Based on the findings, [56] proposed that a successful website of service operator needs to show responsibility on the concerns of traditionalist group while simultaneously minimizing the awareness of privacy for the non traditionalist group.

2.5.4 Common user behaviour on privacy context

Most surveys have presented their findings that users do have concerns about their privacy, it has also been found that their behavior rarely reflects those concerns and that they do not take steps to actively protect their privacy online [70]. In a survey, it was found that only 16 percent of the respondents had purchased tools to prevent privacy theft [71]. Further studies have indicated

that users will express very strong concerns about privacy of their personal information, but be less than vigilant about safeguarding it [72]. According to the survey of [71] , conducted in the year 2001, approximately 24% of the users actually disclosed personal information that was not required to complete a transaction [73] , violating their stated privacy concern. It was found that even though most individuals stated that privacy was important to them, most participants did not live up to their self-reported privacy preferences and as much as 35 to 40 percent of the participants provided their home/contact address without any reason. A common user actually disclosed so much information about themselves; that a relatively revealing profile could be constructed on the basis of only one shopping and found it alarming that the user`s behavior stood in such sharp contrast to their self-reported attitude [73]. Users have also shown to be willing to provide personal information in exchange of a small reward. This was found in a 2002 subscribers study by Jupiter Research U.S , where 82 percent responded that they would give personal information to new shopping websites in exchange for a chance to win just \$200 USD in a sweepstakes (i.e. a risky venture that promises to give reward) [70, 74].

2.6 Other related work on privacy policy

There are many studies that highlight the difficulty in developing privacy-protecting and trust-enhancing policies. It may even be difficult to write domain-specific policies, because even within the same domain, differing circumstances may call for differing privacy protections [2]. The internet allows for the efficient, inexpensive collection of information without the user's consents. It can track users in unique ways whether or not a users is aware of it. This may include user's preferences, interest or even sensitive credit card information and bank account details. The Federal Trade Commission (FTC) U.S Government conducted a survey in March 1999 and it discovered that 92.8 percent of websites were gathering at least one type of identifying information's like (name, surname, father name, email address, telephone/cell number, permanent address),while 56.8 percent were collecting at least one type of demographic information (gender and preferences).The monetary value of this information explains why so many websites are gathering this sort of information and what is their intension with that sensitive information [12]. Highlighting again the report of FTC published in United States of America (1998), the commission examined the practice of *1,400* commercial sites on the

internet. Although 85 percent of the sites surveyed collected personal information from ordinary consumers, only 14 percent provided any notice of the purpose of collection, and only 2 percent provided notice by way of a comprehensive privacy policy [15]. The above results show that personal information is being collected from websites, most of which do not have a good comprehensive privacy policy [15]. It is a fact that Internet is an international network, and largely unregulated. This also means that the laws of any single country do not usually apply to Internet activities originating in order countries. Thus it is necessary to discuss how a privacy policy and its protection could be achieved in a globally and in a consistent manner. The global consistency on internet security and privacy protection is compulsory factor to boost the growth of commerce. To protect a local subscriber or a common user (whether it is a buyer or a seller) in a global consistent manner, a proper legislation, self-regulation, technological solution and combination solutions are different means that have be implemented [10].

In [11] the author has also noted that "*the notion of privacy is fraught with multiple meanings, interpretations, and value judgements. Nearly every thread of analysis leads to other questions and issues that also cry out for additional analysis; one might even regard the subject as fractal, where each level of analysis requires another equally complex level of analysis to explore the issues that the previous level raises*".

On the other hand in the context of legislation the privacy advocates that the legislation and regulation is needed to stop the internet data collection and authorization without any permission. Other positive people and supporters for legislation suggested regulating the privacy concerns and issues by law better; if and only if self regulation fails to address privacy issues & concerns adequately. The people that votes against privacy legislation argued that compliance cost (whether in terms of time or money) is a major concern. In fact the creation of legislation does not necessarily generate higher compliance costs than a self regulatory regime. This also indicates that legislation may not be enforceable unless it is properly organized [15]. The voice of a local user about their privacy is rising day-by-day. Users worry about the security of personal information and fear that it may misuse in future. They are concerned about how their personal information may be treated now or in future after it has been collected [15].

2.7 Summing up

By analysing the related work done on the trust and privacy issue, it can be concluded that there is a lack of awareness in designing and implementing the policy framework and setting up its contents. A common user is not confident in protecting the personal integrity and ensuring adequate quality for his personal information. The above work is not reflecting to tackle the language difficulty and a proper way to present it.

Chapter 3

Privacy Legislations and Privacy Principles

This chapter is highlighting the necessity to understand the complexity of the underlying legislations and regulations that form the basis for the current content and structure of privacy policies in today`s era. We will see that different approaches to regulate privacy protection has led to a global patchwork of privacy laws, regulations and enforcement mechanisms which vary greatly from state to state, region to region , adding complexity to the privacy landscape. Many of the laws and regulations enforced today do however have something in common which is that they are based on privacy principles and guidelines developed over past 40 years. We will therefore begin this chapter by looking at these principles and guidelines, before turning our focus to historical regulations in some OECD member Countries, United States (*US*) and European Union (*EU*).

3.1 The privacy principles and guidelines

The basis for privacy principles worldwide can be said to be the fair Information Practice Principles (FIP) which was first formulate by the US. Department of Health, Education and Welfare Services in the year 1973 [31]. These great principles can be seen on as a set of ideas around data use and FIP itself does not carry the force of law, but provide a set of principles for legislation and government oversight [31]. Despite advantages in the technology the last decade, and the fact that they predate the internet, they still remain universal recognized to bring any privacy standards onwards [32]. Some of the fundamental principles described below are presented by the authors *Schartum & Bygrave* [38]. Here they state all the principles are full abstraction that is supposed to be taken from all the legislation and laws on data protection & identifications of different regions, States or Countries. These principles are also guidelines for the Data Inspectorate in Norway (*Datatilsynet i Norge*). Since the privacy interests affect the passing of new laws, the principles that can be derived from the legislation

correspond to the interest in many cases. These principles will, in many cases, correspond to the principles presented by OECD guidelines, the article 6 of EUDPD Data law (1995), and US COPPA 1998 [39]. In the following sections we would highlight some basic privacy principles that are supported by the FIP.

3.1.1 Fairness and lawfulness

This principle implies that personal information should be handled fairly and lawfully. Behind this important principle is a requirement that the data controller should respect and take into consideration the data subject's interests and reasonable expectations [38]. The data subject should not be forced to submit personal information or to accept that this information is used to other specific purposes. The data subject should be informed of the purpose of the collection of the data, and the processing of the data should be understandable [38].

3.1.2 Limitations on collection

The basic purpose of this principle is to limit the amount of data collected to what is necessary to carry out further processing of the data which corresponds with OECD's collection limitation principle. In [38] the authors mention that there is not enough reason that the information is useful, the information must be necessary. The further processing of data should correspond with the purpose of which the data was collected for [38]. When the data is not longer necessary to fulfill the purpose they should be deleted or made anonymous [38]. This principle does also propose that individuals should be able to be anonymous in transactions with other service provider.

3.1.3 Purpose binding

This principle means that personal information should be handled to a stated, legitimate purpose and should be handled to this purpose only. The purpose should be stated in a reasonable accurate way not later than at the time the information is collected, which complies with the purpose specification principle and the use limitation principle of OECD [38].

3.1.4 Quality of the information

This principle is concerning the quality of the information. The information should be correct compared to what the information is supposed to represent [38]. The information should also be relevant, adequate and complete based on the purpose of which the information is to be used, and to be up to date, which correspond with the data quality principle of OECD [38].

3.1.5 The co-determination

This principle implies that the data subject should to a certain degree be able to participate and influence other's processing of information concerning it [38]. Persons can decide themselves if personal information about them is to be collected by others and for what purpose, unless the collection is done by the legal authority. This implies that persons can oppose to some types of processing of personal data, such as personal marketing [38]. At last, this principle implies that persons can demand that information concerning them should be deleted or corrected if the information is incorrect, incomplete or illegal to register [38].

3.1.6 Security safeguards

The confidentiality and integrity of personal data should be protected by reasonable security safeguards [38]. Confidentiality here means protection of personal data from unauthorized access or disclosure, and protection of integrity means protection against unauthorized destruction, use and modification of personal data [38]. This principle encourages actions like use of firewalls, IDS (*intrusion detection systems*) etc. This principle complies with the security safeguard principle of OECD [38].

3.1.7 Sensitivity of data

Certain types of personal information are more sensitive for the data subject than other personal information. This is mostly information concerning the data subject's health, sexuality, race or ethnical background, political, religious or philosophical opinions, or memberships in certain type of organizations (e.g. Trade agreements, unions, joint business

strategies etc). Processing of such information should be placed under stricter regulations than what apply to ordinary personal information [38].

3.2 OECD Guidelines on protection of privacy & Trans-border flow of personal data [2010]

These guidelines are to guide the members of OECD on their national work with the protection of privacy. There are several other organizations that have extended the principles of security and privacy policy from the Organization for Economic Cooperation and Development's (*OECD*) [33]. A proper set of guidelines was drafted on the protection of privacy along with the trans-border flow of personal data [34]. The OECD is a pure international economic organization providing a setting where the governments compare their policy experiences, and seeks to answer the problem of identification along with a proper check system of monitoring the international regulations [35]. OECD currently has 31 member countries including Canada, United States, Australia, Brazil, Norway and other European Countries. During the early 1980's, privacy laws to protect personal data were starting to emerge throughout Europe as development of automatic data processing enabled easy data transmission across national border [36]. As these laws differed from country to country, they could potentially hamper the free flow of personal identification data across frontier and OECD recognized that there was a need of developing guidelines which could harmonize national privacy legislation without restricting trans-border flows [35]. OECD therefore drafted a set of regulations, commonly known as the Fair Information Practice Principles (*FIPP*). Totally there are 8 (*eight*) principles set by the OECD Board (*see in appendix A*);

The main goals of these principles have been summarized as followings by the (*NCJA*) National Criminal Justice Association [32];

- Limiting the purpose of collecting and use of personal information;
- Ensuring data accuracy;
- Establishing security safeguards;
- Being open about the practices and policies regarding personal data;
- Allowing individuals access to their personal data and the ability to have it corrected;
- Identifying person accountable for adhering to these principles;

These guidelines were not forced and not binding for the member countries [37] and the OECD can only recommend that the member countries took these into account in their existing policies and legislation [35].

3.3 The Norwegian personal data act (POL) [2000]

This law was passed on the 14th of April 2000 and came into force on the 1st of January 2001 [41]. This law contains a general view of the processing of personal information and it is based on the EU directives. The Norwegian Personal data Act is also referred as POL Act of Norway. The purpose of this law is to “*protect the individuals against invasion of privacy by the processing of personal information*” [38, 41]. It regulates all electronic processing of personal information, with no concern about how the information is stored or what kind of operations are performed on the information. This means that the law regulates the processing from the day the information is collected to the day the information is deleted [41]. The law applies to all organizations which are established in Norway, even if the processing itself is not carried out in Norway. The law does also apply to organizations established outside Norway that process personal information with the help of some remedy placed in Norway [41]. The law does also apply to organizations established outside Norway that process personal information with the help of some remedy placed in Norway [41]. According to POL, the data controller must have a legal basis for handling the information before the processing can start. This means that the data controller must either hold consent from the data subject, or the processing must be founded on some law, or the processing must be ‘necessary’ to fulfill some purposes that are stated by the law. The consent from the data subject should be voluntary, explicit and informed. In other words, the data subject should not be forced or fooled to give up information concerning him or her [41]. The data subject can only be forced to give up information if there is a legal basis for doing so, such as the police can force a person to state his or her name and the whereabouts in the investigation of a criminal act.

According to clause 30 of POL, if the consent from the data subject doesn’t exist, or the process is not founded on some law, the information can still be processed if it is necessary to fulfill some purposes stated by the law, such as ‘*to fulfill an agreement with the data subject*’

[41]. According to POL, anyone can demand information about how personal information is handled by the data controller. In such cases, the data controller must reveal what kind of information is processed, where the information is collected, who is in charge of the daily processing and if the information is forwarded to a third party. This is a right everyone has, whether or not the organization in question processes information about that person [38]. According to POL clause 18, anyone can demand information about how personal information is handled by the data controller. In such cases, the data controller must reveal what kind of information is processed, where the information is collected, who is in charge of the daily processing and if the information is forwarded to a third party [41]. The POL clause 28 also contains a prohibition against unnecessary storage of personal information. This is to avoid that organizations store personal information longer than necessary.

An organization is normally allowed to store the personal information for as long as the organization has a customer relationship to the data subject [41]. According to POL clause 26, there must be established a reservation register to restrict direct marketing against individuals. All organizations, which make use of direct personal marketing, are bound to use this register before sending out direct advertisement the first time and POL Clause 27 thereafter compare their lists against the reservation register at least four times per year, in order to avoid sending advertisement to individuals who are guarded against it [41]. All organizations and individuals that are going to process personal information have an obligation to notify the Norwegian Data Inspectorate at least 30 days before the processing starts [41]. If the organization is handling sensitive information, then it must apply for a license and receive the data inspectorate's consent before the processing can start [41].

3.4 Privacy practicing of personal data

According to the POL 2000 personal data cannot be used for other purposes than the purpose stated when the data was collected without the approval of the data subject or the processing is done due to legislation, which means that any organization that operates its business activity or simply does the online activity for enforcing the privacy policy must somehow manage to associate system activities on personal data to purposes, or in similar ways be able to interpret

the purpose of the processing [41]. In some cases the data subject has agreed to that the data processor can use the personal data for other purposes than what the data was collected for. Any application for enforcing privacy policies must therefore be able to handle policies that may vary from data subject to data subject. And therefore the identification of the data subject is an important feature in such application [41]. The POL 2000 requires that the confidentiality and integrity of personal data are protected. An application for enforcement of privacy policies is a type of an access control system and will therefore, at least partially, contribute to the protection of the confidentiality and integrity of the personal data [41]. POL 2000 limits the period an organization can store personal information about their customers, but the Norwegian data inspectorate (*Datatilsynet i Norge*) may instruct the organization to take further actions to preserve the privacy of their customers.

3.5 EU data protection directive (EUDPD) [1995]

The EU directive on the protection of individuals with regard to the processing of personal data and on the free movement of such important data was agreed upon on the 24th of October, 1995 by the European Parliament in Brussels and the EU's Council of Ministers [42]. The directive instructs the members of EU to pass legislation which corresponds to the rules in the directive. According to article 4 of the EUDPD directive, the member countries are not allowed to pass legislation that suggests a poorer protection of privacy than what the EU directive proposes. The purpose of the directive is to harmonize the legislation of the member countries which in turn will encourage trans-border flow of personal data between member countries.

The author in [38] explains clearly that that the reason for this wish is, among other factors, the desire for the internal EU market to function as good as possible. The directive introduces a minimum standard of protection of privacy which the member countries cannot deviate from. But the directive allows the countries to do small changes. Although the member countries cannot pass laws that suggest a poorer protection of privacy, the directive does not suggest any limit for how strict this legislation might be in each country. The member countries can pass laws that suggest a better protection of privacy [38]. The directive is covering both governmental and private sectors, but the directive does not cover processing which concerns the security of a state or country, including the countries' economical interests when

processing is associated with questions regarding the safety of the country [42]. This means that a country can pass legislation which provides no protection of privacy as long as the processing of the personal information is concerning the safety of the country. The directive also demands that every member country establishes a regulatory agency which governs the use of personal data and makes sure the legislation is followed by (*article 28th of EUDPD*) and every member country is to introduce an arrangement of obligation to submit reports for every organization which wishes to handle personal data [42].

3.6. EU Convention for protection identification with regards of automatic data processing [1981]

This convention was approved on the 28th of January 1981 by the European council w.e.f 01st October of 1985. Norway ratified the convention on 20th of February 1984 [38]. By ratifying we mean that a state or country commits to incorporate the principles of the convention. The convention establishes some minimum norms for automatic processing of personal data. Beyond that the convention does not describe any rights that individuals can employ, or demand for establishing a data inspectorate. The convention has two purposes, first to improve the protection of privacy, and second to encourage international business [38]. The reason for the last purpose is that countries like Norway had laws that restricted trans-border flows of personal data. The principal rule of this convention is that any country that has ratified the convention “*shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorization trans-border flows of personal data going to the territory of another party*” [41]. A restriction like this is allowed if the information is directly protected by the country of origin and the host country cannot offer the equivalent protection. The convention is political binding for the members of the European Council and therefore the convention makes up an important basis for preparations of national laws [38].

3.7 United States privacy act of [1974]

The legislation bodies in Unites States of America have taken action to assure the public that the private information provided to the various websites hosted in the United States will be

lawfully collected, stored, processed and communicated. Although, it should be kept in mind that the privacy /security policies is treated slightly different in the U.S compared to the EU and other Countries, but the guiding principles behind the existing legislation in US are the same as of EU and OCED member Countries. The guiding on privacy principles behind the data privacy legislation in the EU and US are glanced [44]. Based upon these set of regulations a series of Acts in the US have become the guiding legislations in the area of private data protection. As we have already mentioned, although the guiding principles are the same, there is a difference in the way privacy is treated in Europe and the United States. In United States data and thus private data, are treated as an asset and as such, they are subject to a variety of property protection legislations. In order to ensure legal compliance for organizations hosted on both sides of the Atlantic, the EU and the US have proceeded in the enactment of the U.S - E.U Safe Harbor statute [45]. As a result of this statute, companies and organizations collecting users' private information are asked to create and host privacy policies on their web pages in order to comply with the safe harbor statute [45] (*refer also section 3.8.4*). Following are the basic principles over which the foundation of US privacy act of [1974] is based;

- I. ***Minimalism.*** This refers to the amount of information and the time it needs to be collected, processed and stored. According to this principle, only the absolutely necessary information should be collected and processed while the time it needs to be stored should be reduced to the absolute minimum necessary to complete the specific activity [44].
- II. ***A Minimal Disclosure:*** This restricts as much as possible the disclosure of personal information details to 3rd party or vender [44].
- III. ***Information Accuracy & Quality.*** This entails that the information collected for any particular reason should be as complete, accurate and relevant as possible [44].
- IV. ***Purpose & Specification of Data.*** The Collection and processing of private information should always take place for obvious, specific and lawful purposes clearly stated [44].

- V. **Lawful- Processing.** Any collection and processing of private information should be undertaken with respect to the subject's privacy, autonomy and integrity [44].
- VI. **Sensitivity.** The collection, processing and communication of private data, should be subjected to protection measures, which are in direct relation to the level of sensitivity these data pose for the data subject [44].
- VII. **Information Subject- Control.** Any processing of a subject's private details should be constantly under his control [44].
- VIII. **The Consent.** Before any personal data can be collected, the subject has to provide his explicit approval [44].
- IX. **Information- Security.** Private data should be collected and processed in ways which can be reasonably considered secure according to up to date standards [44].

3.8 Other legislations and sector specific laws for Privacy

There are some additional specific privacy laws and regulations which will not be described in more detail, because those are especially dedicated to some particular organizations/institutions.

3.8.1 The health data filing system act

The purpose of this act is to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy [40].

3.8.2 The U.S Federal Trade Commission and self regulation

The principle of self regulation has been strongly fronted by the FTC, United States and the White House which has stated belief in that self regulation is enough and no new laws are

needed more on this matter [47]. The FTC is an independent agency of U.S government with a mission of promoting the consumer's rights and protection within United States [48]. The FTC pursues vigorous effective law and policy enforcement and research tools through hearings, seminars and conferences and shares its experiences with federal and state level legislature in United States and other government institutions [48]. Federal Trade Commission of U.S has its own guidelines on fair information travel and retrieval which consists of five main principles that are adopted from the OECD principles [31]. They are as follows;

- ***Awareness / Notification*** (a statement of how the personal identifications can be collect and its usage).
- ***Choice / Consent*** (a choice regarding the usage of the personal data from users).
- ***Access and Participation*** (levels of participation by users to their personal information so that it can be review, update or amend).
- ***Security and Integrity*** (An integrity to protect against unauthorized access, destruction or disclosure of the personal data).
- ***Enforcement*** (to ensure compliance).

While the Federal Trade Commission supports industry self regulation, they also recommend legislation in certain areas such as children's privacy as a result of concerns regarding privacy on the internet [49]. They also initiated a series of reports to determine how well and efficiently industry self regulations work, and according to their own metrics it appeared that the self regulation model was successful [31]. Other studies however, had been more critical to the self regulatory approach, and particularly a study by [47] which found evidence that pointed to a sustained failure of business to provide reasonable privacy protection under the self regulatory model. It was further claimed that self regulation has helped malicious and spyware develop and flourish and that emerging technologies represent serious threats and problem to privacy and are not addressed by self regulation [47]. The study concludes with the statement that FTC could be better capable of protect privacy and security than what the US industry can with self regulation. But still FTC has remained with the self regulatory approach and instead of usual legislation they have expressed great hope in enhancing technologies [31].

3.8.3 The U.S children's online privacy protection act (COPPA) of [1999]

The children's online privacy protection act of 1999 is another protection act. This law applies to website owners and service provider for commercial and advertisement purpose that are directed to children under the age of 13 or have actually acknowledge that US children under age 13 are providing information online [49].

The COPPA is an American law, but the FTC has made it clear that it also applies to foreign operated websites if such websites are directed to US children in the United States or knowingly collect information from children [50].

3.8.4 The EU and U.S safe harbor privacy framework of [2000]

For the efficient and transparent export of information with U.S the EU directives has allowed American companies to exchange information with European business [32]. For that matter the United States Department of Commerce developed International safe harbor privacy principles [32]. The safe harbor is indeed an important way for U.S organizations and companies to avoid experiencing interruptions in their business operations and dealings inside EU or facing any prosecution by European authorities under the European privacy laws and a certification to safe harbor assures that EU agencies and organizations know that the certified and authorized American operators provides a proper privacy protections for the common users and subscribes as defined by EU legislation [51].

3.9 Comparison of privacy acts with common instruments

In *Table 3.9*, we have identified some common instruments on privacy and compared them with some privacy acts of major stakeholder countries. With the help of these instruments of privacy policy we can compared legislation on privacy policy phenomena that are currently enforced by different States / Countries. By reviewing the above mentioned privacy protection laws, we suggested these ten instruments vital in differentiate and designing an effective legislation on privacy policy .These instruments would help us to signify what factors are

lacking in these different laws or acts. For this we have selected the well known privacy protection laws.

S.no	Common Instruments of privacy policy	United States privacy Act [1974]	Canada personal information Act [2009]	Norwegian personal data Act [2000]	OECD privacy principles [2000]	EU personal data directive [1995]	New Zealand data privacy Act [1993]	Australia data privacy law [2008]
1	Automation for processing personal information	X		X	X	X	X	X
2	Concomitant of sharing personal information	X	X	X	X	X		
3	Covering Public and Private sectors	X	X	X	X	X		X
4	An extensive set of procedures on data privacy regimes	X	X		X	X	X	X
5	Restriction on trans-border flow of personal information	X	X	X	X	X	X	X
6	Channeling privacy complaints to another Law agencies/bodies	X	X	X		X	X	X
7	A stringent procedures over sensitivity of data	X	X	X	X	X	X	X
8	Extensive use of "Opt-in" for validating by data subject		X	X		X	X	X
9	Ensuring the data accuracy through proper mechanism	X	X	X	X	X	X	X
10	Notifying the reasons of collecting personal information	X	X	X	X	X	X	

Table.3.9 : Analysis of different Privacy Laws of different countries.

The first instrument of privacy policy is *automation for processing personal information* and this instrument is adopted by all the different countries' privacy legislation, except the Canada personal information protection & electronic documents act of 2009. The second instrument of privacy policy is *concomitant of sharing personal information*, and this instrument is adopted by all famous privacy policy laws and act, except New Zealand's data privacy act of 1993 that

means that this law does not give much priority to this important instrument. Next instrument of privacy policy is *covering Public and Private Sectors*. There is a lack of this instrument in the New Zealand data privacy act of 1993. But generally this instrument is being adopted by all the other countries. This shows that the New Zealand data privacy act of 1993 does not govern on the private sector business or industries, when a privacy issue is being discussed.

An extensive set of procedures on data privacy regimes is one of important instrument in design the effective privacy policy, but this is not covered by the Norwegian personal data act of 2000. This instrument checks how well procedure is followed on data privacy regimes. There is a lack of this instrument in the Norwegian privacy protection.

Another instrument is *restriction on trans-border flow of personal information*. This instrument is considered as a strong base for designing the standard and an effective privacy policy. As we can see in the analysis table this instrument is found in all the privacy protection laws and acts of different countries. This instrument allows a particular restriction on trans-border movement of personal information, this instrument safeguards the identity of one country user when there is a request of sharing the details of the user. *Channeling privacy complains to another Law agencies/bodies* is another useful instrument considered in policy legislation. In the policy guidelines for protection of personal data for OECD, we can see that this instrument is not present. OCED is the organization of many Countries that they follow their own legislation and constitutions; whatever the issue may arise about the data protection each country will be responsible to deal with their own local law enforcement bodies. A country cannot interfere another country's enforcement bodies on handling the privacy and data protection problem. An interesting analysis we have noticed in the above table that all the privacy laws are agreed on the instrument of *stringent procedures over sensitivity of data* and on the other hand over the *extensive use of "Opt-in" for validating by data subject*, United States of America privacy act of 1974 and OECD privacy principles of 2000 are unable to give much priority of this instrument. It should be noted that the extensive use of opt-in the process of validating data varies between countries, because every country have different mechanisms for validating the personal information. We have also noted that over the instrument of *ensuring the data accuracy through proper mechanism*, all the privacy acts have a strong consensus. All the data protection acts in major countries are agreed on the data accuracy through a proper channel. In the end, we analyzed that on *notifying the reasons of collecting*

personal information, the Australian data privacy act of 2008 is unable to notify that why they are collecting the sensitive data from user or a subscriber, but the rest of all privacy laws are agreeing on this main instrument.

Chapter 4

Research Approach

This chapter starts by defining the research questions, then it describes which appropriate research approach & methodology is adopted to get reliable results and achieving the primary objectives of the study. In order to get a solid background on what the users think about the privacy policy a survey has been conducted. The survey and its implications are described in this chapter.

4.1 Research Questions

The privacy policies of past decades do not seem to be adequate to deal with new challenges. Previously we have tried to make a strong foundation to build a consensus about the issue of privacy policy, for this reason, we have done a mandatory specialization project course TDT4520 autumn 2010, and in that project we have conducted a small scale survey based on a paper based questionnaire to investigate this issue [90]. In that paper based survey we have asked about 10 persons about the response of accepting a privacy policy before registering on a new site. We have gathered impressive, but a small level response from the students, researchers, faculty members of NTNU and makes valid idea to go for large scale online survey in order to collect an original mind set of users [90]. We have split the research questions in two groups;

From the common user`s / subscriber`s perspective;

RQ#1. How important is the phenomenon of privacy policy for a common user to accept it?

RQ#2. Are the contents fully read and understood by the users before accepting the policy?

RQ#3. From users perspective do the policies that are accepted have a difficult language and format?

From the organization / service provider`s perspective;

RQ#4. What is the current level of enforced privacy policy in different organization?

RQ#5. How well is a privacy policy integrated in different service provider / organizations?

RQ#6. When a policy is presented, what role it can play in framing trust of a common user?

4.2 Methodology

The basic methodology used in this work is;

Exploratory Research:

An exploratory research is selected as a methodology for obtaining qualitative primary data. It will be used as its name reflects (i.e. exploring a problem for which a hypothesis will or might be created and tested). It provides data for an initial step of research that would be helpful in testing concepts & ideas before they can be implemented or put into the marketplace [22]. An exploratory research methodology allows researchers to discover the general nature of a problem by being flexible and allowing changes or enhancements to the survey methodology as the study progresses. An exploratory research provides two main approaches;

1. It can be informal as is the case of discussion with main stakeholders.
2. It can be applied from a more formal approach such as in-depth interviews, case studies, pilot studies, survey, questionnaires etc.

For the purpose of this thesis work, it is decided to adopt an exploratory research methodology, from a formal approach, through the survey as a qualitative designed technique. Surveys are found as the most suitable way of obtaining data from specific stakeholders. This methodology will answer '*who, what, when, where*' issues of the problem and it is relatively inexpensive in nature.

4.3 Survey research

As we have mentioned in previous section that in order to get a solid background on what common users think about the privacy policies, a small scale survey was conducted in autumn 2010 as a specialization project at NTNU [90]. The survey was based on paper format questionnaire has served as a ground to conduct a more comprehensive research in this area [90]. In general, surveys have for a long time been viewed as important tools for obtaining information about people's thoughts on a particular subject or topic. A survey indeed, tends to be inexpensive and easily carried out, although they are subject to bias, sometimes depends upon the questions and the way they are presented them to the audience. For conducting an effective survey a researcher wants a good response from the participants and it also helps to save other resources (e.g. finance, manpower, transportation etc).

4.3.1 What actually is a survey research?

Survey research is one of the best approaches for collecting information to gain insight into people or problems under study. A survey is a data-gathering and analysis approach in which respondents answer questions or respond to statements that were developed in advance. Using surveys is one way to conduct research. But before a researcher decides to invest the time and resources in the survey approach, it should be considered whether a survey is the best way to find out what that researchers want to know [27]. A survey, when conducted properly, allows generalizing more about the beliefs and opinions of many people by studying a subset of them. However, a survey can only be used for generalization when the survey process follows some strict procedures. Survey-based research can be used to characterize the knowledge, attitudes, and behavior of a large group of people through the study of a subset of them [27]. For this solid reason, surveys are used extensively by software systems and systems engineering organizations to provide insight into complex issues, assist with problem-solving, and support effective decision making. The concept is more clearly explained in figure 4.3.1 where, there is a triangular relationship describing a general survey structure [27].

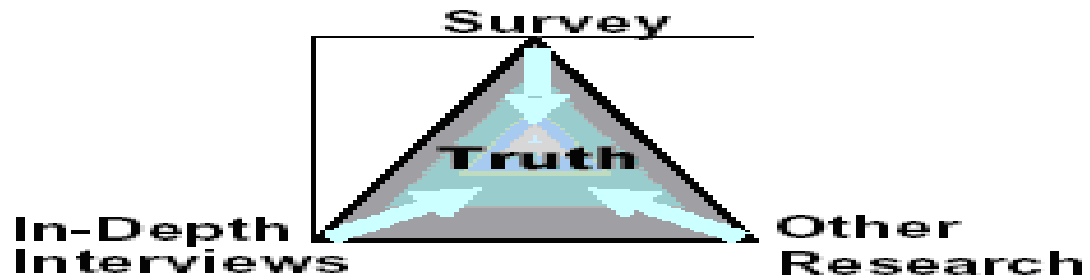


Figure 4.3.1: The figure shown above is describing a general survey structure. It shows a relation between interview data gathered and the efforts put-up by the researcher to conduct a survey to extract the truth from it. This is a triangular relation between the a research, interviews and survey, when all these factor are combined together is a systematic way, then a desired results can be obtained [27].

4.3.2 Elaboration

There is no data available telling what a common user thinks about the privacy issues and security policies that relates to these issues. In order to find out what a user thinks about these issues and what exactly they want and how important this phenomena of accepting the privacy policies. It was decided for this research to perform the survey as a qualitative examination instead of a quantitative one to get open answers from users. This is more explained in figure 4.3.2

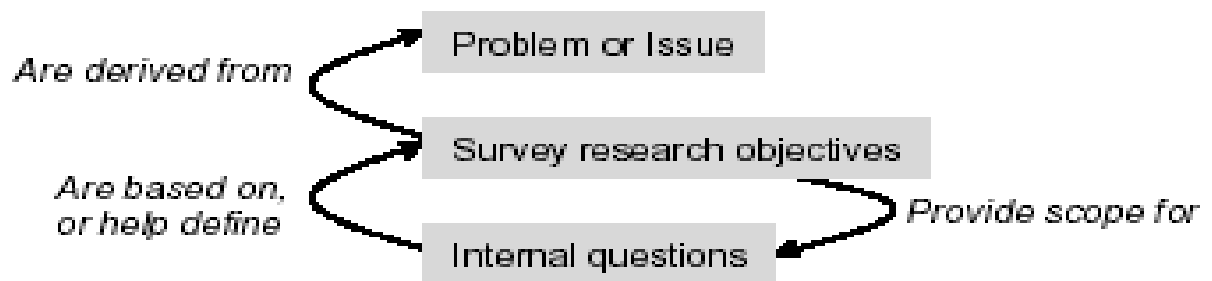


Figure 4.3.2: This diagram is describing a solid relation from deriving the core issue towards achieving the objectives and providing a broad scope of designing the questions to reach the goal of a research [27].

4.3.3 Generality in survey & Target audience

It is possible to conduct a qualitative study in a number of ways. One of these is in the form of questionnaires. Selecting a target audience is always based on the perspective of a research and interest to obtain the results. That is, for the research objectives we have to identify, who can best provide the information we need? Therefore, the target audience we select depends on the problem we are trying to understand and who can provide that information to us. The target audience in this project is;

1. Professionals / Administrative / Technical staff.
2. Intermediate / Students level.
3. Academia / Researcher / Scientific level.
4. Business/ Commercial/ Trade level.
5. Media / Communications / Marketing level.
6. Medicine / Healthcare level.
7. Common subscriber / Users.

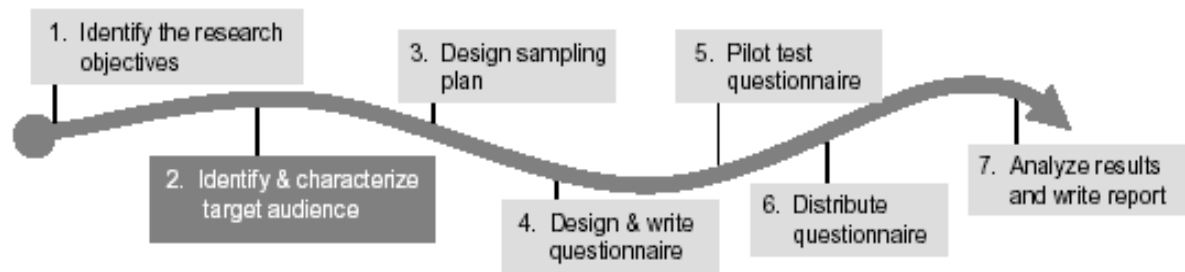


Figure4.3.3: The figure mentioned above is determining the structure of how to conduct a general survey to collect the desired results. In this specialization research the pilot test questionnaire technique has not conducted because it a useful and indeed a time consuming technique to setup the group of audience. Pilot testing gives an opportunity to make revisions to instruments and data collection procedures to ensure that appropriate data collection would work [27].

It is important to be very explicit about who the intended respondents for our survey are. This assumption has a dramatic influence on the design of the survey instrument and the distribution method for the survey. Once we have identified the target audience for the survey, conduct an

audience analysis to characterize the intended respondents. An audience analysis is conducted for a number of reasons. Understanding the audience will help us in developing questionnaire items that can be interpreted by the respondents.

4.3.4 Measurement and data gathering approach

The information derived from the audience analysis is indispensable when specially we are designing and writing the questionnaire instrument, because it will help us to understand the precautions we must take to formulate the questions in a way that the respondent understands. Then comes the task of pulling the information together to make observations, conduct analyses, make interpretations, and draw conclusions. The first task is to compile the questionnaire data and transform it into meaningful representations that can be interpreted and analyzed. As a result of the analysis, observations are made, leading the researchers to form interpretations and draw conclusions [27]. The second task is to package the analysis as an information product that can be interpreted and used by others. If a researcher is using hard copy forms of the questionnaire, it will be necessary to organize the response information into a spreadsheet or a database. Many spreadsheet programs provide powerful native tools for statistical analysis and graphical depiction. Also, most spreadsheets can export the spreadsheet information to computer applications that perform on statistical analysis [27]. The easiest way to do this is to organize a spreadsheet area with each row corresponding to a single respondent and the columns representing the specific answer choice variables. Once the data has been organized appropriately, statistical analysis can be conducted. Statistical analysis for survey data examines response patterns—frequencies of different responses, what response occurred most frequently for each question within a group, variation in responses within a group, and differences in ways different subgroups (within the same survey) responded. Quantitative research is about collecting, analyzing, and interpreting numbers. However, the human mind is rather limited when it comes to understanding patterns within lists of raw numbers. In order to make sense of large volumes of data, the raw numbers need to be transformed into something intelligible, such as a graph or a picture [27]. With today's technology, almost any type of data graph can be displayed with standard applications available on every desktop. However, it is still up to the human-in-the-loop to ensure good design.

4.3.5 Accuracy and Relevancy in survey research

As a survey author and using a survey research approach it should be kept in mind that a survey should be well structured, with direct questions and answers using a suitable and easy language that survey participants will understand. There are no hard and fast set of rules on the wording of survey questions, there are few principles that are used to make the efficient survey design [82]. The relevancy & accuracy are two major poles that are the foundations and main outcome of designing reliable and attractive surveys. These two important principles play a vital role in writing effective survey questions. It is a goal of every researcher of his/her field of study to turn the basic research objectives into a proper set of information requirements for getting the desired results [80]. In order to achieve an effective relevancy we should look closer on three main factors that are described in figure 4.3.5 [80].

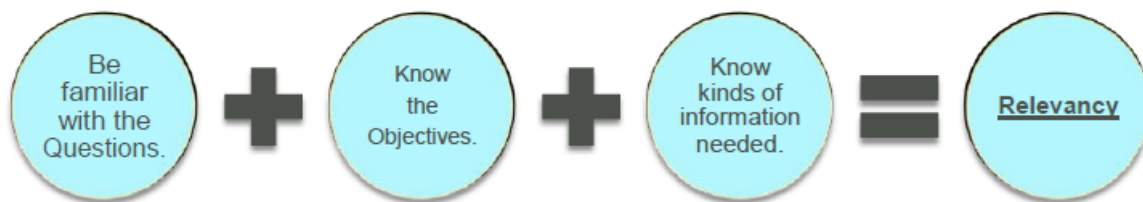


Figure 4.3.5: This simple mathematical expression describes how an effective relevancy can be obtained in a survey research. If we combine three main terms together then a relevancy can be visible in a project. We have to be familiar with the core question that we are willing to get answer and knowing the theme of our project and focus on particular details we required to answer our research questions [80].

Accuracy counts much in the survey research; an accurate survey is one where the basic question collects the suitable data in a reliable manner. If the questions ask from respondents; for things they do not actually know, then it would be a high risk of conducting the survey and results would be invalid. In order to enhance the accuracy of participant's answer, the following items should be taken into consideration [80].

- i. Use appropriate style, type, and questionnaire sequence [80].
- ii. Make the survey interesting, focused and notice the survey timing that how long it

would take to answer the entire web survey [80].

- iii. When constructing a good survey, then author should try to put himself in a position of typical user, or rather the least educated respondent [81].

It is always a good strategy to write clear and direct, and brief questionnaire because they will help the survey participants to know exactly what a researcher asks for [81]. It must be kept in mind that the questions asked in the survey should not have ambiguous meanings, because it also helps in preventing participant confusion [81]. Asking a hard questions in the alternative way may also helps to alleviate participants' concerns and finally we have to take into account the capability of survey participants; because many respondent may not be able to correctly answer certain questions and if you are surveying employees of company or organization, it is a possibility that they cannot recall certain details of a project work carried out years ago [81].

4.4 Survey response

“The survey research community solely believes that representative sampling is essential to permit generalization from a sample to a population. Survey researchers have also believed that, for a sample to be representative, the survey response rate must be high” [87]. Response rates for most surveys have been falling during the last 4 decades or may be more, so surveys often stop short of goal of a accurate response rate [23]. People who select NO responses have characteristics suggesting that they are least likely to have formed real opinions. For example, such responses are offered more often by people with relatively limited cognitive skills [24]. People who are more knowledgeable about a particular topic are presumably better equipped to form relevant opinions and are less likely to offer NO responses. The more interested a person is in a topic, the more likely he or she is to form opinions on it, and the less likely he or she is to offer NO responses. More evidence raises questions about the reliability of NO responses. The frequency of NO responses to a set of items is fairly consistent across different question sets in the same questionnaire [25]. Although NO responses sometimes occur because people have no information about an object, they occur more often for a variety of other reasons.

People sometimes offer such responses because they feel ambivalent about the issue or because they do not understand the meaning of a question or the answer choices. Some NO responses occur because respondents think that they must know a lot about a topic to legitimately express an opinion, and some occur because people are avoiding honestly answering a question in a way that would be unflattering [26].

4.4.1 Survey response calculations

The percentage of people who respond to a survey is known as a response rate. A maximum response rate helps a lot to ensure that the results are representative of total survey population [85]. In order to calculate the response rate, we can use the following equation [85];

$$\frac{\text{Number of Complete Surveys}}{\text{Number of Participants Contacted}} = \text{Response Rate}$$

Example: We have contacted about total 100 users and just 40 users are respondent then we would get $40/100 = 0.4$ and if we will multiple with 100 percent then the total response rate of the survey would be 40%.

4.4.2 Maximizing the rate of survey response

Every questionnaire is important in a survey based research; because there is no exactly universal right / wrong of questionnaire wording and we can make a survey effective by adopting the following theme of making an efficient survey to get best possible results [80].

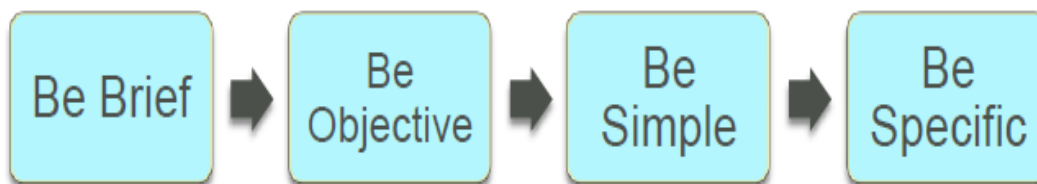


Figure 4.4.2: This figure is high lightening the technique of design and write questionnaires in- order to conduct a research. There are 4 main steps to do that; first be brief with your question; second the question have some motive; third the language of the question should be simple to understand and the last is a question should be specific with the research topic [80].

There are 7(*seven*) useful tips by which we can maximize the rate of survey response;

- a) Happily greet the respondent and explain the purpose of the survey [82].
- b) Include the information about the reason of participation and confidentiality that how the result would be used [82].
- c) Do not restrict your survey with any time limit or with a particular date [82].
- d) Explain how to navigate, submit the survey and include instructions for each section if that is applicable [82].
- e) A survey structure should be user friendly and easy to follow with clear and direct instructions [82].
- f) Send some reminders for those respondents that have not filled the survey questions [82].
- g) It is not compulsory to offer any gift or intensive for the participants, but as a researcher you can promise to share the results with your respondent [82].

4.5 Questionnaires

The instrument of a survey is the questionnaire. While surveys always make use of a questionnaire; it is the survey process itself that determines whether the information obtained through the questionnaire is valid and can be used to generalize about the population that the sample is intended to represent [27]. It is also a fact that developing and distributing a questionnaire in a random fashion is not the same as using a well constructed questionnaire within a carefully designed survey process. Questionnaire design is one of the most controversial issues among survey researchers because how respondents are asked questions has a great effect on the results. One political scientist conducting a public opinion poll has remarked that different question formats yield different results, even though they are asking about the exact same content [29]. Therefore, various ways of asking have been proposed and evaluated to date, from the perspective of appropriateness for representing each respondent's perception.

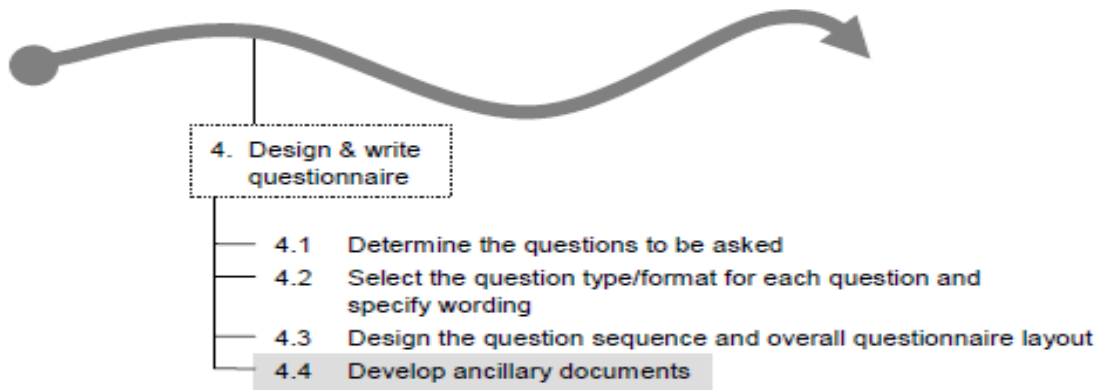


Figure 4.5: The figure is elaborating the technique of design and write questionnaires in- order to conduct a research. There are 4 main steps to do that; first a researcher have to determine the important question that could answer the objective of the research & second is to select the format of those questions; third step is to make a feasible layout & sequences of questions. The last step is to make a complete questionnaire into a document or well arranged form [27].

4.6 Types of Questionnaire

The types of questions used in a online survey will play a positive role in producing a relevant survey responses. As the survey designer, it is necessary that what types of questions are appropriate to asked from the respondents [86] . The question types range from open-ended questions to closed-ended. Indeed the questionnaire type that determines what type of data is collected. It is also better to get some help / consult with a good statistician or mathematician; if a survey designer is uncertain about the measurement scale of the results or it would help to ensure that data and research questions wwould match with the statistical analysis [86].

1. Open-ended questions are those types of questions that allow participants to answer in their own words and with their own idea about the issue. In an online survey research, textfields are provided in order to type in their answer. An open end question seeks a fair response and aims to determine what is inside the participant’s mind. These techniques are best to use when asking for feelings and attitude, likes and dislikes, opinions or some additional comments on issue [83].

2. **Closed-ended questions** are specially those types of questions that have a pre arranged answers with a small or a large set of potential choices. A dichotomous question is also one of the types of close end question, which allows respondents to choose one or more choices (*E.g. in Yes or in No*) and another type is mutlichotomous question, which gives a fair chance to respondents to choose one of multiple answer choices [83].

4.7 Advantages and Disadvantages of web based survey

A web based survey ultimately gives the freedom to be creative when designing survey through the use of titles, logos, photos etc. The glance of a web based survey is their dynamic nature and as soon as a participants click on submission button, his / her response comes suddenly into the result sections [82]. As a web survey author it is not necessary to deal with the long mail process and not necessary to waste paper to send out to participants [82].

There are many advantages of using website based surveys as compared to a traditional mail or face to face conversations. An online survey has the same grip as paper based versions in that they allow participants to take as much time to complete the survey; and iff (*if and only if*) that is administered anonymously then the online surveys may be a reliable at addressing most confidential questions and issues, because at that time frame an interviewer is not present probing the questions directly [83]. E-mail technique is very less expensive, efficient and it brings a revolution end as compared to slower and ordinary mail process. It is also a reliable and quick transmission of the survey itself to the participants, and results returns quicker to you (*i.e. researcher*). Additionally web survey sometimes known as environmental friendly due to the online filling the questionnaire and non-use of paper [84]. Interesting and interactive computer graphics are important features in a paper based survey, but an online research methodology can truly present well laid out and visually pleasant survey structure. Website surveys can utilize colors, images etc. Website based surveys are indeed dynamic in nature, which clearly means they can easily provide a good statistical results on an urgent basis [84]. Many people think that e-mailed surveys raise ethical concerns and can be unreliable. Sending the unsolicited emails may try to invade a person's privacy [84]. It must be also an important consideration is that the World Wide Web is not always a perfect world. There are potential

technical glitches that may arise at any step in ending or beginning of the survey. Many times a survey respondent have reported that their Internet provider may be experiencing issues or maybe the respondent's machine may not be properly functioning [84].

4.8 Limitations in a survey

While surveys can provide significant advantages over other data collecting approaches, there are certain limitations that should be kept in mind:

- ✓ To generalize for a population, a survey must follow strict procedures in defining which participants are studied and how they are selected.
- ✓ Implementing the survey with the rigor that is necessary can be expensive with respect to cost and time.
- ✓ Survey data is usually superficial [28]. It is typically not always possible to go into details.
- ✓ Surveys can be obtrusive. People are fully aware that they are the subject of a study. They often respond differently than they might if they were unaware of the researcher's interest in them [27].

4.9 Adopting the privacy practices in online surveys

There is no doubt that it is good to disclose your privacy practices to your survey respondents. Adopting this strategy helps to increase response rates by putting potential respondents more at ease and as the author of the survey you should disclose your privacy statement on the introduction page of your survey [82]. If you are conducting a survey for an organization which already has its own privacy policy, then you also have to indicate the privacy and security policy of your organization. It is best that you should describe a statement before your survey starts [82]. There are few steps that would help to declare a privacy statement for your survey;

- What personal information you are collecting in survey should be clearly specified [82].
- How would you plan to use the information for the survey [82].
- How respondent can access their responses [82].
- How respondent can contact with you [82].
- Streamline the amount of personal information you are collecting in the research [82].
- It is highly recommended to use an encrypted survey link to distribute survey [82].

By explaining the pros and cons of the online web based survey we have concluded that online surveys are more feasible in term of collecting a good response from the user in less duration of time frame. An online survey provides a comprehensive idea about the topic and helps a researcher to collect the original response from the subscribers.

Chapter 5

Evaluations, Results and Discussions

Before this work can be considered a success, a number of analysis and evaluations have to be performed. This chapter is briefly discussing the important observations related to the research topic theme. We have divided this chapter in two sections. The first section will discuss the evaluation and results of the user survey, and in other section will answer the service provider point of view on privacy policy.

Section # 5.1: User survey

5.1.1 Evaluating results of user survey

Several recent surveys conclude that people are very concerned about the privacy and consider it to be an important factor in their decision making on computer [2]. As seen in the figure 5.1.1 we circulated a questionnaire to the peoples that are working and living in Norway. It took approximately 4 months to collect the response. This response was collected by sending 3 times reminder on different working days via email and messages to fill out the survey. Approximately, 81% incorporate their opinions about the privacy and security issues that have risen in this survey. About 19 percent rejected or did not try to record their response. We have sent the questionnaire to our Norwegian friends and fellows and requested them to pass on the questionnaire as many people as they can. For this level, it was indeed a good initiative to collect the above mentioned number of respondents to calculate the ideas and understanding about the issue.

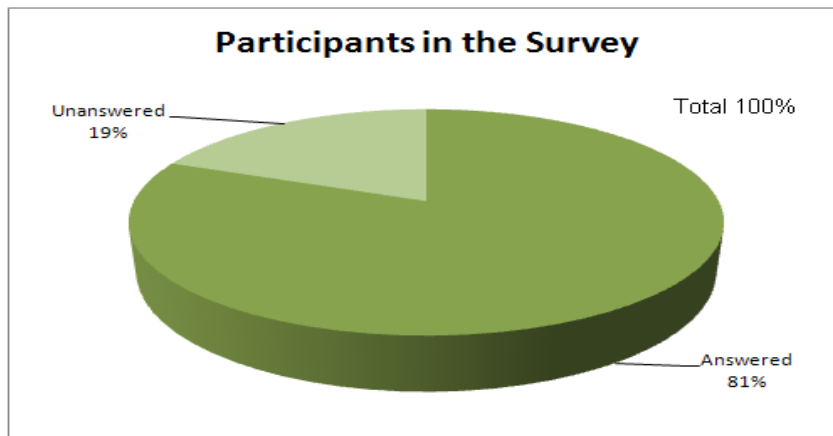


Figure: 5.1.1 Number of user participants in the survey

5.1.2 Participants in terms of gender

The following figure 5.1.2 shows that the majority of the respondents were male participated (59 percent) and 22 percent of the respondent were female.

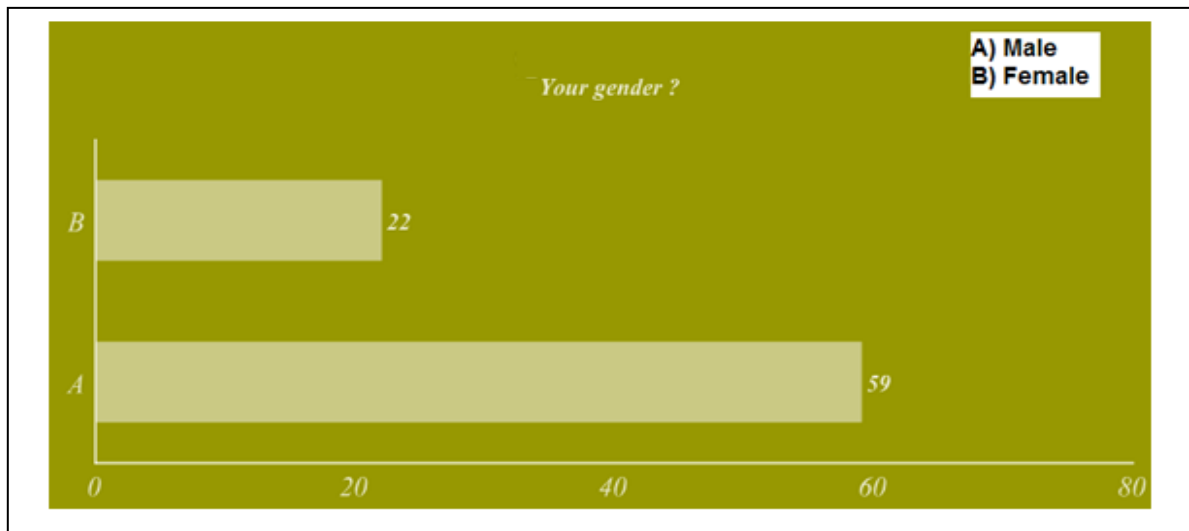


Figure: 5.1.2 Response level of gender in survey

5.1.3 Participants in terms of age category

In the survey we have categorized age factor in categories. By analyzing the figure 5.1.3 in our user survey we have identified respondents from five different age categories.

- *Category A: From age 20 Years To 30 Years.*
- *Category B: From age 30 Years To 40 Years.*

- *Category C: From age 40 Years To 50 Years.*
- *Category D: From age 50 Years To 60 Years.*
- *Category E: From age 60 Years To 70 Years and above. (Just one respondent belongs to 70 year above)*

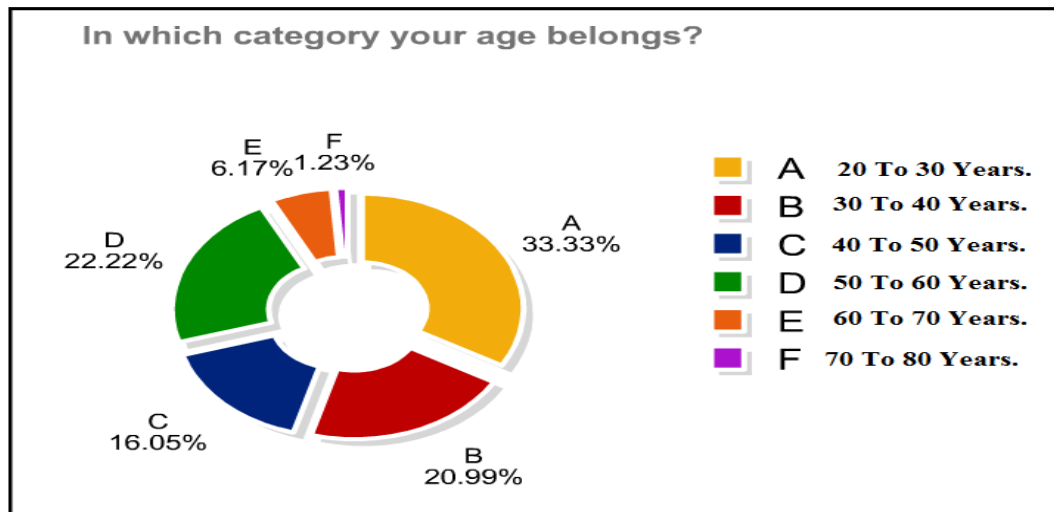


Figure: 5.1.3 Number of Participants in survey according to age category

The majority of the respondent belongs to Category A having a response of 33%. Moving forward to Category B holding 20% of the response and the next Category C having only 16% of respondent. In Category D we can observe that only 22 % of the participants answered the questionnaire. The second last Category E has 6% of the participants and just one respondent belongs to the category F 70 years and above.

5.1.4 Participants in terms of education level

In the following figure 5.1.4 we observed that most of our survey participants were highly educated. We have set up the five basic education levels in the user based survey.

- High School.
- Completed the Bachelors Degree.
- Completed the Master`s Degree.
- Completed the Doctorate Degree.
- Completed the Post Doc.

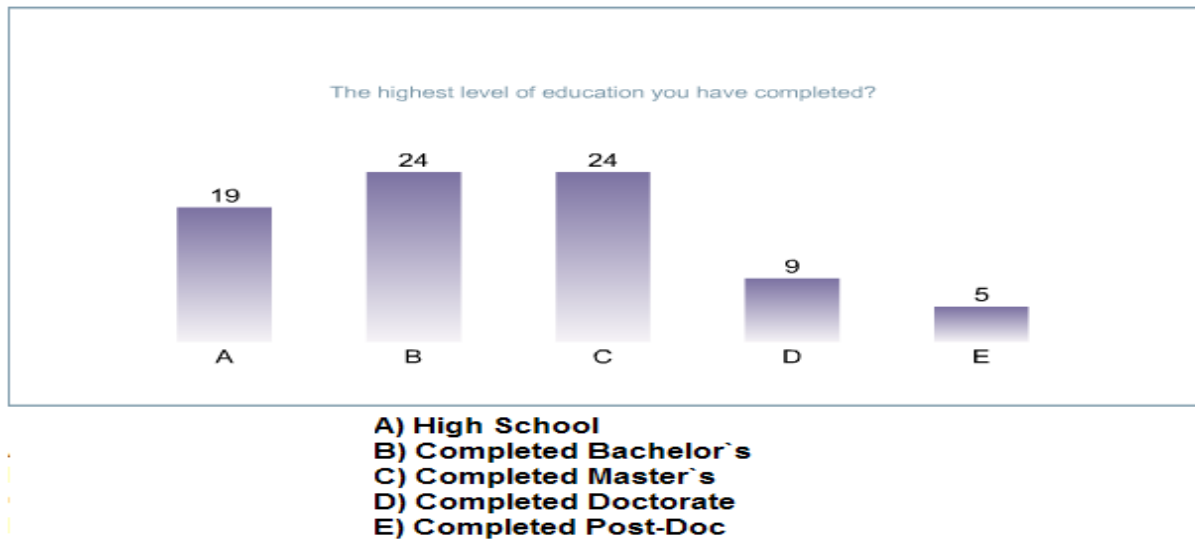


Figure: 5.1.4 Responses to Level of Education in survey

About 19 percent of the participants were at high school level. We have 24% of the respondent completed bachelor's degree and 24% of respondent completed master's degree. Furthermore we can observe that participants with a doctorate degree were 9% and 5% finished post doc.

5.1.5 Participants in terms of occupation

In figure 5.1.5 we show the occupation types of respondents in our survey. On top we have found about 30% of the participants were Home / Common user. It was our motive in this survey to target primarily the home user. The next higher categories of participants were from Academia / University / Research level containing 13% of the total participants.

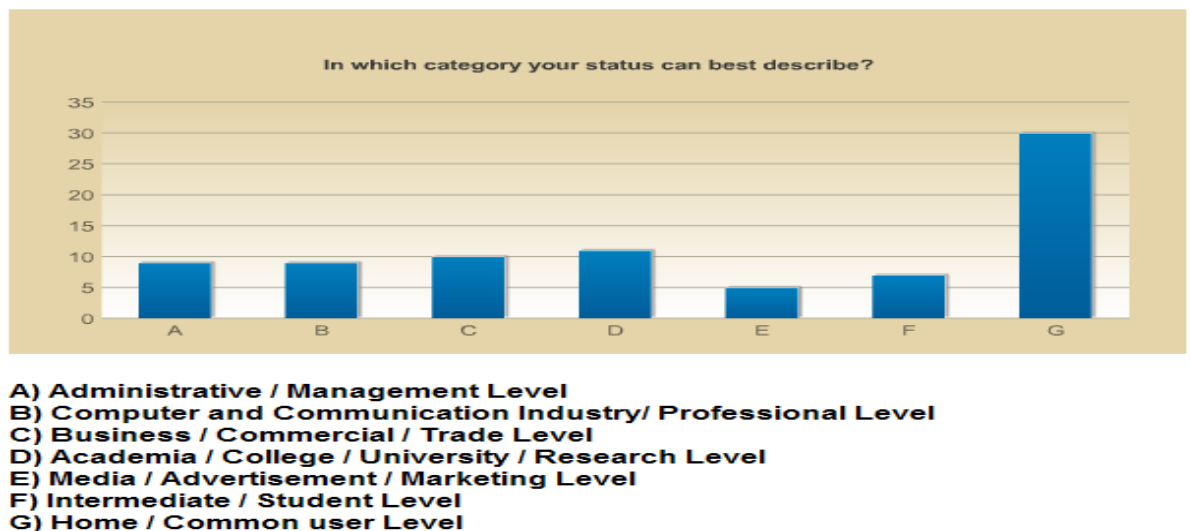


Figure: 5.1.5 Response level of participants on occupation

Moving onwards is the category of Business and Commercial/ Trade having 12% of the respondent. We have 9% each in the category of Administrative / Management level and Computer /Professional level. Only just 7% of the participants were Intermediate /Students and lastly about 5% of the respondents belong to the Media/Advertisement / Marketing level.

5.1.6 Level of Internet usage of participants

Figure 5.1.6 shows the level of using the internet from the participants. This highlights the quantity of using the internet among the participants and their familiarity with different concepts of internet. There is a high level of usability of internet in the option D (which is 30 to 40 hours) using internet per week and about 24% of the respondents belong to this option.

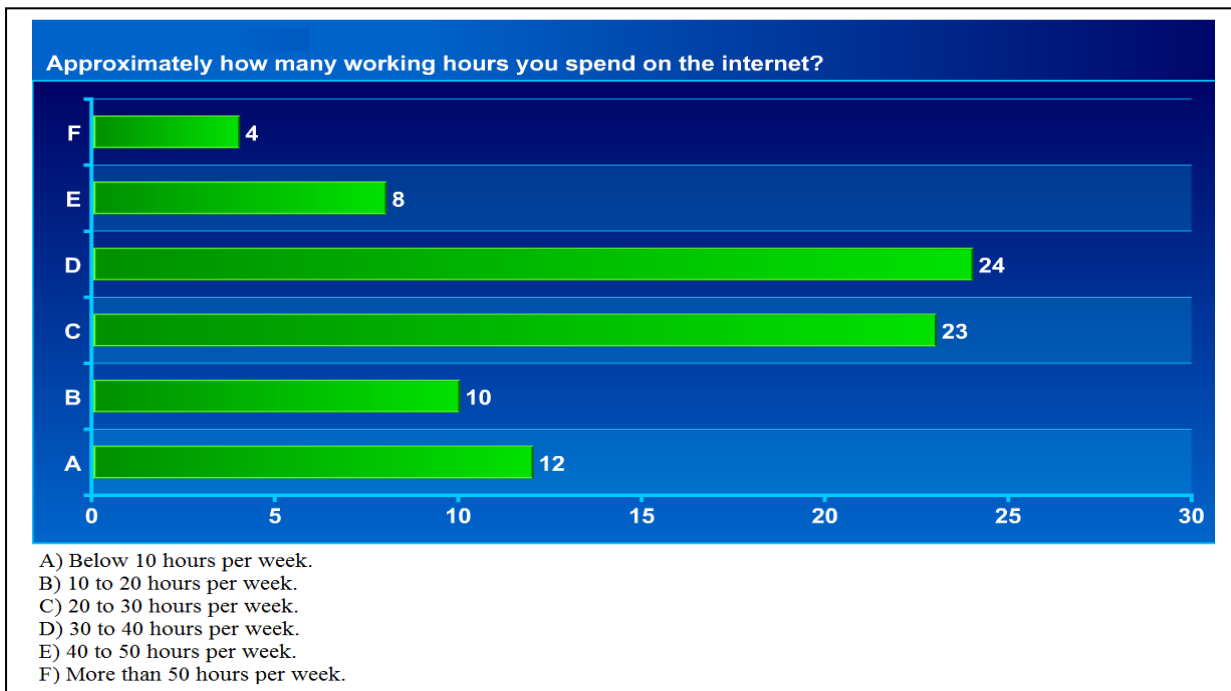


Figure: 5.1.6 Response level of participants on internet usage

Next higher visibility we can see is in option C which shows that 23% of the respondents use (20 to 30 hours) per week on the internet. Just 12% respondents use (below 10 hours) per week and 10% participants were in the option B (10 to 20 hours) per week. Eight percent of the participants are using (40 to 50 hours) per week. Finally only 4% of the respondents are spending more than 50 hours per week.

5.1.7 Participants familiarity with the term “*privacy policy*”

We have asked a question of familiarity with privacy policy from our respondents in the survey and we have got some confusing answers as shown in figure 5.1.7. The majority of the respondents, which is 36%, are familiar with privacy policy but they do not actually know what exactly it means and what concept is behind in privacy policy. 23% of the respondents knows exactly what it is and how it works whenever they subscribe them self to a service provider. Lastly, 22% of the respondents have never heard this term before and may be they have no idea about the privacy policy.

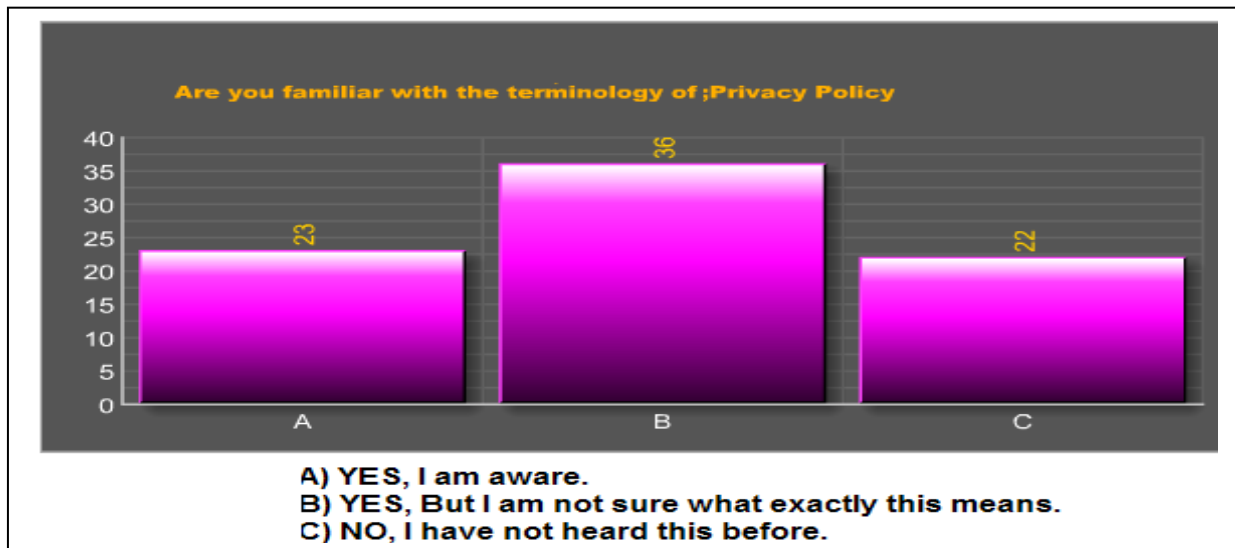


Figure: 5.1.7 Response of participants over privacy policy

5.1.8 Participants perception of “*privacy policy*”

Analyzing figure 5.1.8 23% of the respondents feel that “*privacy policy is just a law notice that tells about the legal status of the organization*”. Furthermore we have found that 22% of the respondents have stated that “*privacy policy is a legal document that shows how a service provider collects personal information and the proper usage of that information*”. Around 18% of the respondents think that “*privacy policy are just explains the contact information and reliability of service providers*”. Finally, 18% of the respondents think that “*privacy policies only show organization good will*”.

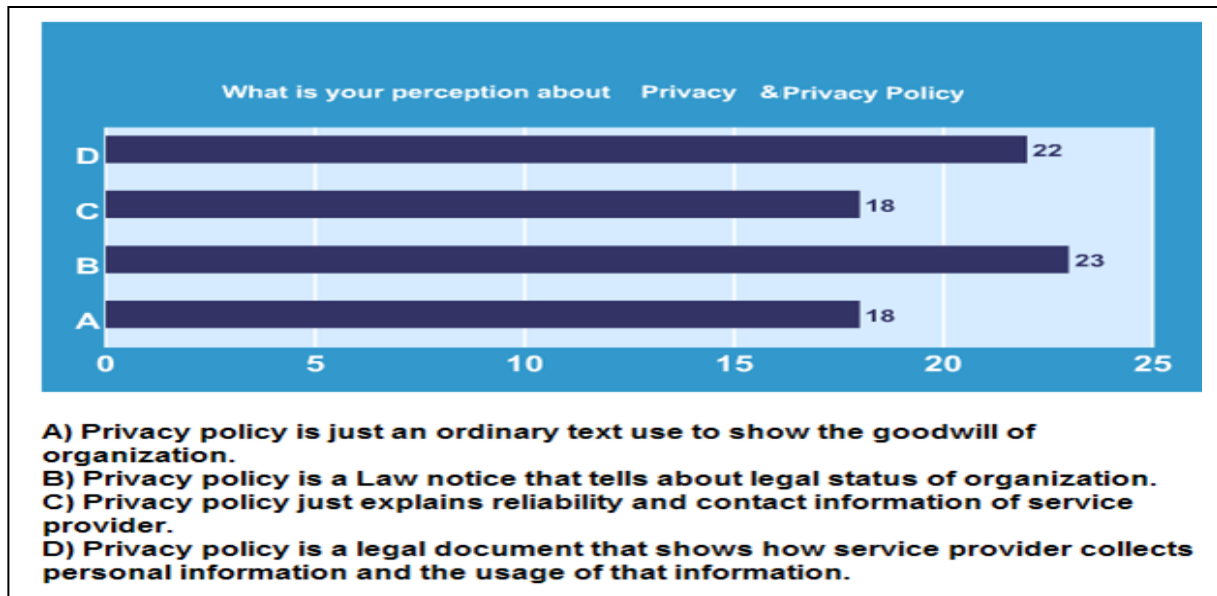


Figure: 5.1.8 Response of terminology of privacy policy

5.1.9 Advantages of having a “privacy policy”

The goal of this question was to discover the respondents view on the advantages of having the privacy policy on the service operator website and to investigate its value. Refer to figure 5.1.9 32% of the respondents feel that “it helps to prevents Trojan attacks, spamming and virus threats”.

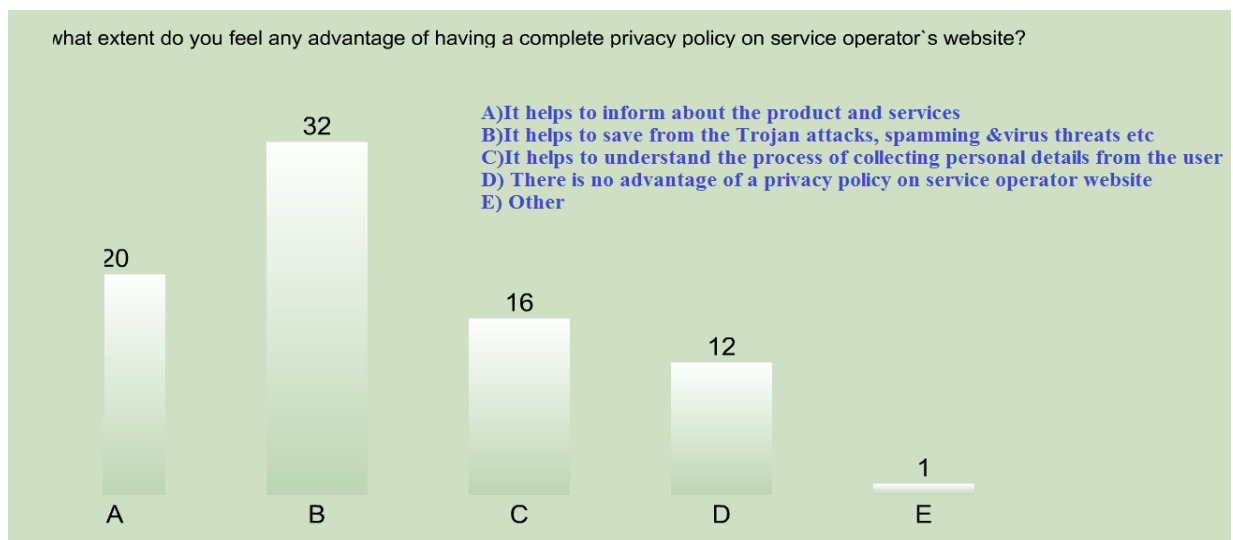


Figure: 5.1.9 Responses to advantages of privacy policy

Almost 20% of the respondents feel that the “privacy policy is used to inform about different products and services from the service providers” and just 16 percent of the respondents think that “a privacy policy is quite meaningful and it helps to understand the process of collecting

personal details from the common user". Only 12 percent of the respondents think that *"there is no any big advantage of having privacy policy on a service provider`s website"*.

5.1.10 Disadvantages of having a "privacy policy"

As can be seen in figure 5.1.10 which shows respondent`s reply to disadvantages of having a privacy policy. Majority of the respondents (26%) have concerns that there is a great chance of phishing or harassing a common user, if there is no privacy policy defined by the service provider.

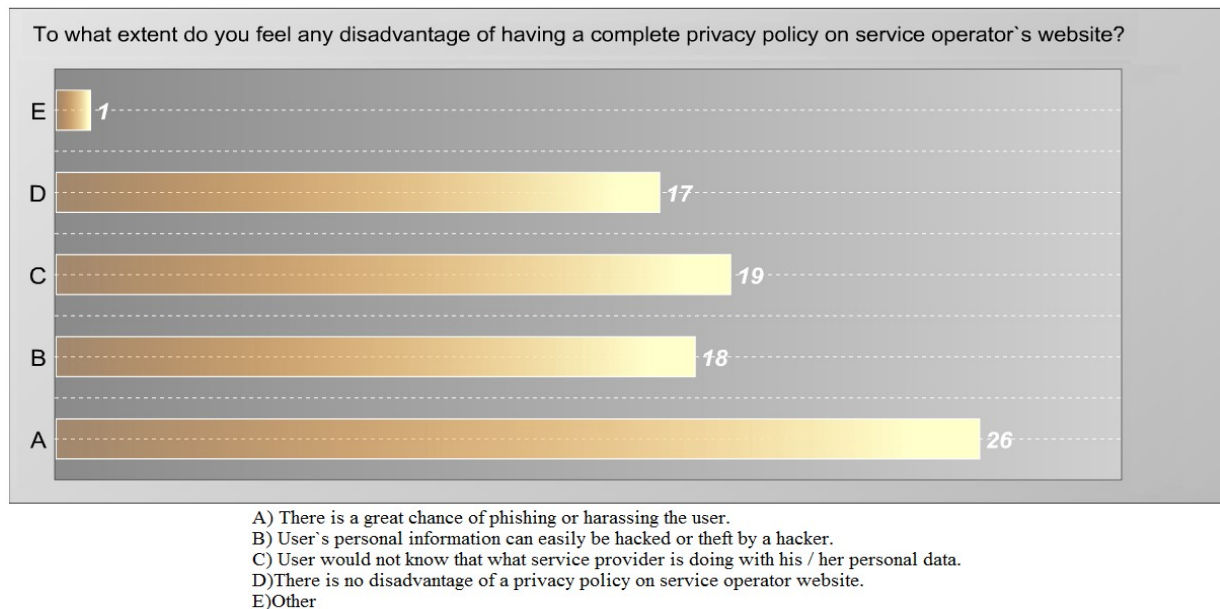


Figure: 5.1.10 Responses to disadvantages of privacy policy

19 percent of the respondents voted that the big disadvantage of not having a privacy policy is that a common user would not know actually what the service provider would with the personal information that a user have given. The next high percent is 18% which shows that there possibility that user`s personal information can be traced or hacked easily, if there is no privacy policy defined by the service provider. Further we have seen that 17% of the users feel *"there is no disadvantage of privacy policy and it does not matter for them if it is not mentioned by the service provider"*. Just only 1% of the participants told that *"may be he/she is unable to access the website if there is no privacy policy mentioned by service provider"*.

5.1.11 Reading policy contents before registering

The result in figure 5.1.11 shows out almost 50% of the users have no interest to read the privacy policy whenever they became a new subscriber of a service provider.

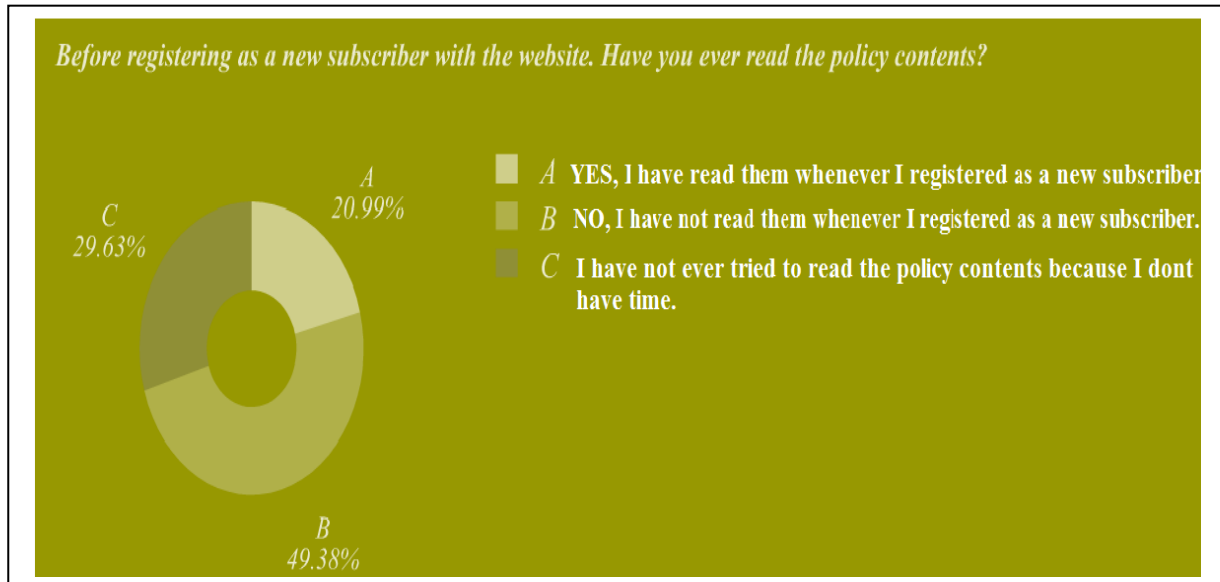


Figure: 5.1.11 Response of reading the policy contents

Around 30% of the respondents has no time at all to read the policy contents before getting registered. Finally just 21% of the respondents have voted that they read the contents of the privacy policy when they are registered as a new subscriber. The basic purpose of this question was to analyze how important a privacy policy for a subscriber, whenever they register and give their personal information to the service provider.

5.1.12 Degree of difficulty in understanding policy contents

In this question we have asked from our survey participants how difficult they feel when they read the policy content. By looking at figure 5.1.12 , majority (36%) of the total respondents are feeling problem in understanding the content of the privacy policy. 29% of the respondents have informed us that they have not ever read & understand the privacy context before using the services. Lastly, just 16% of the respondents do not feel any difficulty in understanding the context of the privacy policy.

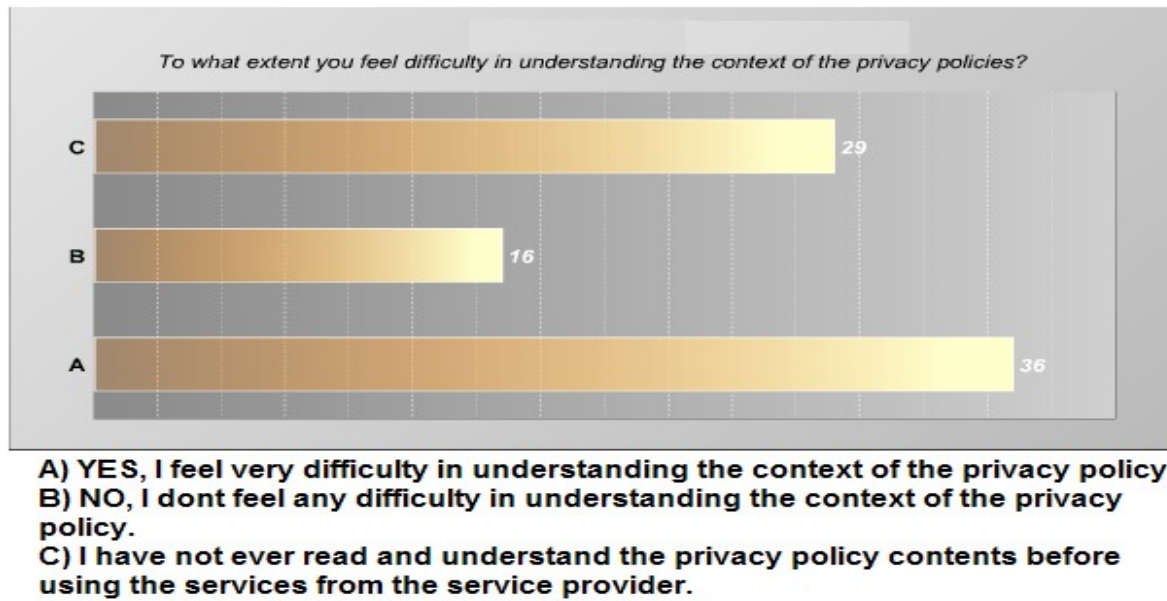


Figure: 5.1.12 Level of difficulty in policy contents

5.1.13 Relevance of privacy contents as a subscriber

As shown in figure 5.1.13 about how relevant are the privacy policy contents from a common user point of view, almost 42% of the respondents agreed that they are not at all relevant from them. Around 30% of the respondents says that “yes, the privacy policy contents are useful whenever they registered and relevant for them”. Finally we can see that round about 28% of the survey respondents has no any idea about the relevancy of these privacy policies from the subscriber point of view.

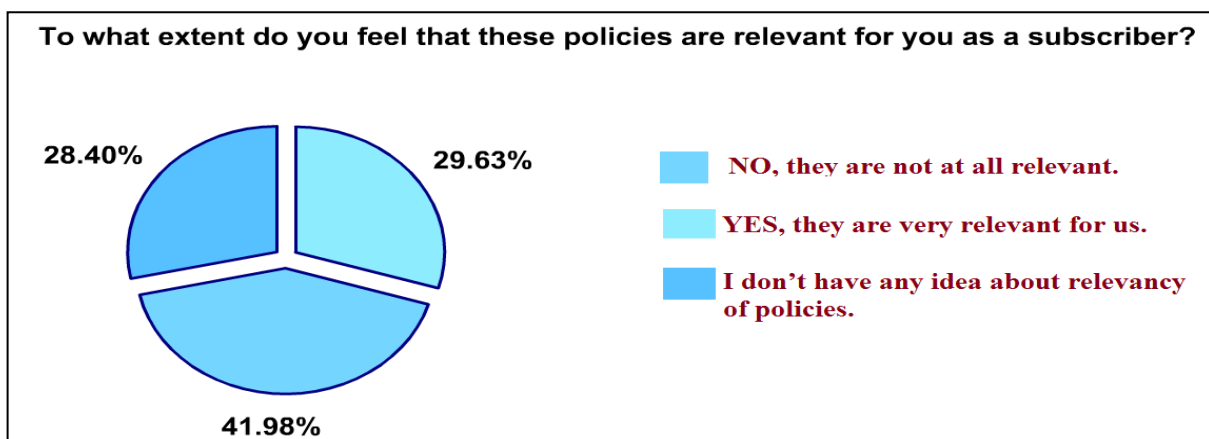


Figure: 5.1.13 Response of relevancy of privacy contents

5.1.14 Level of confidentiality to give personal information

We have asked in our online subscriber survey to what extent a user is confident enough to give his/her personal information (e.g. social security number, date of birth, Telephone / cell number and addresses) to a service provider. We analyzed the results as shown in figure 5.1.14 that 40 percent of the respondents are “not confident to give their personal social security number to the service provider” and 24% of the respondents are “not willing to give their date of birth”. Just 8% of the respondents are “not confident to give their address” and 5% of the respondents are “not giving their telephone number to the service provider”.

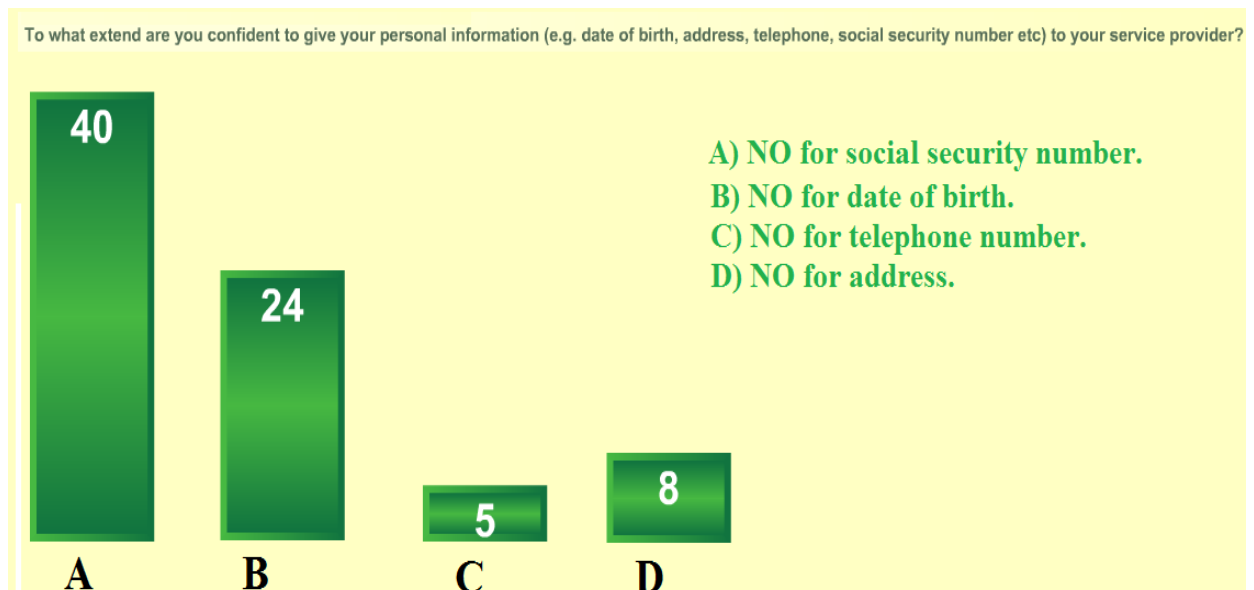


Figure: 5.1.14 Level of confidentiality of personal information

5.1.15 Amendment of privacy policy contents from service provider

We have asked the participants whether they are aware or they are informed, whenever their service operator amends the privacy policy on the website. The results are given in figure 5.1.15;

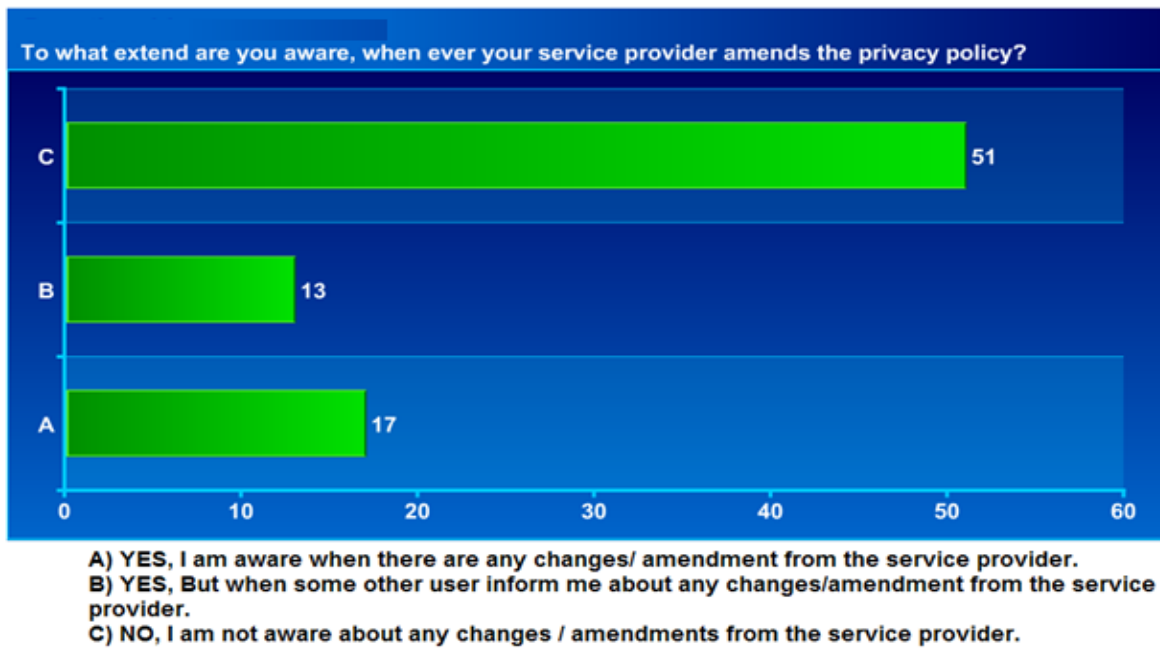


Figure: 5.1.15 Response of amendment of policy contents

The majority of the respondents (51%) are “not aware when there is any change / amendments performed by their service provider”. According to this survey 17% of the respondents are “aware when there are any changes / amendments from the service provider” and just about 13% of the respondents are “informed from other users, when there is any change / amendments done by their service provider”.

5.1.16 Request / Review of personal information from service provider

We have asked how frequent the subscribers send the request to review / update their personal information which they have given to the service provider. In the figure 5.1.16 majority of the respondents (24%) have “not ever sent any request to update / review their personal information from the service provider”.

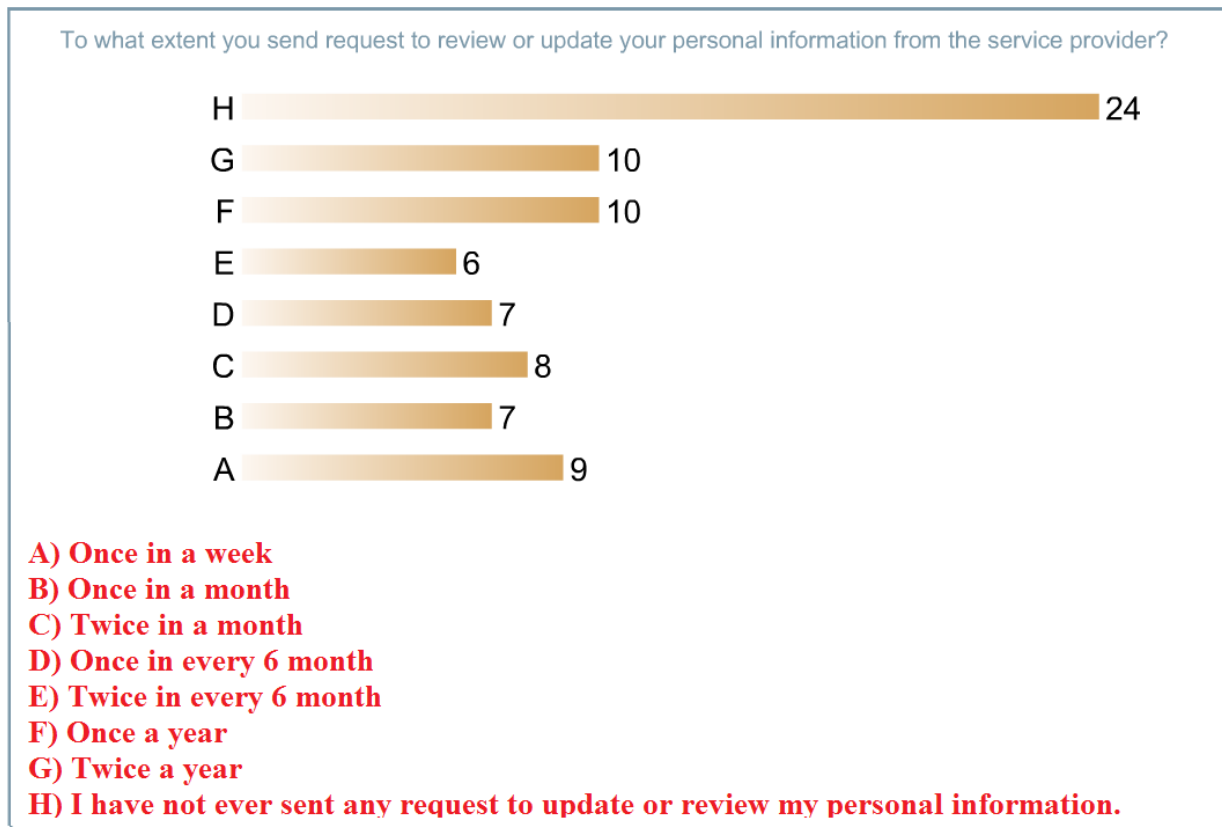


Figure: 5.1.16 Response level of review of personal information

Only 10% of the respondents have voted that they send the request “*twice a year*”. Same 10% of the respondents have voted that they send the request “*once a year*”. Just 9% of the respondents send the update / review request “*once in a week*” and only 8% of the respondents request “*twice a month*”. About 7 % of the respondents send the request for updating the personal information “*once a month*”. Only 7% of the respondents send the request “*once in every 6 month*” time frame. Lastly, 6% of the respondents would like to update their personal information “*twice in every six month*”.

Section # 5.2: Service provider's survey

5.2.1 Evaluating results of service provider's survey

This was the second part of the online survey that we have conducted to investigate the service provider's point of view about the privacy policy and its impact on their subscribers.

At this level of research, it was feasible to target the Norwegian service providers because; the working environment of this work was in Norway and also due to limited time constraints & resources etc. In order to get a large number of responses, we distributed our online survey to 40 large service providers that are operating in Norway. It was suitable to get the response from Norwegian Service provider because; it will show how Norwegian companies perception on the privacy policy. We have selected the companies according to their reputation in the business world and their large number of registered subscribers. Our primary target was to collect responses from the Internet / Telecommunication/ Scientific / Research sector as they often collect the sensitive data from their subscribers.

This online survey was answered by 17 service providers but 23 service providers did not recorded their response , may be due to their chartered rules and regulations that not allow them for disclosing the company's information to public or media etc. It took approximately 4 months time to collect the response from these service providers. This response was collected by sending 3 times reminder on different working days via emails.

5.2.2 Categories of participated organization in survey

The figure 5.2.2 is showing the different categories of the survey organizations. As it was mentioned in the previous section that our primary target was to focus on Internet / Telecommunication / Scientific / Research organization because they have a good knowledge about the privacy policy issues and they can record their response positively to our survey.

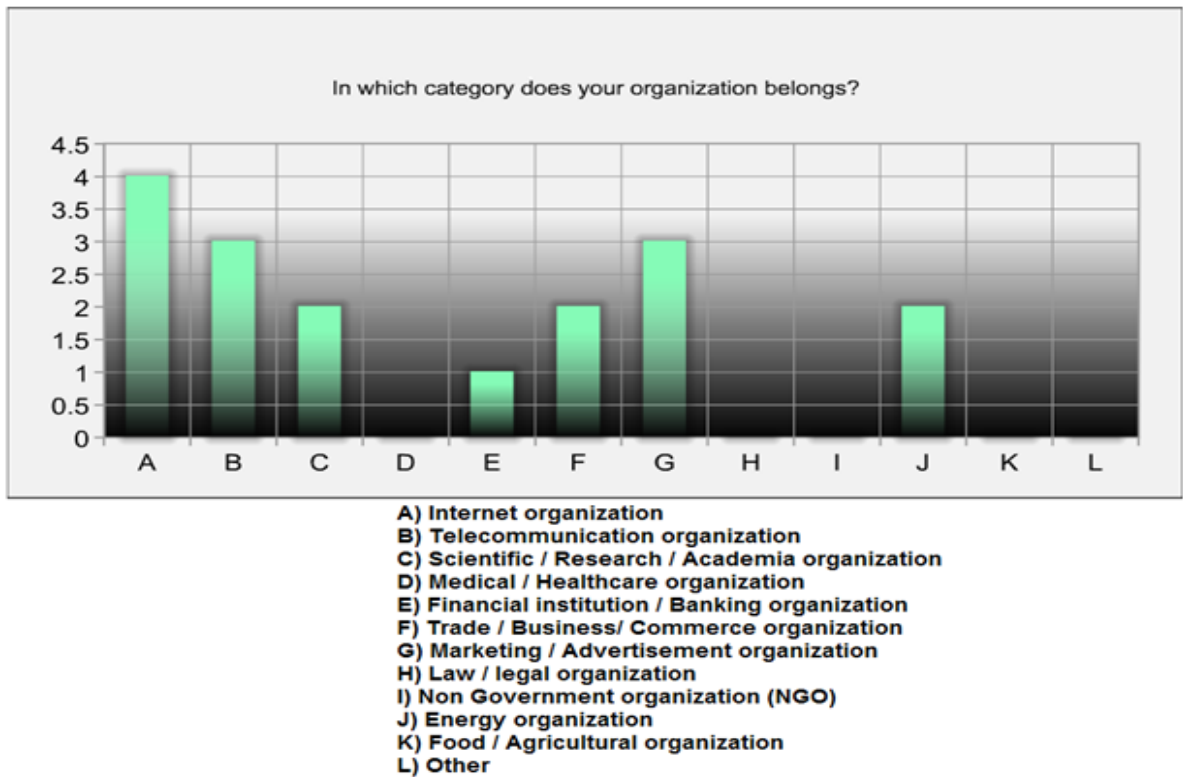


Figure: 5.2.2 Categories of participated organization

In figure 5.2.2 we can see that majority is the internet organizations with 4% of the response, and next higher response is 3% from telecommunication organizations. Only 3% response comes from marketing / advertisement organizations. Just 2% of the response collected from scientific/research and academic organizations and 2% of the response comes from the trade/business organizations. 2% of the response was given by the energy sector and 1% of the response from financial institutions.

5.2.3 Service provider`s location

Analyzing figure 5.2.3 we see that most of the service providers operates inside the territory of Norway and their services are being used by the local Norwegians.

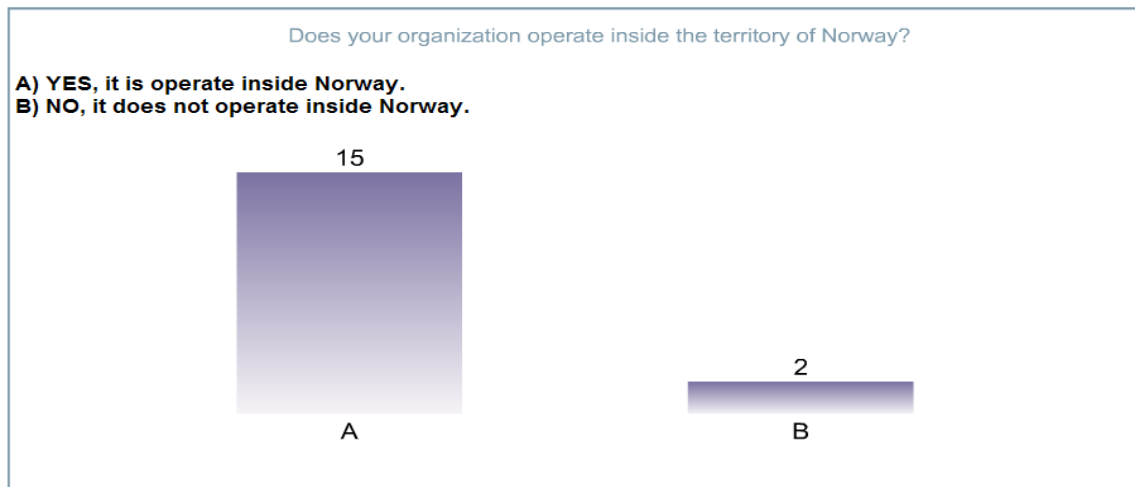


Figure: 5.2.3 Response of service provider's location and operations

About 15 respondents are Norwegian service operators and just 2 respondent service operators are operating their business outside the Norwegian territory.

5.2.4 Number of registered subscribers

We have asked our respondent service providers about their approximate number of registered subscribers that are getting services from them. 6% of the service providers have approximately more than 300, 0000 registered users. Next we have 5% of the service providers having between 15, 0000 and 2 00000 registered users.

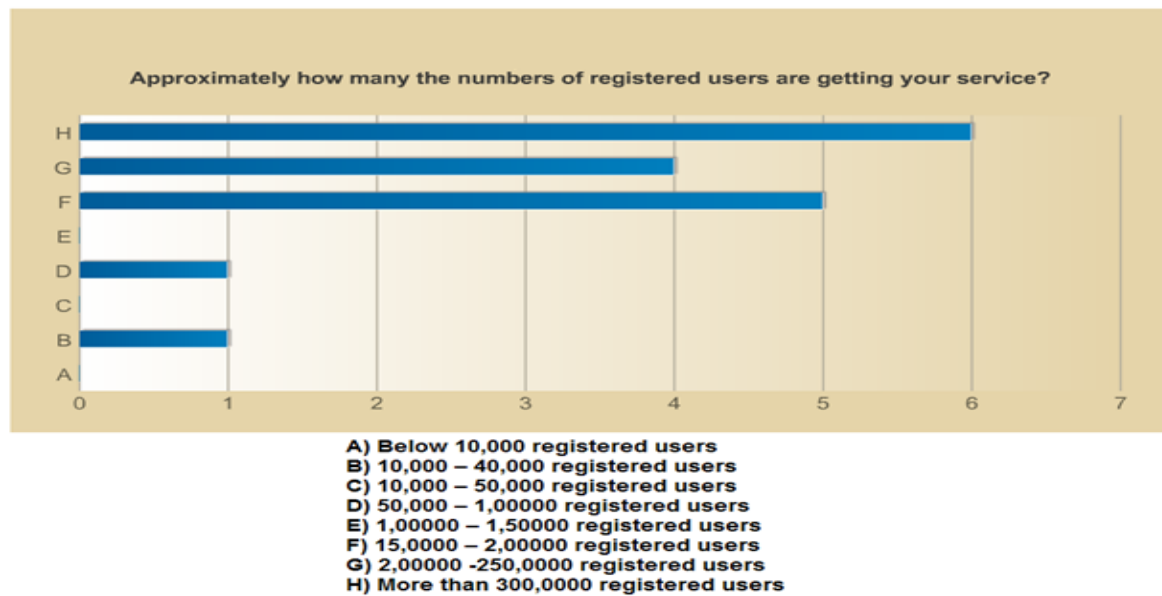


Figure: 5.2.4 Level of registered subscribers of service provider

About 4% of the respondents have between 2, 00000 and 250, 0000 registered users. 1 respondent service provider have the registered users between the range 50,000 and 1 00000. Finally we have 1 service provider with registered users between 10,000 and 40,000.

5.2.5 Service provider`s importance on “*privacy policy*”

With this question we want to figure out that how much importance the service providers give put to setting up the privacy policy for their subscribers. By examining figure 5.2.5 we see that 47% of the responded service providers give a strong and keen importance on the privacy policy because they know how important this is for them to acquire goodwill in terms of securing their customer`s privacy, this percentage is high among all the other responses. Next recorded response is 35% in which the service provider has given an average importance to privacy policy. Lastly 18% of the respondent service providers give a low importance on privacy policy for the subscribers.

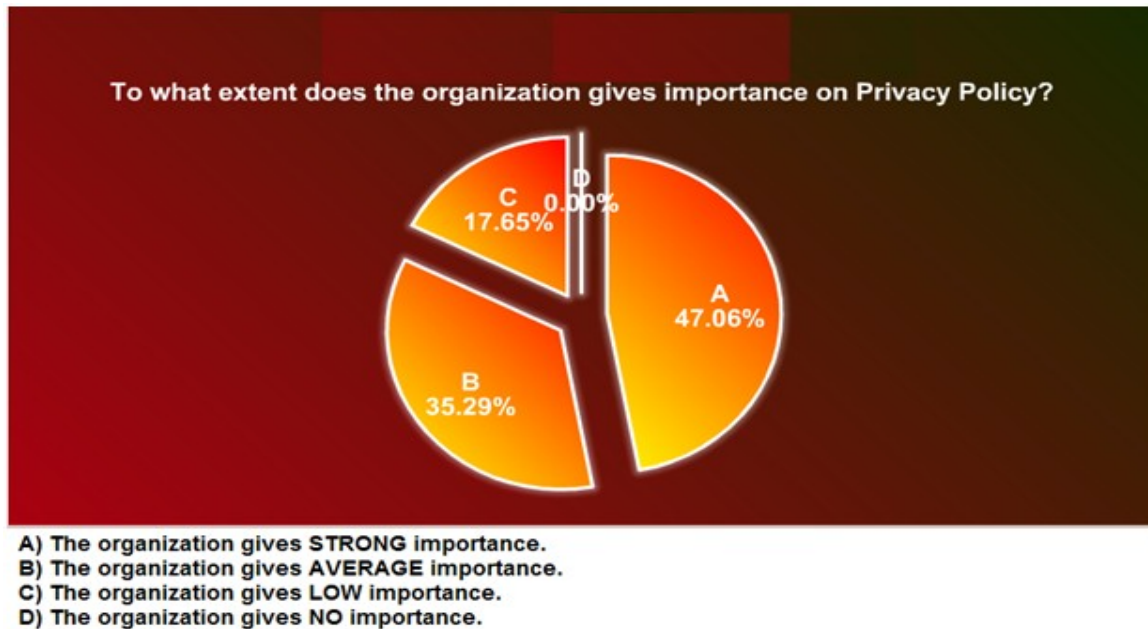


Figure: 5.2.5 Level of importance on privacy policy

5.2.6 Standards of privacy regulations and laws

From this question we have tried to investigate what standards or a regulation of privacy and its defined laws does the service provider use while collecting the personal information from the common users. In the survey we have mentioned many privacy standards and laws to see which of them are used by the Norwegian service providers.

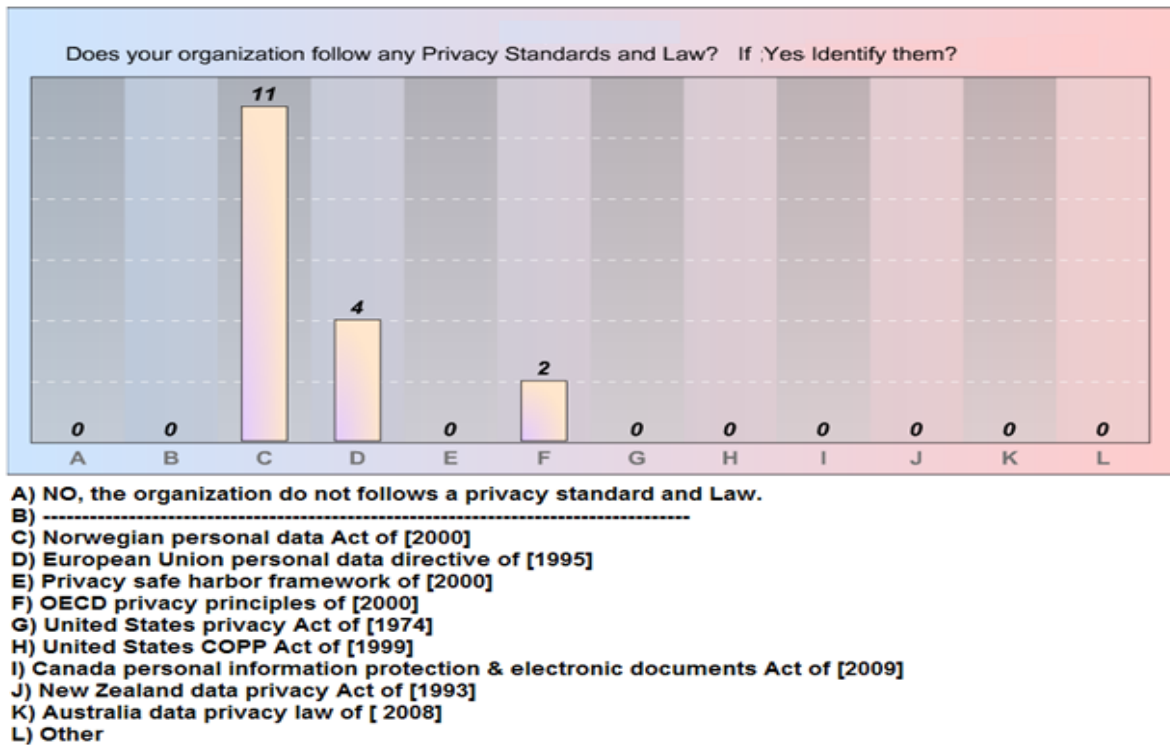


Figure: 5.2.6 Response of following privacy standards & regulations

As shown in figure 5.2.6 that most service providers use Norwegian Personal Data Act of [2000], whenever they collect the personal information from Norwegian users. This is 11% of all the responses we have received. The next higher score is 4% which is of European Union personal data directive law of [1995]. Just 2% of the service providers are following the OECD privacy principles of [2000].

5.2.7 Response of reading privacy policy from subscribers

Figure 5.2.7 shows the response to the question on how large portion of the users read the privacy policy when they are registered. This is a service provider perspective. Just 29% of the respondent organizations think that (*10 to 30 percent*) users read their privacy policy. Another response given by the organization which is 29% thinks that (*30 to 60 percent*) users read the organization's privacy policy. Around 24% of the respondent organizations think that (*60 to 90 percent*) users read the privacy policy. Finally we can see that 18% of the service providers think (*below 10 percent*) of their users read the privacy policy.

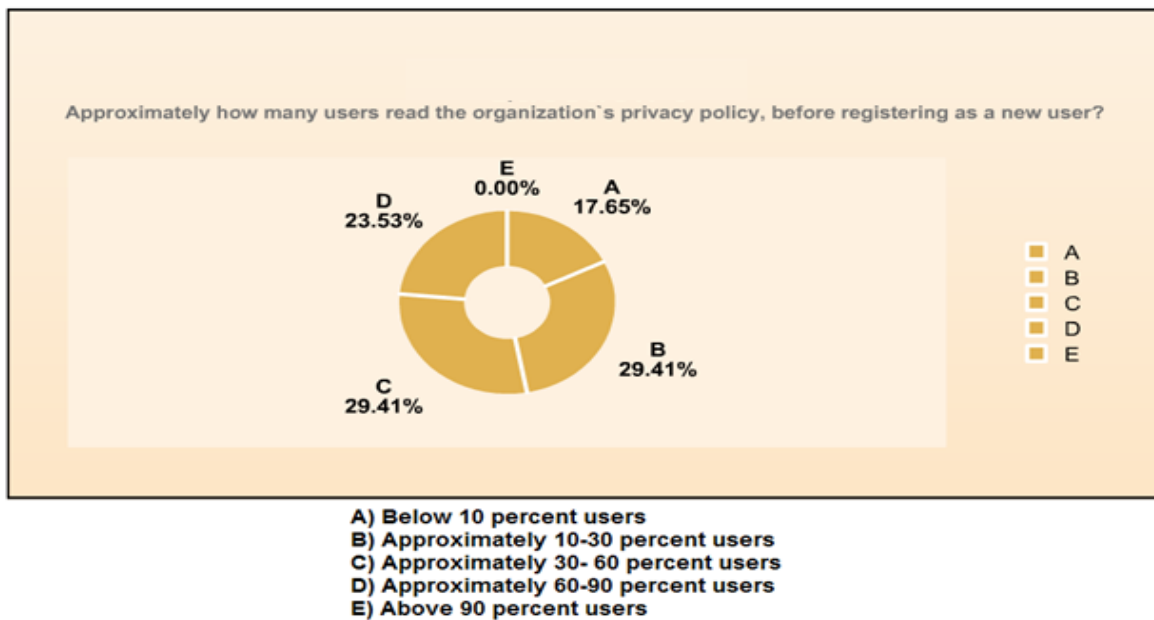


Figure: 5.2.7 Response reading the policy contents from subscribers

5.2.8 Level of understanding privacy contents for subscriber

With the help this question, we got an idea of the level understandability of privacy contents for subscriber from the service providers' point of view. In figure 5.2.8 a bar chart is showing that 80 percent of the respondent organizations think that "*some of contents of privacy policy deal with the legislation and they are not relevant for common users*". While 60% of the respondent organizations think that "*privacy contents are highly relevant and they determines the user's operational limitation*". Finally 30% of the respondent service providers think that "*the privacy policy contents are not relevant for them*" and they just explains unnecessary text etc".

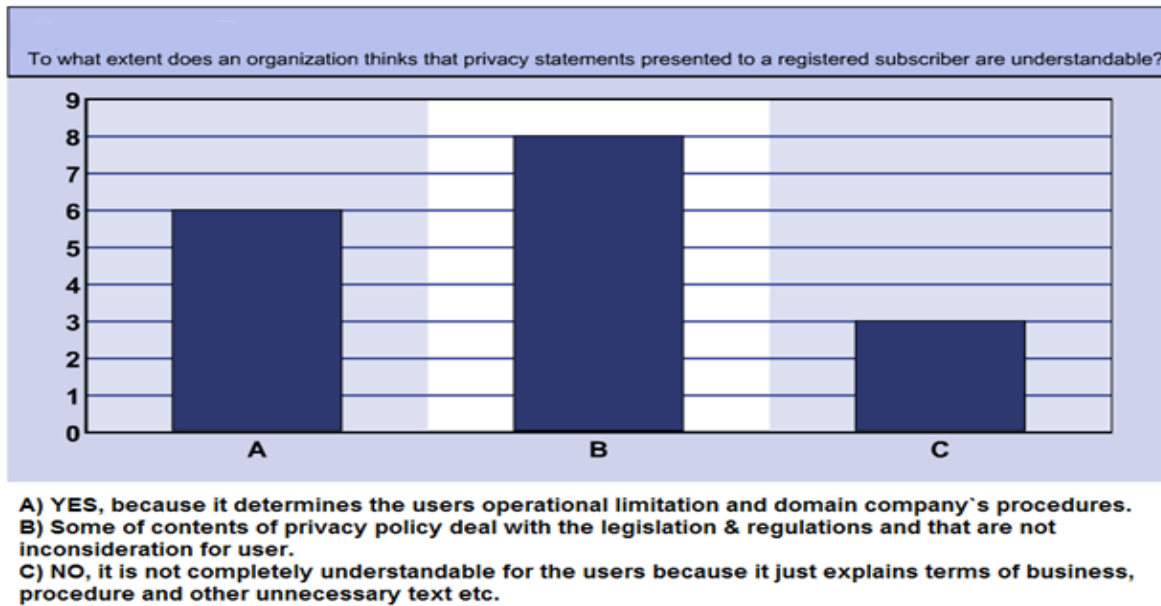


Figure: 5.2.8 Level of understanding privacy contents

5.2.9 Any review body on setting up “privacy policy”

From this question we were asking from the respondent companies if they have some review body and all the respondent companies answered that they have a review committee on privacy policy. Total 6% of the respondent companies voted that they have a review body / committee on privacy policy and they amend or modify the policies “every year”. As shown in figure 5.2.9 five percent of the companies amend their privacy policy after “more than two years”.

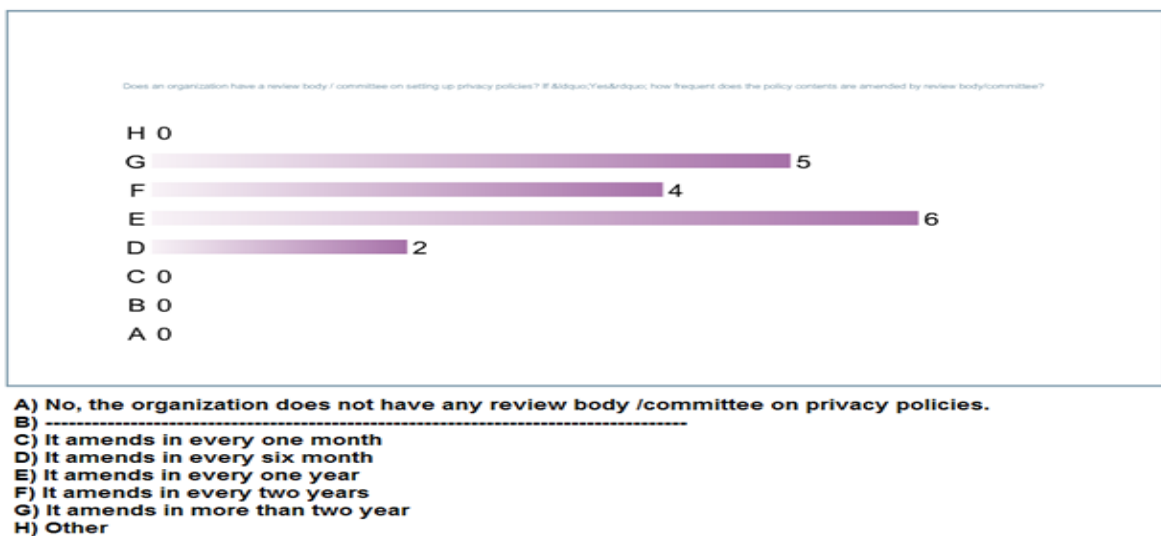


Figure: 5.2.9 Response of having review body on Privacy policy

By evaluating the graph we can observe that just 4% companies amend their privacy policy context in “*every two year*”. Next percentage is 2 percent, showing that just few companies review their privacy contents after “*every six months*”.

5.2.10 Retention regulation in service provider privacy policy

Figure 5.2.10 shows the responses to our question about the retention regulation followed by the service provider in their defined privacy policy. The retention regulation is an important part of any privacy policy.

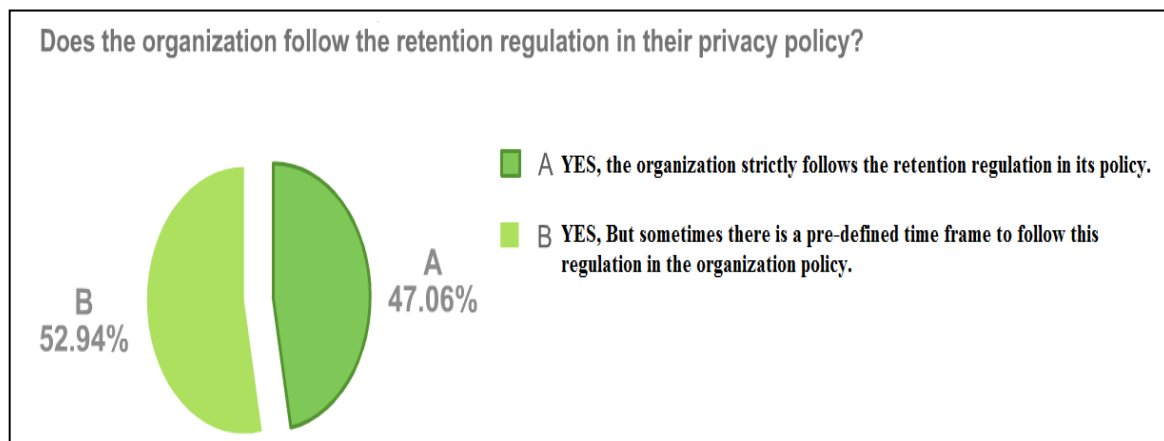


Figure: 5.2.10 Response of following retention regulation

By analyzing the pie chart we see that majority (i.e. 53 percent) of the respondent companies in Norway follow the retention regulation but there is a pre-defined time frame to follow this regulation. Next we have 47% of the respondent service providers that strictly follow the retention regulation in their privacy policy.

5.2.11 Disclosure of subscriber`s personal information

As explained in figure 5.2.11 we have asked the companies about to what extent they disclose the subscribers` personal data to any 3rd party or 3rd vendor. We have got a positive response that 7 percent of the service providers are mentioning in their privacy policy that “*the organization can disclose the personal data of subscribers if the Country / State law enforcement agencies or bodies request*”.

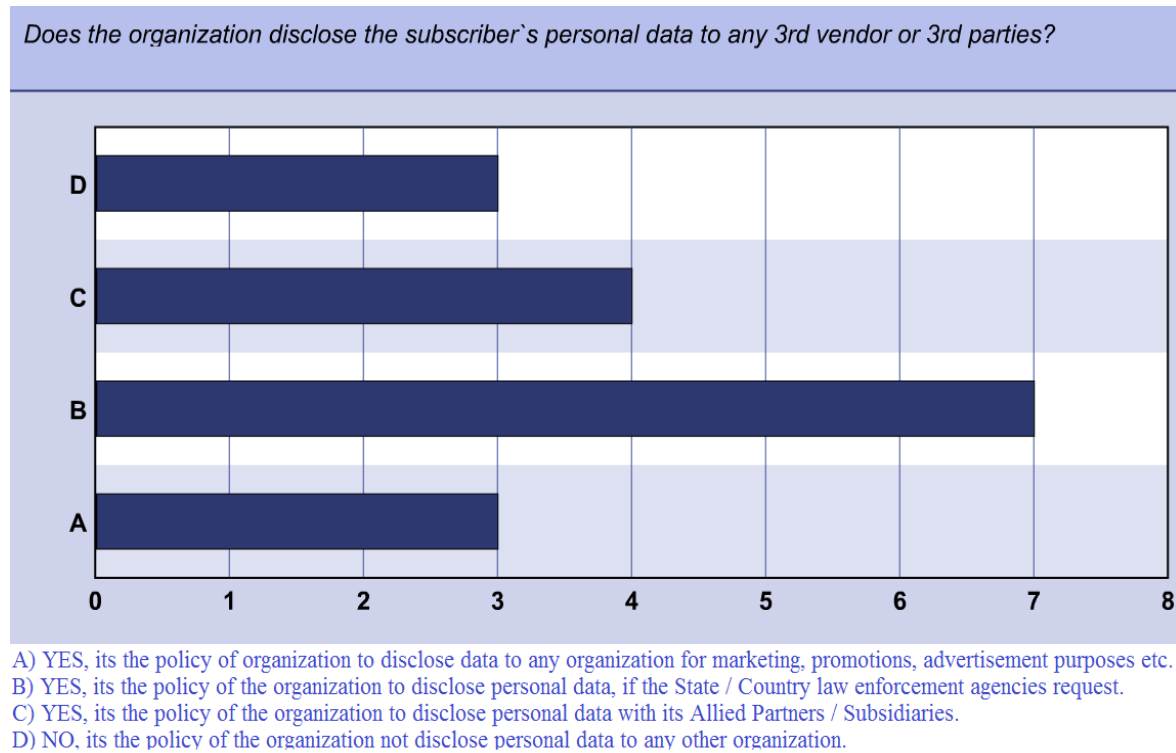


Figure: 5.2.11 Response of disclosure of personal information

About 4 percent of the respondent service providers voted that it is in their privacy policy that “they can disclose the personal information of their users to allied partner, collaborator or subsidiary firms etc”. Nearly 3 percent of the service providers “do not disclose the subscriber`s personal data to any other organization what so ever happened and this is mentioned in their privacy policy”. Finally, 3 percent of the respondents said that “they disclose the personal data to any organization for marketing, promotion and for advertisement purposes etc”.

5.2.12 Request from subscribers to review personal information

Figure 5.2.12 shows the frequency of requests to review the personal information from the registered subscribers. Here, 6% of the respondent organization have answered that they receive such requests “twice a year” from their users. 4% of the service providers voted that they do receive the request “twice every 6 months”. 3 percent of the service providers answered that once a year they receive the update information request from their registered

users and with the same percentage the organization receives request more than twice in a year. Finally, just only 1% of the service providers said that after two years of time they receive the request from their users.

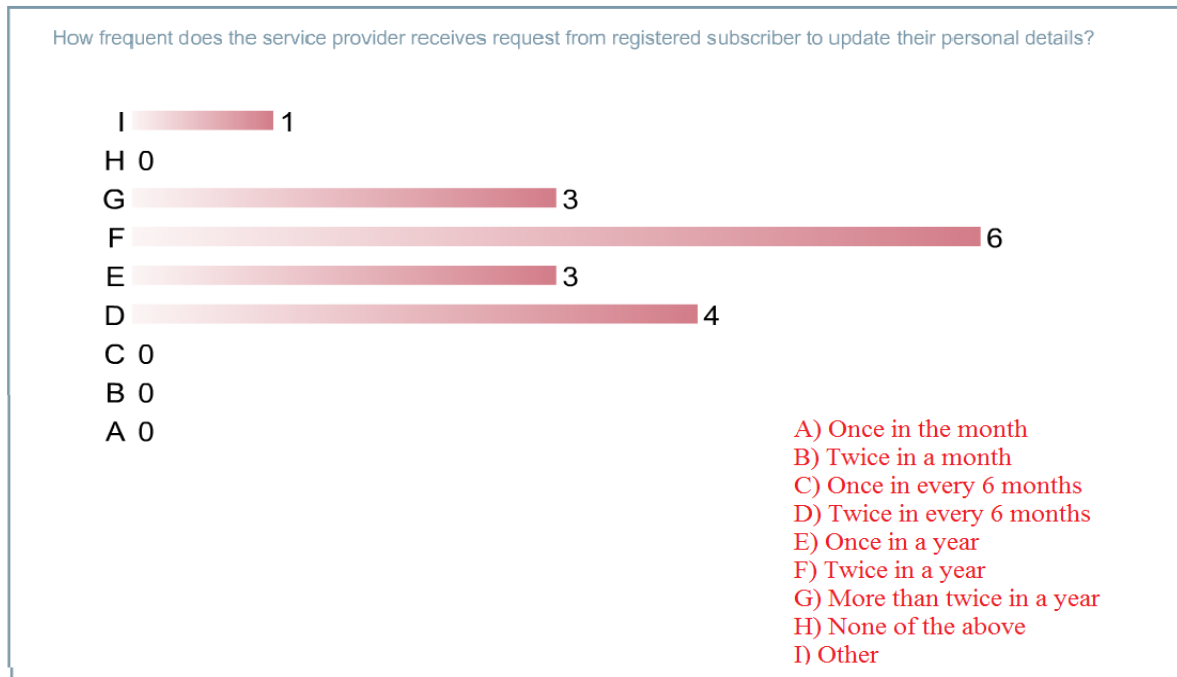


Figure: 5.2.12 Level of request to review personal information

5.2.13 Level of building confidence & trust for subscriber

The result shown in figure 5.2.13 describes how the service providers build confidence and trust for a subscriber in terms of privacy and how they performing their operations which are trustful to their users.

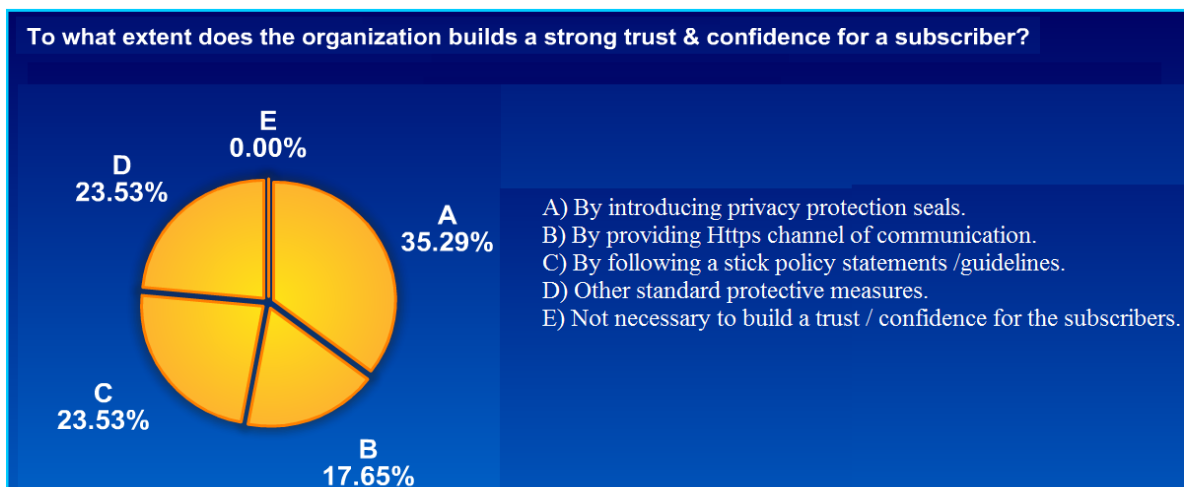


Figure: 5.2.13 Level of confidence and trust for a subscriber

Approximately 35% of the respondent service providers said that by introducing the privacy protection seals on their website they can build a strong trust and confidence for their subscribers. 23% answered to this question that to build a trust by following a strict policy statements and guidelines in their website. About 23% of the service providers take other standard protective measures. Just 18% of the service providers are providing Https secure channel of communication to ensure the privacy of their subscribers.

5.2.14 Response of handling privacy violation reports from subscriber

Figure 5.2.14 shows how often a service provider handles privacy violation cases and reports from subscribers. We noticed that 7% (which is in majority) deal the privacy policy violation reports more than twice a year.

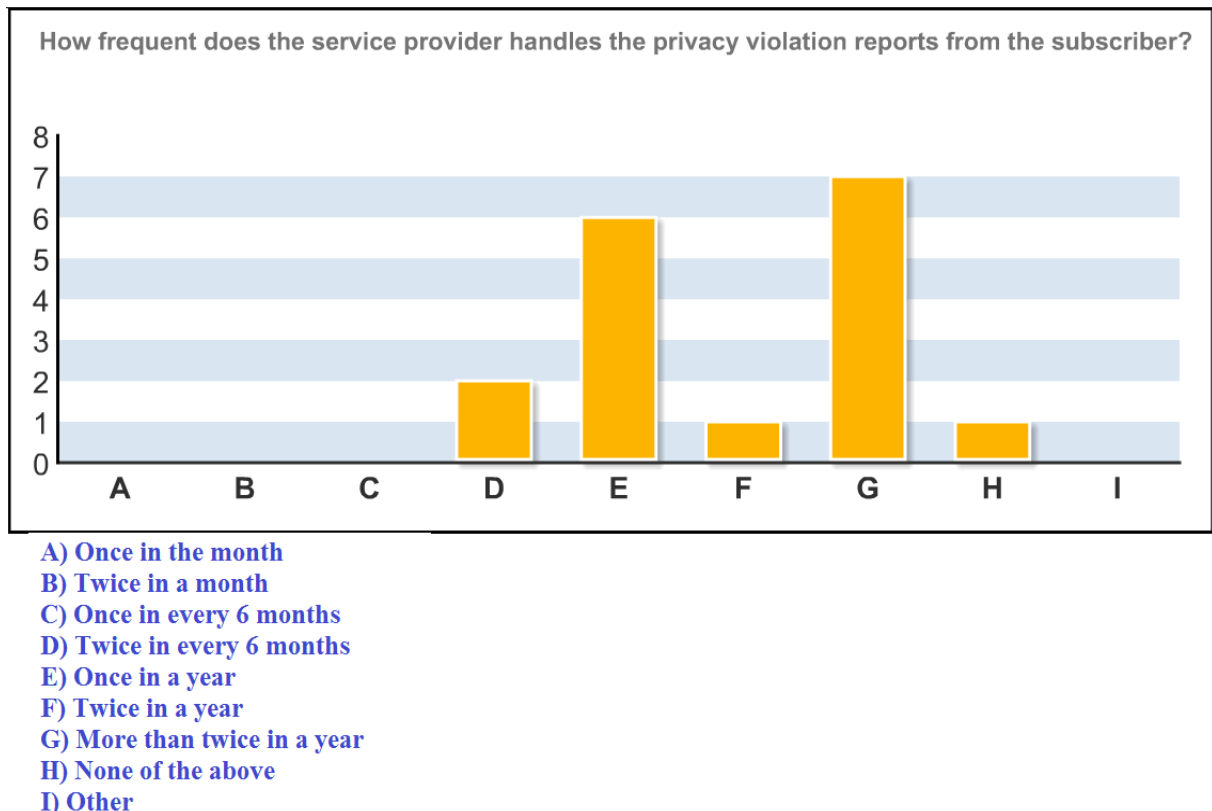


Figure: 5.2.14 Response of handling policy violation reports

About 6% of the respondent organizations once in a year handle privacy violation reports from the subscribers. Just 2% of the respondent service providers say that they handle the privacy

policy violation reports twice in every 6 months. Only 1% respondent's service providers receive twice a year privacy violation cases from the subscribers. Just 1% of the response comes from the service provider that they have not received any privacy violation reports from any subscriber.

5.3 Discussion

The results from these two surveys (*i.e.: one is user survey and the other is service provider survey*) were unexpected and interesting for us.

The ratio of answering these online user surveys could be biased by the male responses as compared to female responses. Another aspect is that, it mostly the result of knowledge of privacy policy could however have been biased by the high level of knowledge and education among respondents (*24% user survey questions were completed by the bachelors and masters degree holding participants*). Here it is also a fact that the majority of the user survey respondents belong to (*20 - 30 years of age category*). Similarly, the results showing that a large number of respondents claimed to have a high frequency of not reading the policies (*40% participants have not read them whenever they registered as a new subscriber*) and it was very surprising that 24% of the participants have not ever tried to read the policy contents because they don't have time. About 34% of the participants said that they don't feel that the privacy policies presented to them while they are registering are relevant, and it was shocking for us to see that 23% of the participants said that they do not have any idea about the relevancy of policy. Furthermore we have observed from the results of the user survey that 40% of the respondents do not feel comfortable to give their social security number and 24% of the respondents are not giving their date of birth to service providers. In this user survey we have found that 24% of the users have not ever sent any request to update or review their personal information from their service provider and, interestingly, 51% of the participants in this user survey are not aware about any changes / amendments from their service provider.

By further analyzing the online service provider survey we have noticed a difference in opinion as compared from the user survey.

The first factor we have noticed is that nearly all the services providers are giving a strong importance on the privacy policy aspect; but as we have discussed above why just (*10 to 30 percent*) of the users completely read the policy contents. The users have mentioned that they do feel difficulty in reading and understanding the privacy policies. In this survey at least 3%

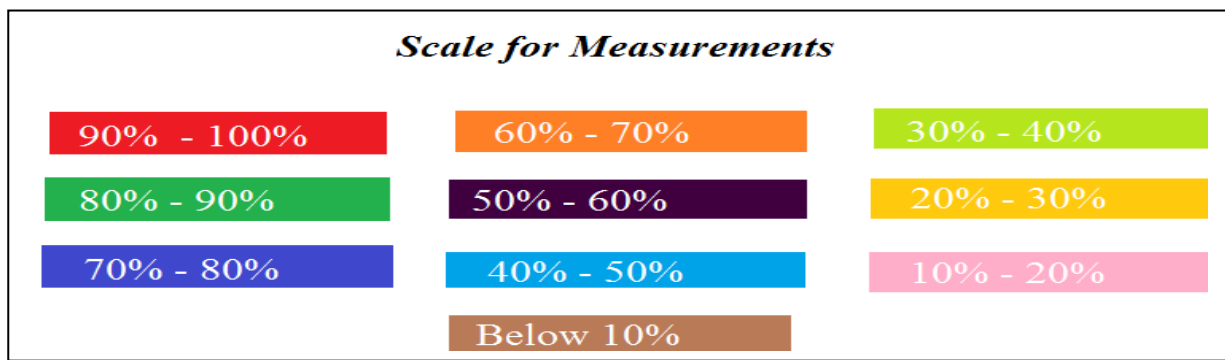
of the service providers agreed that policy presented by them mainly contains the business and legal terminology and they are not in concern from their subscribers. Highlighting again the service provider survey, nearly 6% of the companies claim that their policy contents are relevant and they explain all the procedure and operation of company dealing with the personal information of users. This differs from the user survey in that 34% local user think that these policies are not relevant for them.

5.4 Trends

In this section we will show some different trends of these both online surveys. In user survey we have 6 age categories and each category have different set of responses as compared from other category. We would also show the responses from different service providers. This would give us a brief perception from both sides (i.e. from users and from service providers);

5.4.1 Age category from 20-30 years (*27 respondents*)

In table 5.4.1, there are total 27 respondents in this age category and it seems that in this category there is a male dominancy and mostly all respondent are in high school. The majority of the participants are common / home user, but they used to spend below 10 hours over the internet. Similarly these respondents are not familiar with the terminology of privacy policy and they don't read the policy contents when they became a new registered user with any service provider. That is the main reason that they don't understand them and always ignore the regulation inside the privacy statements. This age category feels that privacy policies are not relevant for them and whenever there are any changes done by the service provider they are not aware.












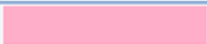


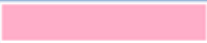
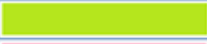






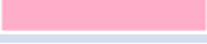





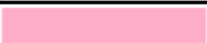
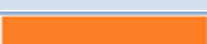

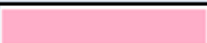
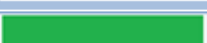

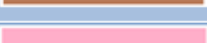


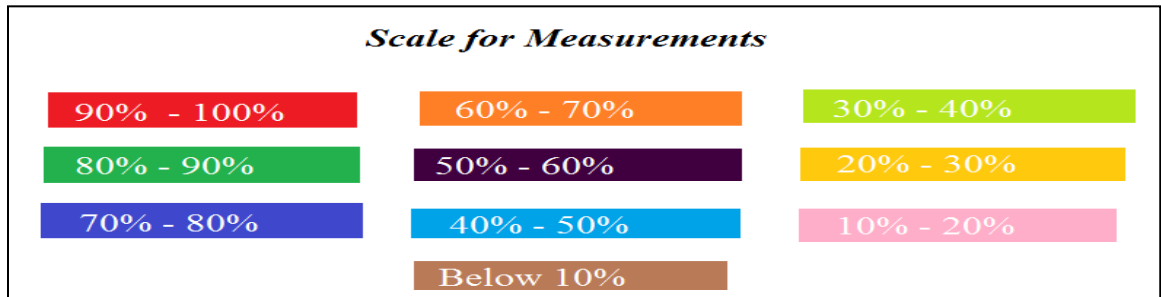
S.No	Questions in User Survey	Categories	Results
1	Gender	Male	
		Female	
2	Education	High School	
		Bachelor's	
		Master's	
		Post Doc	
3	Status	Administration / Management	
		Professionals	
		Research / Academia / University	
		Marketing / Advertisement	
		Students	
		Home / Common Level	
4	Working Hours Per Week	Below 10 hours	
		10 to 20 hours	
		20 to 30 hours	
		30 to 40 hours	
		40 to 50 hours	
		More than 50 hours	
5	Familiarity with privacy policy	YES, I am aware	
		NO, I am not aware	
		I am not sure exactly	
6	Reading of Privacy policy	YES, I read	
		NO, I don't read	
		I don't have time to read	
7	Difficulty in understanding	YES	
		NO	
		I don't understand and read always	
8	Relevancy of the privacy policy	YES, they are relevant	
		NO, they are not relevant	
		I don't have idea of relevancy	
9	Awareness about the Changes/ Amendments	YES, I am aware	
		NO, I am not aware	
10	Request for update/review of personal information	Once in week	
		Once in month	
		Twice in month	

Table 5.4.1 Analysis in tabulated form in terms of percentage (20 To 30 years)

5.4.2 Age category from 30-40 years (*17 respondents*)

There are total 17 respondents in this age category and by analyzing table 5.4.2, we noticed that respondents are mature in terms of education level and majority are male respondents but 6 percent of the females also participated.



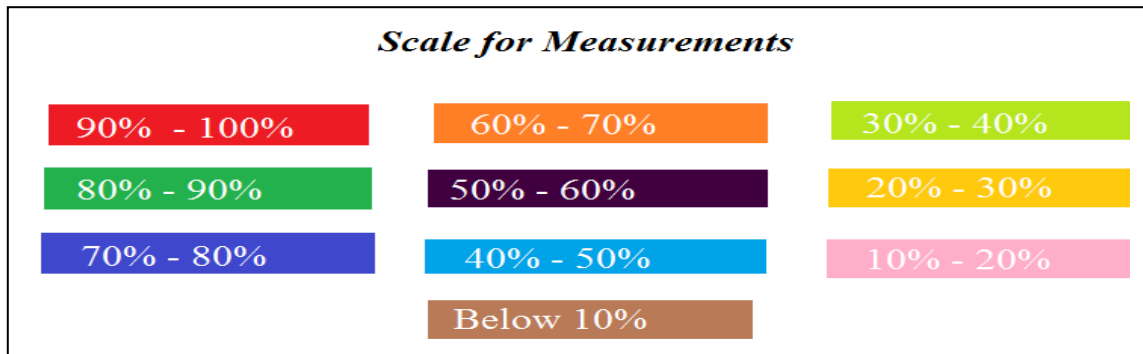
<i>S.No</i>	<i>Questions in User Survey</i>	<i>Categories</i>	<i>Results</i>
1	Gender	Male	
		Female	
2	Education	High School	
		Bachelor's	
		Master's	
		PhD	
3	Status	Administration / Management	
		Professionals	
		Research / Academia / University	
		Marketing / Advertisement	
		Students	
		Home / Common Level	
4	Working Hours Per Week	Below 10 hours	
		10 to 20 hours	
		20 to 30 hours	
		30 to 40 hours	
		40 to 50 hours	
		More than 50 hours	
5	Familiarity with privacy policy	YES, I am aware	
		NO, I am not aware	
		I am not sure exactly	
6	Reading of Privacy policy	YES, I read	
		NO, I don't read	
		I don't have time to read	
7	Difficulty understanding in	YES	
		NO	
		I don't understand and read always	
8	Relevancy of the privacy policy	YES, they are relevant	
		NO, they are not relevant	
		I don't have idea of relevancy	
9	Awareness about the Changes/ Amendments	YES, I am aware	
		NO, I am not aware	
		Other users inform me about any changes / Amendments	
10	Request for update/review of personal information	Once in week	
		Once in month	
		Twice in month	
		Once in every 6 months	
		Twice in every 6 months	
		Once a year	
		Twice a year	
I have not requested ever			

Table 5.4.2 Analysis in tabulated form in terms of percentage (30 To 40 years)

Here we can find that most of them have professional level status and work between 20-30 hours per week on the internet. Mostly these are familiar with privacy policy. This category of participants don't read the context of the privacy policy when they registered and about 77% of the participants feel difficulty in reading them.

5.4.3 Age category from 40-50 years (*13 respondents*)

There are total 13 respondents in this age category. In table 5.4.3, approximately 76 percent of the respondents are male and just 24% of them are females. Majority of the respondents have a masters degree and 8% percent of them have a doctorate degree. In this age category we have the academia and business community. These category respondents are not sure about what the privacy policies are but they do have some related knowledge. This age category respondents do not read the policy and they do feel difficulty to understand them. This category respondent feels that privacy policy contents from the service provider are not relevant for them, and they are not informed about any changes in the privacy policy.

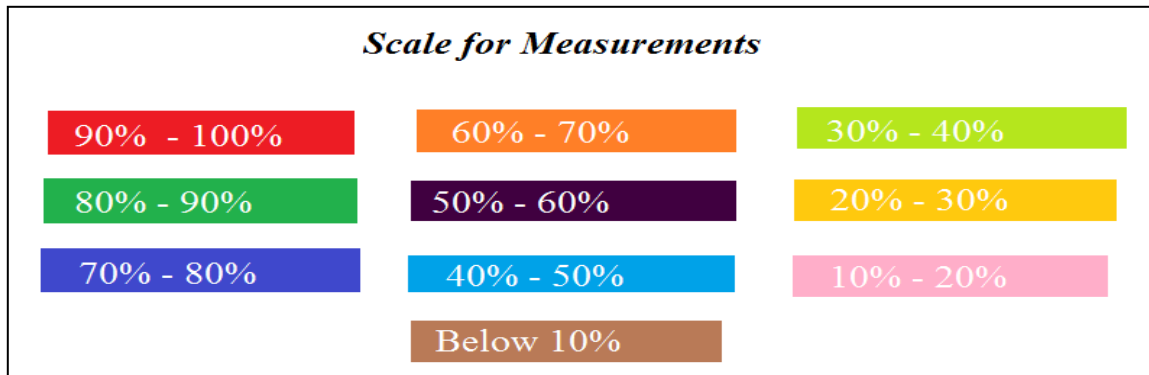


S.No	Questions in User Survey	Categories	Results
1	<i>Gender</i>	Male	
		Female	
2	<i>Education</i>	Bachelor's	
		Master's	
		PhD	
		Post Doc	
3	<i>Status</i>	Administration / Management	
		Professionals	
		Research / Academia / University	
		Business / Trade	
		Marketing / Advertisement	
		Home / Common Level	
4	<i>Working Hours Per Week</i>	20 to 30 hours	
		30 to 40 hours	
		40 to 50 hours	
5	<i>Familiarity with privacy policy</i>	YES, I am aware	
		NO, I am not aware	
		I am not sure exactly	
6	<i>Reading of Privacy policy</i>	YES, I read	
		NO, I don't read	
		I don't have time to read	
7	<i>Difficulty in understanding</i>	YES	
		NO	
		I don't understand and read always	
8	<i>Relevancy of the privacy policy</i>	YES, they are relevant	
		NO, they are not relevant	
		I don't have idea of relevancy	
9	<i>Awareness about the Changes/ Amendments</i>	YES, I am aware	
		NO, I am not aware	
		Other users inform me about any changes / Amendments	
10	<i>Request for update/review of personal information</i>	Once in week	
		Once in every 6 months	
		Once a year	
		Twice a year	
		I have not requested ever	

Table 5.4.3 Analysis in tabulated form in terms of percentage (40 To 50 years)

5.4.4 Age category from 50-60 years (*18 respondents*)

Analyzing the table 5.4.4, there are total 18 respondents and in this age category. We have 66% of the participants are male participants. These category respondents have a higher education level as compared to the previous categories. There are high percent respondents from research / academia and from the business / trade sector.















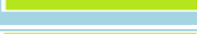




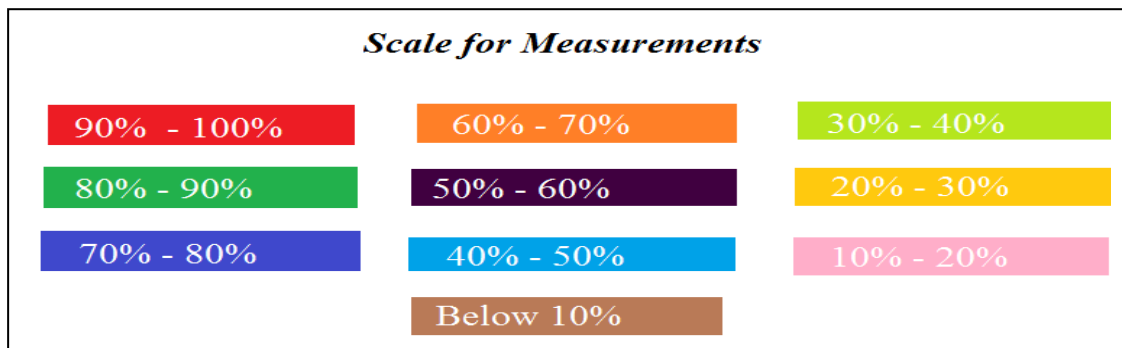
S.No	Questions in User Survey	Categories	Results
1	Gender	Male	
		Female	
2	Education	High School	
		Bachelor's	
		Master's	
		PhD	
		Post Doc	
3	Status	Administration / Management	
		Professionals	
		Research / Academia / University	
		Business / Trade	
		Marketing / Advertisement	
		Home / Common Level	
4	Working Hours Per Week	Below 10 hours	
		10 to 20 hours	
		20 to 30 hours	
		30 to 40 hours	
		40 to 50 hours	
5	Familiarity with privacy policy	YES, I am aware	
		NO, I am not aware	
		I am not sure exactly	
6	Reading of Privacy policy	YES, I read	
		NO, I don't read	
		I don't have time to read	
7	Difficulty in understanding	YES	
		NO	
		I don't understand and read always	
8	Relevancy of the privacy policy	YES, they are relevant	
		NO, they are not relevant	
		I don't have idea of relevancy	
9	Awareness about the Changes/ Amendments	YES, I am aware	
		NO, I am not aware	
		Other users inform me about any changes / Amendments	
10	Request for update/review of personal information	Once in week	
		Once in month	
		Twice in month	
		Once in every 6 months	
		Once a year	
		Twice a year	
		I have not requested ever	

Table 5.4.4 Analysis in tabulated form in terms of percentage (50 To 60 years)

The working conditions in this category are 30-40 hours per week on internet and these respondents do not read the privacy policy when they give their personal information to the company. This category respondent are comfortable with the language and easily understand the policy contents.

5.4.5 Age category from 60-70 years and above (*5 respondents +1 respondent of age 70 above*)

There are total 6 respondents in the category including one respondent that is above 70 years. Female respondents are in major respondent as compared to the male respondents. These respondents are mainly home users and they use to work below 10 hours per week on the internet. About 60 percent of the respondents are not sure about the privacy policy but they have a good knowledge.



S.No	Questions in User Survey	Categories	Results
1	<i>Gender</i>	Male	
		Female	
2	<i>Education</i>	Master's	
		PhD	
		Post Doc	
3	<i>Status</i>	Administration / Management	
		Business / Trade	
		Research / Academia / University	
		Home / Common Level	
4	<i>Working Hours Per Week</i>	Below 10 hours	
		10 to 20 hours	
		20 to 30 hours	
5	<i>Familiarity with privacy policy</i>	NO, I am not aware	
		I am not sure exactly	
6	<i>Reading of Privacy policy</i>	YES, I read	
		NO, I don't read	
		I don't have time to read	
7	<i>Difficulty in understanding</i>	YES	
		NO	
		I don't understand and read always	
8	<i>Relevancy of the privacy policy</i>	YES, they are relevant	
		NO, they are not relevant	
9	<i>Awareness about the Changes/ Amendments</i>	YES, I am aware	
		NO, I am not aware	
	<i>Request for update/review of personal information</i>	Once a year	
		Twice a year	

Table 5.4.5 Analysis in tabulated form in terms of percentage (60 To 70 years)

These category respondents do read the policy when they give their personal information to the service provider but these respondents are not aware on any changes / amendments in privacy policy.

5.4.6 Response from the Internet sector

In figure 5.4.7, we have collected the response from the internet sector in Norway. The entire service provider follows the Norwegian personal data act of [2000] as a privacy regulation whenever they collect the personal data from the Norwegian subscribers and 17 percent of the

registered users are approximately are more than 300, 0000. The internet sector is giving the high priority to the privacy policy phenomena.

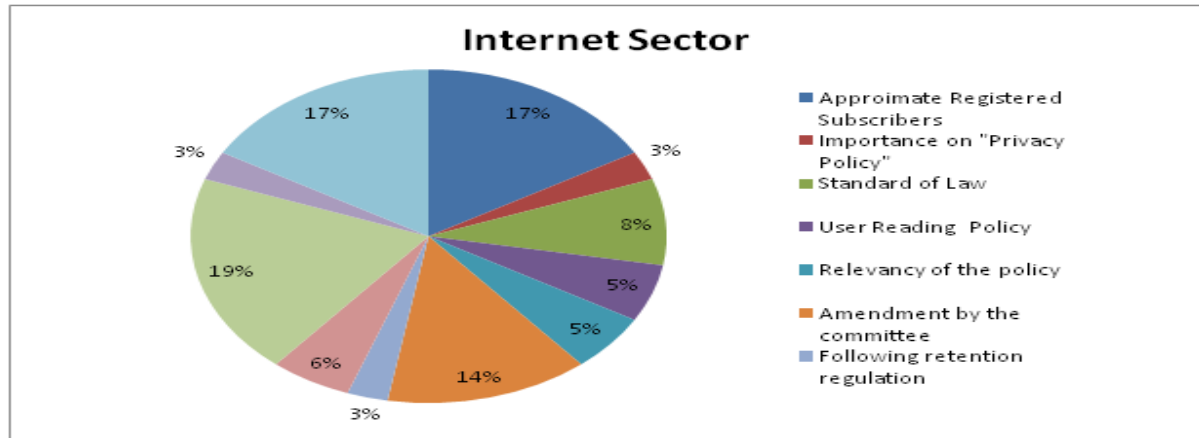


Figure 5.4.6 Response from the Internet sector

This sector thinks that a 30 to 60 percent of the users read their privacy statements before registering themselves as a new user. It is interesting to note that some policy contents in this sector are deal with the legislation & regulations and that are not inconsideration for user. The policy amendments are generally performed after every year. Majority of this sector companies follows a strict retention policy.

5.4.7 Response from the telecommunication sector

As shown in the figure 5.4.8, the response from the telecommunication sector of Norway. Just one service provider was operating outside the Norway. There were approximately More than 300, 0000 registered users with these service providers and they follows the Norwegian personal data act of [2000] as a standard law for collecting the personal information from there users only one service provider follows the European Union personal data directive of [1995].

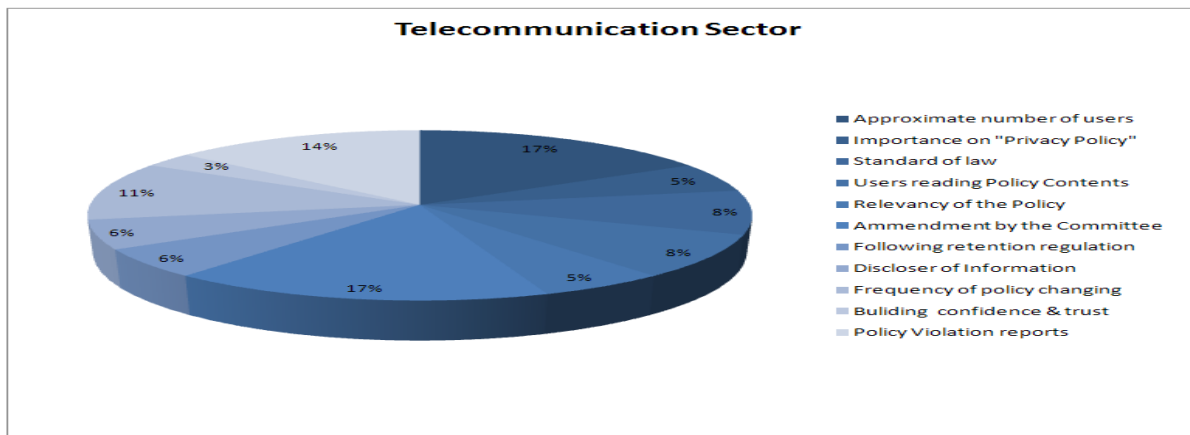


Figure 5.4.7 Response from the telecommunication sector

Here the respondent companies give an average importance on the privacy policy phenomena, and these respondent organizations perception is that round 60 to 90 percent of their users read the privacy statements before signing up as a new user with the organization. The majority of respondent service provider also thinks that some of contents of privacy policy deal with the legislation & regulations and that are not inconsideration for user and very few thinks that regarding the understanding of their policy context that it is not completely understandable for the users because it just explains terms of business, procedures. This respondent sector after every two years time gap amends their policy and they have a proper review committee of amending the privacy policy.

5.4.8 Response from the scientific / research / academia sector

The figure 5.4.9, examines the response comes from the research / academia sector from our online based survey. All the respondents are operating inside Norway. There are 2, 00000 - 250, 0000 registered users associated with this sector and all the respondent organization gives strong importance to privacy of the user and its policy contents. All the respondent organization follows the Norwegian personal data act of [2000] when the request user to enter their personal information.

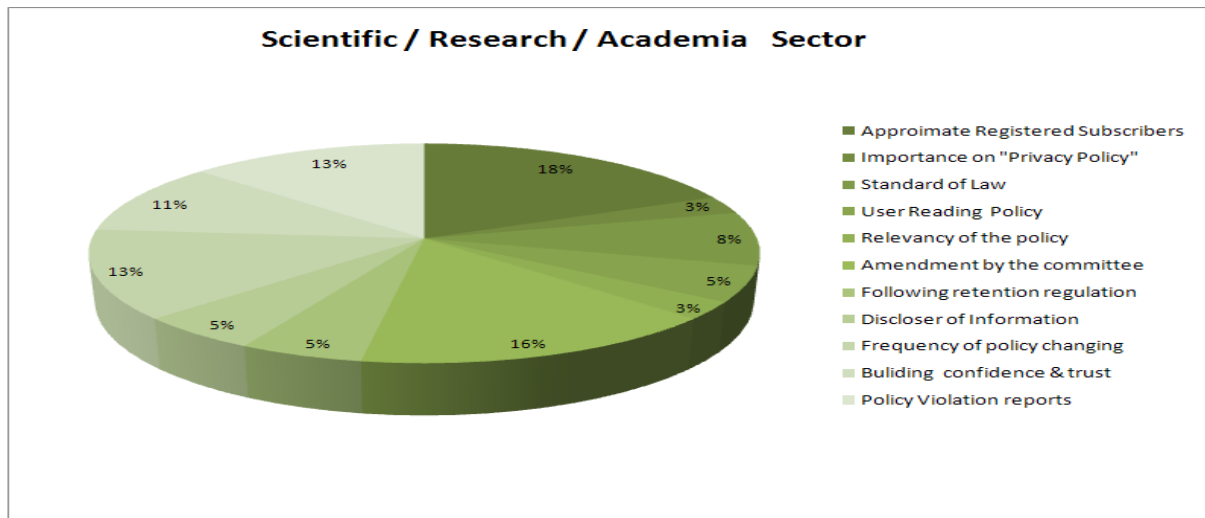


Figure 5.4.8 Response from the scientific / research / academia sector

It was surprising for us to see that according to the respondent organization thinks just 10 to 30 percent of the users read privacy policy and they thinks that privacy policy presented to the users are very well understandable because it determines the user's operational limitation and

domain company's procedures. These respondent organizations also disclose the user's personal data because it is mentioned in their policy that the organization to disclose personal data, if the State / Country law enforcement agencies request and it can share the data to their allied partners, collaborated firms or their Subsidiaries.

5.4.9 Response from the financial sector

We are showing in figure 5.4.10, the response comes from the financial sector from our survey research. This financial sector purely operates in Norway and follows strictly the Norwegian personal data act of [2000]. Approximately it has more than 300, 0000 registered users and indeed the financial sector gives a very high priority on privacy of their registered users which shows a positive sign of their operations.

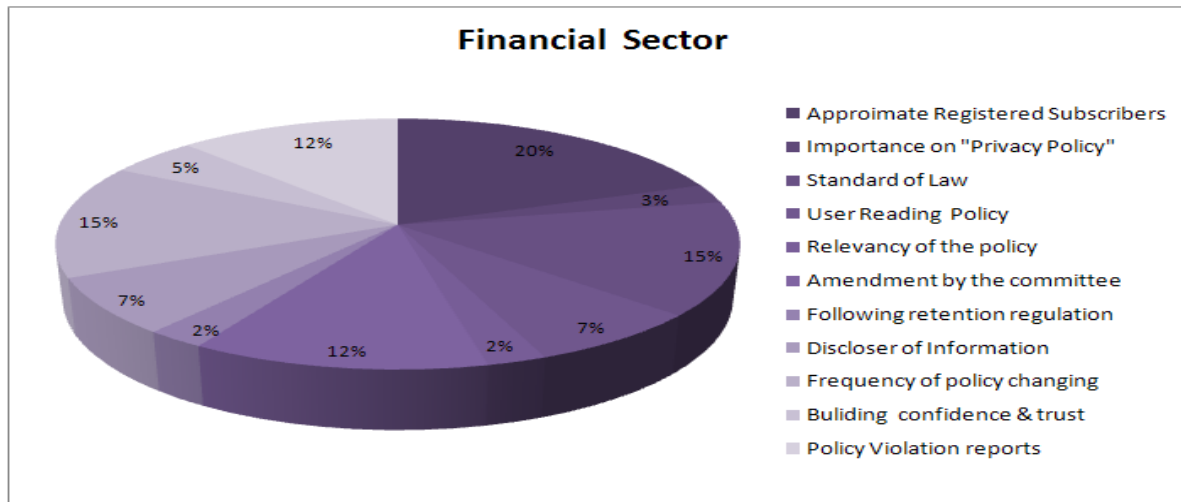


Figure: 5.4.9 Response from the financial sector

The financial thinks that between 30 to 60 percent of the users read their privacy policy before they are using their services and this respondent sector also thinks that their privacy policies are well understandable and they purely determines the user's operational limitation and domain company's procedures. The respondent sector amends its privacy policy every year and they follow strictly the retention regulation in their privacy policy. This sector builds a strong trust & confidence for a subscriber by providing the Https channel of communication on their official websites.

5.5 Answering of research questions

The first research question that we have defined from the user's / subscriber's perspective was;

RQ#1. How important is the phenomenon of privacy policy for a common user to accept it?

We received some interesting facts from the user survey saying that 90 percent among all the age categories are somehow familiar with the privacy policy phenomena, but they exactly do not know what the actual terminology is and its professional meaning. They usually think that it is a just Law notice that tells about legal status of any service provider/ organization. As we have seen in (*chapter#2, Background realities*) and privacy regulations, acts, standards, and laws vary extensively from country to country and from state to state, and some of the organizations are yet to apply the privacy regulations. It might be an indication that a common user is not finding any reasons to deny any context that are presented in front of them.

Another interesting finding in this survey was that a majority of the respondents were between age 20 to 30 years, and most of them were male respondents. In our user survey, we have asked that before registering as a new subscriber, have they read the privacy policy? We got the answer that approximately 98 percent of the users do not read the privacy policy before registering and they don't have time to go through the whole policy. In the survey we have asked an important question regarding the awareness of users, when the service provider amends the privacy policy? Approximately 97 percent of the subscribers are not aware about such amendments and do not receive any notification. This indicates like an alarming situation that a common users that is a vital part of any website's privacy policy and are they not informed about any changes. Such actions could damage a website reputation and could lose the subscribers. It is main responsibility of the service providers to take user in to confidence if they are about to change their security settings.

Apart from the survey, we have generally asked two open end questions from different people of different age to get some basic knowledge about the terms "privacy" and "policy". Following are some responses we have got;

For the term Privacy:

- “Control over own personal information’s!”
- “Not to be shared with anyone”
- “Hiding of personal information, stuffs or work from the other people”
- “It is about the rights of end-user’s protection of information”
- “The privacy includes the user being provided freedom & security to publish the information”

For the term Policy:

- “A description with commitments from the end-users!”
- “Rules and regulation for keeping the data secure and guarantying its usage”
- “A legal contract that offers to the user about the rights and obligations of the company/organizations”
- “Set of promises towards the protection of some entity”
- “Description of acts use to regulated a service for usage”

By analyzing the responses, we can conclude that most respondents are not sure that actual concept behind these terms.

The second research question that we have defined from the user’s / subscriber’s perspective was;

RQ#2. Are the contents fully read and understood by the users before accepting the policy?

Consistent with the literature review, we have found that privacy policy content length was also one of the main reasons for why the people do not like to read the whole policy. Policies are boring to read and users believe all policies have the same content with same regulations etc.

Our user survey respondents were very educated (having bachelor’s and master`s degrees), and none of the participants have disagreed with the privacy policy when they become subscribers. According to our results, 85 percent of the participants feel very difficulty in understanding the context of the privacy policy and many participants said *“they dont ever read and understand the privacy policy before using the services”*. As shown in the figure 5.5.1, about 69 percent of the respondents think that these policies are not relevant for them and 16 percent of the respondents have no idea about the relevancy of these policies.

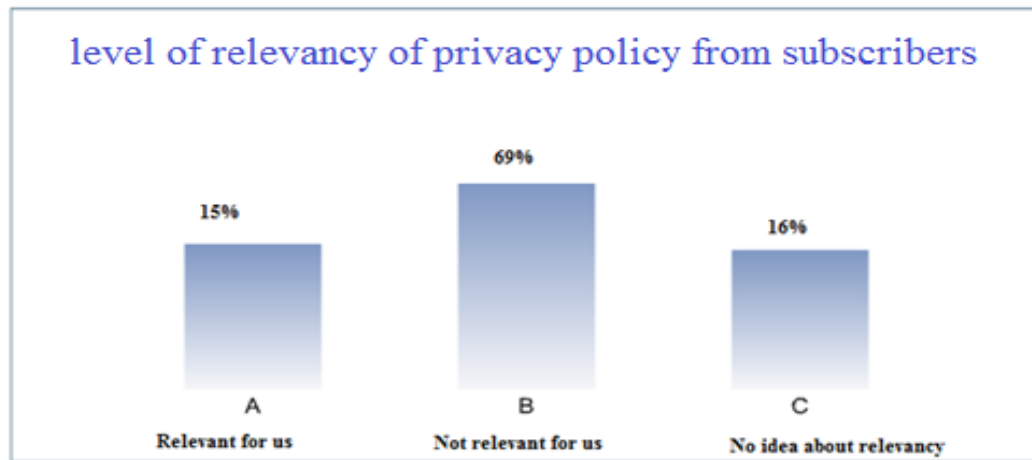


Figure: 5.5.1 Level of relevancy of Privacy Policy

Generally, many people have realized about the importance of this phenomenon. Users have shared their feeling from us that they want to use the services from companies, and they are compromising with their personal information, which is certainly a dangerous act. Privacy arise further issues in comparison to access control policies, as they require a more sophisticated treatment of deny rules and conditions on context information [6].

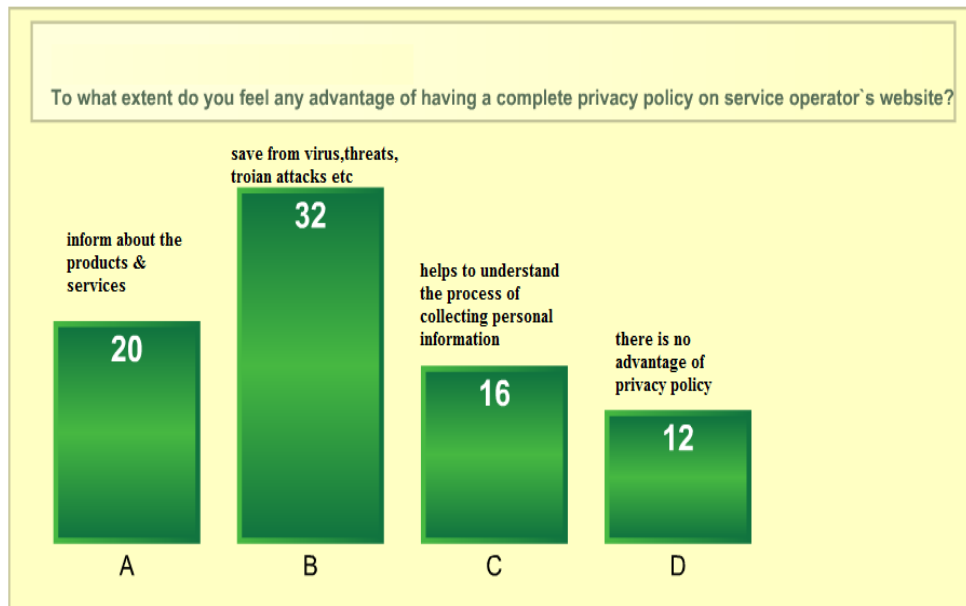


Figure: 5.5.2 Advantages of Privacy Policy

One of the important questions in survey was about advantages and disadvantages of privacy policies. We noticed that majority people have this perception that a privacy policy will save them from the viruses, threats and many Trojans attacks etc as shown in the figure 5.5.3.



Figure: 5.5.3 Disadvantages of Privacy Policy

If there is no privacy policy defined over the service provider's website then people think that a common subscriber can easily be phished by unknown user or maybe their personal information can be easily hacked.

The third research question that we have defined from the user's / subscriber's perspective was;

RQ#3. From user's perspective do the policies that are accepted have a difficult language and format?

Privacy policies are often written in a complicated language which a common user cannot easily understand. From the survey, we have found that policies presented have difficult language and most of the users cannot understand. An interesting fact we discovered in this survey is that nearly 72 percent of the participants feel difficulty in reading and understanding the privacy policy from the service provider website and a majority of the common users have not read the policy, before using the services from the organization. About 18 percent of the users feel that the language is readable and somehow they can get the idea from this complicated legal context. This was a closed question containing three choices of (*Yes, I feel difficulty in reading & understanding ; No, I don't feel difficulty ; I have not ever read & understand policy before using services of service provider*).

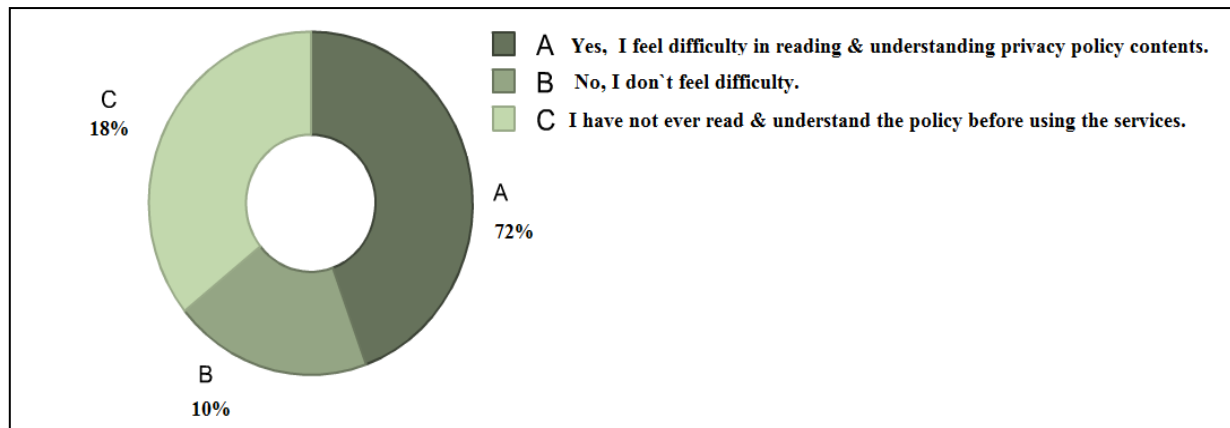


Figure: 5.5.4 Reading and Understanding of Privacy Policy

Mostly privacy policies have complicated legal terms and users are unable to understand. This situation shows that there should be a soft, easy and readable language adopted to help common subscriber to decide whether to accept or reject the policy. As shown in our user survey results, a large number of users are complaining about the language used in a policy. We have concluded from this discussion that a number of issues that are identified via this survey should be addressed by taking the common user into confidence, because users are concerned about their privacy and in order to gain the trust of user and boost the internet business the main player should provide a solid solution over these core issues. Voice of a local user about their privacy is rising day-by-day and users are worried about the security of personal information, and fear that it may be misused in future.

The first research question that we have defined from the service providers perspective was;

RQ#4. What is the current level of enforced privacy policy in different organization?

Analyzing the result from the service provider survey shows that many Norwegian service providers give a high priority to the subscriber's privacy policy and have shown that by giving a high frequency number in one of question about the level of importance to privacy policy;

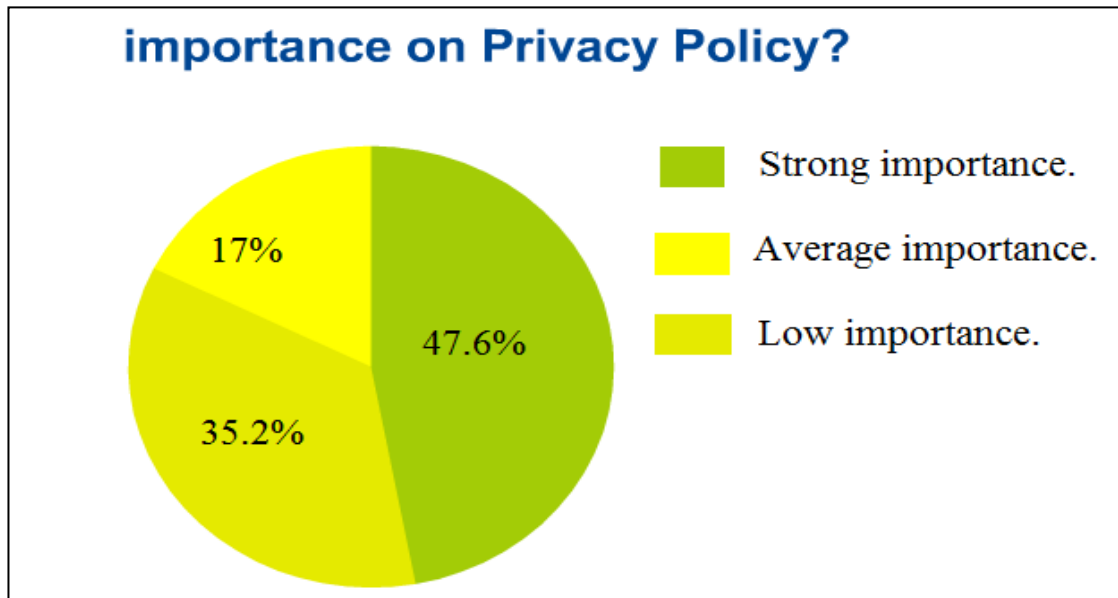


Figure: 5.5.5 Importance on Privacy Policy

This shows that companies are highly concerned about their business reputation in terms of security and privacy and the trust that they are showing to their loyal subscribers for collecting their sensitive information. But this is also a fact that none of the companies have claimed, that their privacy policy are read by every user or the frequency of reading organization's privacy policy is above 90 percent as shown in the following figure. It should be kept in mind that users have shown their reservation to give their personal data to the service provider as discussed in the above sections and, indeed, they also think that these privacy policy contents are not relevant for them. Users do feel problems to understand its language. It is interesting to see that most of the Norwegian service providers amend their privacy contents with the time gap of one year.

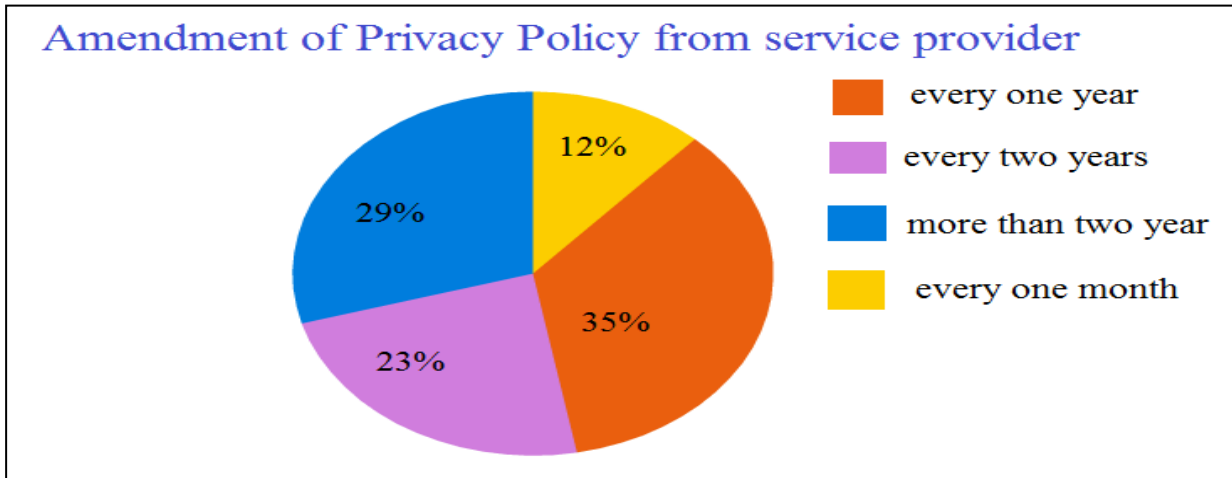


Figure: 5.5.6 Amendment of Privacy Policy

The second research question that we have defined from the service provider's perspective was;

RQ#5. How well is a privacy policy integrated in different service provider / organizations?

According to the POL clause 28 [41] , there is a prohibition against unnecessary storage of common user personal information. In order to keep the information as long as the service provider need, they have to inform user about their retention regulation in their privacy policy. The same clause also protects the user of right of awareness about any changes in the privacy policy. The survey which was conducted for the organization have shown that Norwegian organizations have a review body / committee for setting up privacy policy. Another interesting aspect we have identified in our research is that the Norwegian service provider follows the retention regulation within the defined limits in their privacy policy as shown in figure 5.5.7 .This is an appreciable aspect of privacy policy.

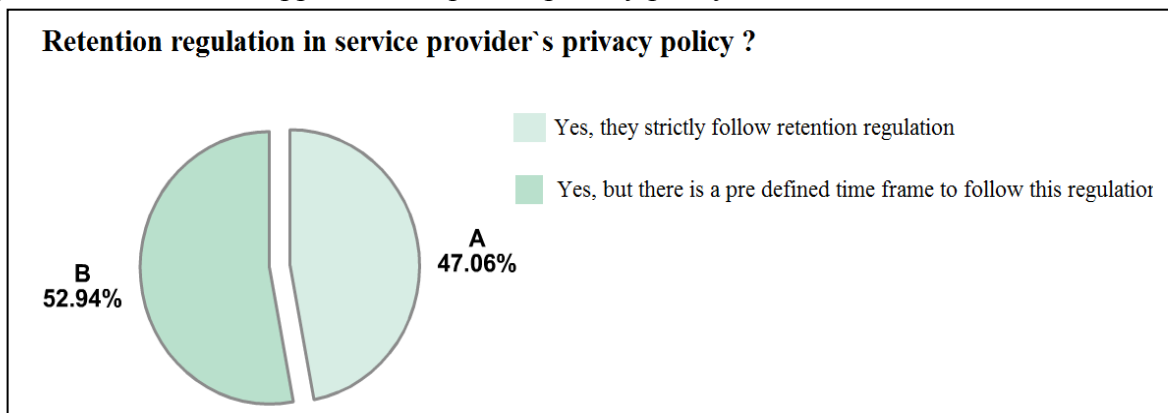


Figure: 5.5.7 Retention regulation in service provider policy

We have received some interesting findings as we have asked the question of disclosure of subscriber's personal data to any 3rd parties etc. The majority of the service providers disclose the information upon requests from state law body or any government agency. However, there exist few organizations, which do not disclose the personal data of users even in case of any requests. Every Norwegian service provider does have a review body / committee for setting up privacy policy. This review body / committee are responsible to design the privacy policy and amend the policy contents after some duration of time that varies from company-to-company and decision of review body.

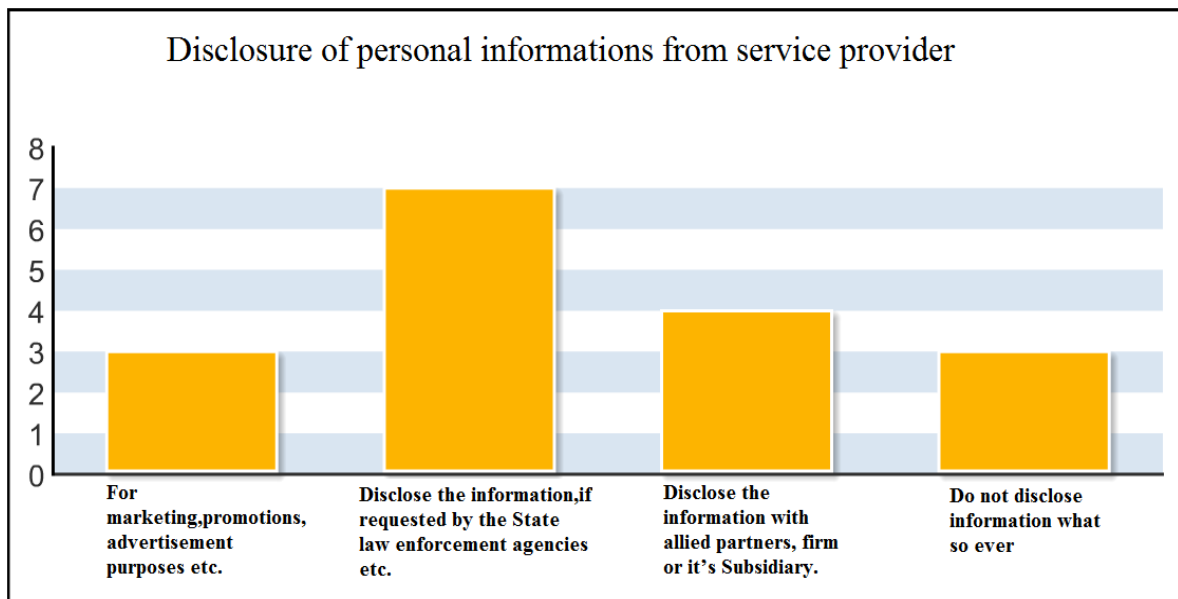


Figure: 5.5.8 Disclosure of personal information from service provider

The third research question that we have defined from the service providers perspective was;

RQ#6. When a policy is presented, what role can it play in framing trust of a common user?

We have mentioned in previous chapter it is necessary to find better mechanisms for privacy of users over the internet to achieve desired online business growth. There are lots of uncertainties and serious risks today concerning the users' privacy and trust. We have seen that users are sometimes compelled in circumstances to surrender their personal data to gain the services from the different organizations / service providers [2]. From our survey, we have found that many people void to give their personal security/ social security number and their date of birth

to their service provider because it might be lack of confidence and trust on these companies. We have asked in our questionnaire about the level of confidence to give their *e.g. social security number, date of birth, telephone, and address* in our survey.

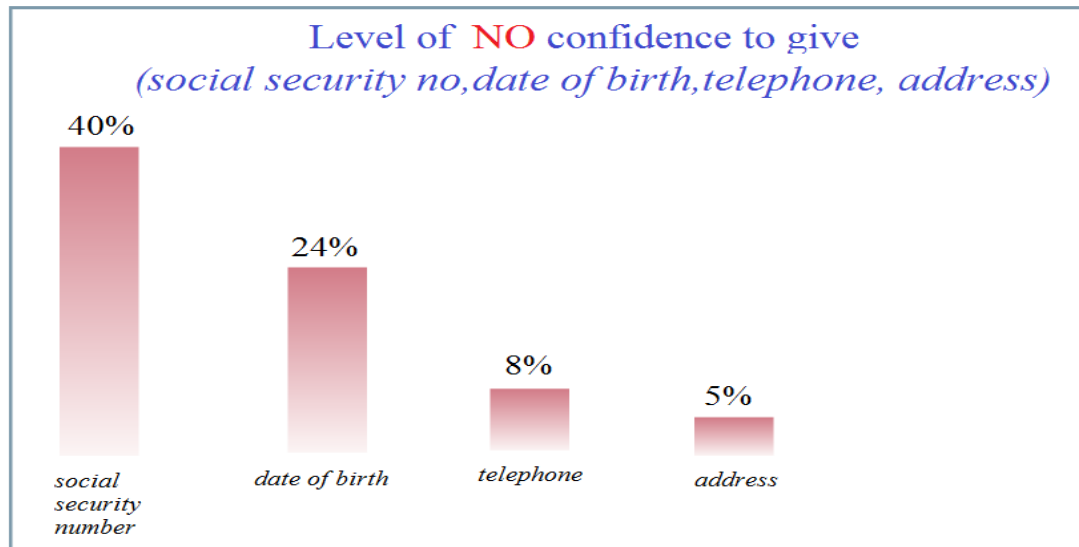


Figure: 5.5.9 Level of confidence from users

It could be good idea for common subscribers, when accepting policy, decisions with a higher importance are presented in a different manner (*e.g. with different font style, colors, images or may be with attractive web interfaces and templates etc*). We are probably entering into a new era that would require developing more effective policies for better and secure transmission of personal information. Furthermore, we have revealed from the survey that there are some policy violation reports coming from the users; so in that case, the service provider should be more focused to take proper protective measures for those violations.

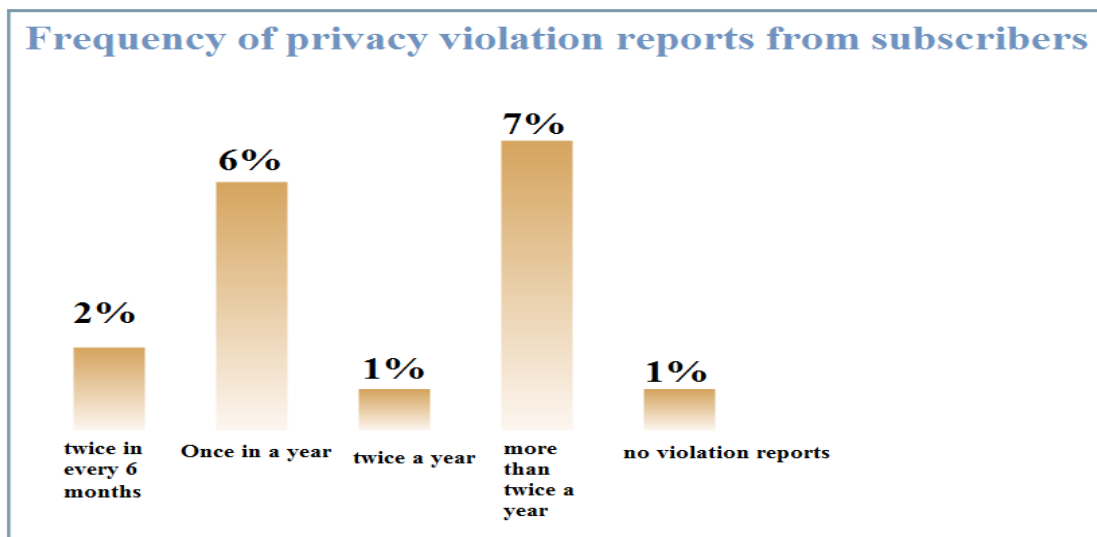


Figure: 5.5.10 Privacy violation reports from subscribers

We have asked in our survey about the privacy policy; how a service provider ensures the confidentiality of personal data and secured transmission of sensitive information over their website.

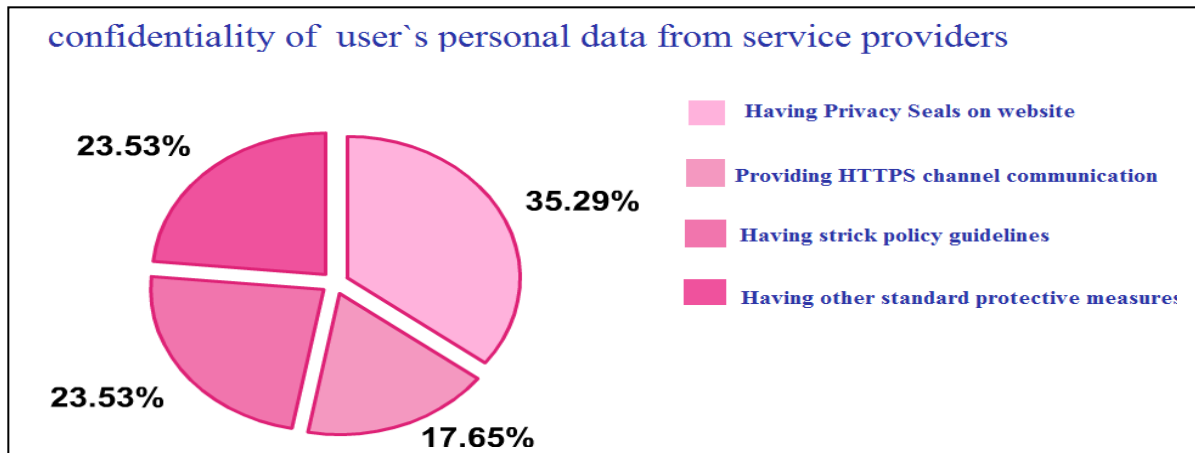


Figure: 5.5.11 Confidentiality of user personal data

We have received a positive response from the results that many service providers prefer to use different privacy seals on their websites to ensure secure data transmission. While others service provider gives importance for using https channel of communication. Some organizations use other standard protective measures etc, for framing the trust of the common users. Finally, we have to make a consensus for a one privacy policy contents to write domain specific policies, because it would very difficult to author the different protection mechanisms for different domains.

Chapter 6

Conclusion and Further work

This chapter is dedicated to give an executive summary of the present research work and discuss the validity of results. The chapter also identifies some possible further work on this topic. Finally, it outlines some research questions, which can be treated as directions for further studies and enhancements in this area.

6.1 Executive summary

Privacy issues have become increasingly important as the tail of information we leave behind us is rapidly growing and the potential misuse and theft of information is well recognized. To minimize the intrusion into a person's privacy caused by the collection, storage and use of the personal data, the field of data security and protection has emerged. An important and serious part of the data protection is to communicate the laws and regulations regarding the usage of the personal data of users, and the privacy policy serves as a path in this context. Privacy policies have the motivation of increasing the user's general confidence in sharing personal information, but most of the research has shown that they have failed to achieve this prospect. A very few users actually read the policies and understand them. Questions have been raised regarding whether they have any effect on the user's trust and confidence at all. Alternative ways of presenting privacy policy and its related regulations to the common users are urgently needed. To be able to propose an innovative approach to present the policy, one needs to explore the current status of the privacy policies and their related aspects. The purpose of this work has been to conduct a survey to lay a strong foundation for further work on the privacy policies and impact on the social and moral grounds. We therefore have conducted an explorative study and read related work on this topic in order to explore some relevant problem definitions. This work was followed by developing a questionnaire, and using a survey technique to answer these problems. We have conducted one survey for users and another

survey for the service providers. The results of both online surveys were unexpected, very few people actually read the policy, and try to understand them. We have also found an interesting fact that this was not due to a lack of privacy concern, but rather due to its complex terms, complicated language and user expectations. The importance of underlying a global patchwork of laws and regulation that serve as a basis for the content and structure of today's privacy policies was discussed in chapter 3 (*privacy legislation & principles*). In conducting this research we also saw that any innovative approach on presenting privacy policy to the user are limited by varying enforcement mechanisms, and that again tries to limit the further research on this important issue.

6.2 Validity and Limitations

We have mentioned in the research approach that this study has limitation related to the time frame and other constraints. The user surveys were based on high probability samples and thus statistically valid (we got response from 82 percent). For the service provider survey the probability sample was lower (response collected 17 out of 40). We have pointed at several possible sources for bias during discussion, and it is important to highlight yet again that the results from these online surveys should be regarded as highly explorative. Our findings are indication of subscriber's privacy concerns and attitude, and should not be understood as evidence. Our finding has also shown the attitude and perspective of different organizations and service providers about the phenomena of privacy policy and how they are treating the user's personal information. We have also tried to let the user know by both surveys that how service operators are liable on retention policy within the privacy contents, and how a company is responsible to handle the user's personal data when they are asking in their website. We have also highlighted the questions about to what extent a service operator thinks about the privacy statements presented to user are relevant for them. Possible sources for bias in these online surveys could stem from the age, education level etc of the respondents. It could have been very useful to conduct a similar and improved web survey based on a large number of participants, which could have opened for more in depth analysis about the topics included in the survey. A correlation analysis to map stated privacy practices to actual behavior could for example have been a useful approach to get wider understanding of the complex relation

between those two. However in the light of this project work, we feel that this size surveys has served its purpose, as an explorative approach to get an idea of the range of responses on ideas people have on the findings discovered in the literature review.

6.3 The road ahead

As seen from the survey evaluations, future approaches to alternative ways of presenting privacy policy are limited. While the idea of a unified policy and regulation on the topic of privacy and is unlikely to ever happen. The development of data protection laws throughout the globe is promising, and could create a better foundation of taking the user into confidence, and creating innovative ways of presenting privacy policies in the future. There have, however, emerged several interesting topics regarding privacy policies through this online web survey, and especially the different aspects that defines user confidence in sharing online information seems fruitful to base future research on. Further analysis in modifying the version of privacy seals could also be interesting to investigate further. Being a self-regulatory approach, the idea of how this approach could effectively work in the context of defined legislation can be a positive aspect for further study.

6.4 Potential research questions for further work

First, the policy makers would need to recognise that privacy and trust issues are both context dependent terms, which do not mean the same thing to all the users in all situations. Second, not all the users attach the same value to these concepts. Third, it is also a fact that for a specific domain, policies will be difficult to write, because some times within the same domain different circumstances may call for different privacy protections [7]. It is also very important to continue researching better tools and mechanisms for security and privacy policy makers, and to establish guidelines for better understanding as we learn more. Indeed the legislation, self-regulations, technical solutions and combination solutions are different ways that can be improved in establishing good mechanisms [10]. To achieve best security goals, it is crucial that policy makers are able to author high quality security polices and to ensure that the specified policy should match the intended policy. By analysing the different responses given by subscribers, we see that they are not aware about their personal information storage

technique and the assurance that their personal information is in safe hands. It is the responsibility of a services provider to notify the users, before they are trying to change the strategy of handling the personal information. If they do not take this initiative then it creates an ambiguity for a common subscriber and this affects the service provider reputation. This act of non-seriousness on privacy policy can be ended with big disasters because, if personal information has been disclosed locally, then there is a chance of harassing the user. There have, however, emerged several interesting topics and aspects regarding security policies through this research work. Especially the different aspects that define user trust and authentication in sharing the online information can provide better future research grounds.

We propose the following future research questions;

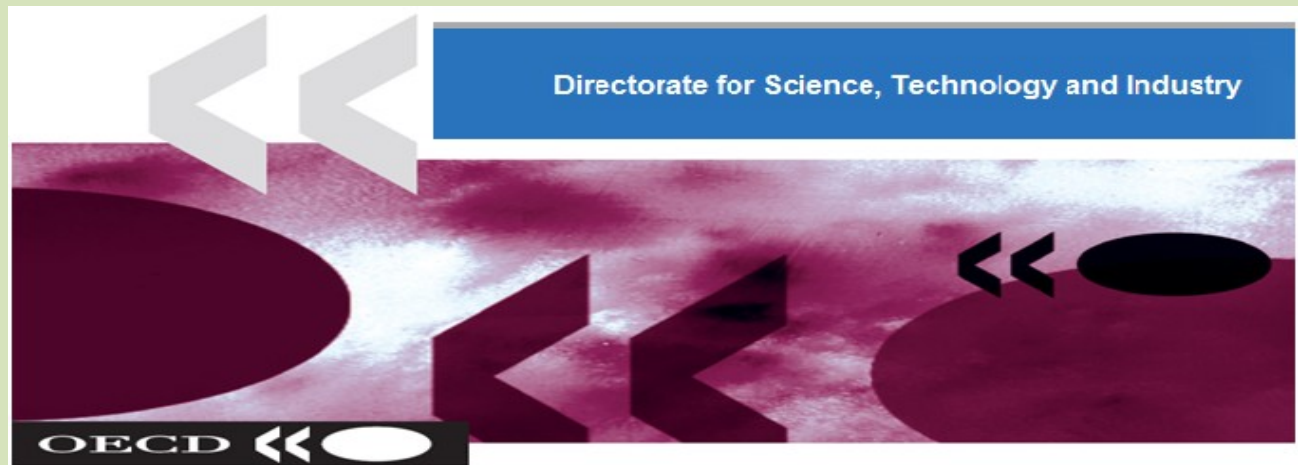
Question 1: How to improve the way the privacy policy is presented to the users by the service providers?

Question 2: To verify the perception that women are more sensitive towards their personal information as compared to men?

Question 3: How important are different webtrust seal programs in formation of trust on the users?

Finally, this can also be a good question for general discussion that policy authors are capable enough of authoring high quality policies if they know the risks and future threats (policy violation and ethical problems etc) [8].

Appendix A



The eight basic principles set out by the OECD Board are as follows;

1. **Collection Limitation Principle**

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data Quality Principle**

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **Purpose Specification Principle**

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation Principle**

Personal data should not be disclosed, made available or otherwise used for purposes except;

- 1) With the consent of the data subject.
- 2) By the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data.

7. Individual Participation Principle

An individual should have the right;

- To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- To have communicated to him, data relating to him within a reasonable time;
- To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Appendix B

Statement of purpose



✓ About the researcher:

Hello! My name is Murtaza Hussain and I am International Student here in NTNU. I am 26 years old and studying M.Sc in Department of Computer and Information Science (IDI) and my specialization is Information Systems Engineering, where I am focusing on perception of users and service provider privacy policies and their concerns. My supervisor is Professor Torbjørn Skramstad. This topic is assigned as a master to fulfil the requirement of M.Sc (Information Systems Engineering) in NTNU.

✓ Master`s Thesis Background:

Ambiguity in information society has raised many privacy and trust issues that are context dependent. These issues will pose many challenges for policy-makers and stakeholders because people's notion of privacy and trust are different and shifting. The policies of the past are not seems to be adequate to deal with new challenges and we are probably entering in new era that would require developing effective policies. In this work we have presented some responses' from users and service providers; indeed this work shows a limited scope due to the time limitation and other course work in this semester of my master degree, but this topic can be more elaborated in my future plans and research on the privacy policy phenomena. To be able to solve this task, I am dependent upon the questionnaires & online surveys from some service providers and Norwegian peoples. I specifically need to know what the common users response to accept the privacy policies, and before accepting a policy the by contents are fully read & understood by them. The questionnaire filling is entirely voluntary and to full the survey 3 reminder emails were sent to the stakeholders. All the information given in the questionnaires will be kept open for all times, and all the stake holders of these online questionnaires will be anonymous during the whole survey research. These questionnaires will be documented as a whole to ensure that they represent the users' and the service provider`s responses.

Prof. Torbjørn Skramstad
Supervisor IDI – NTNU.

Murtaza Hussain
Master`s student IDI –NTNU.

Appendix C

Questionnaires for the users (*total 15 questions*)

1. In which category your age belongs?

- 20-30 Years.
- 30 -40 Years.
- 40-50 Years.
- 50-60 Years.
- 60-70 Years.
- 70 years and above.

2. Your gender?

- Male.
- Female.

3. The highest level of education you have completed?

- High School.
- Completed Bachelor`s.
- Completed Master`s.
- Completed Doctorate.
- Completed Post-Doc.

4. In which category your status can best describe?

- Administrative / Management Level.
- Computer and Communication Industry/ Professional Level.
- Business / Commercial / Trade Level.
- Academia / College / University / Research Level.
- Media / Advertisement / Marketing Level.
- Intermediate / Student Level.
- Home / Common user Level.

5. Approximately how many working hours you spend on the internet?

- Below 10 hours per week.
- 10 -20 hours per week.
- 20-30 hours per week.
- 30-40 hours per week.
- 40-50 hours per week.
- More than 50 hours per week.

6. Are you familiar with the terminology of “*Privacy Policy*”?

- YES, I am aware.
- YES, But I am not sure what exactly this means.
- NO, I have not heard this before.

7. What is your perception about “*Privacy Policy*”?

- Privacy policy is just an ordinary text use to show the goodwill of organization.
- Privacy policy is a Law notice that tells about legal status of organization.
- Privacy policy just explains reliability and contact information of service provider.
- Privacy policy is a legal document that shows how service provider collects personal information and the usage of that information.

8. To what extent do you feel any advantage of having a complete privacy policy on service operator`s website?

- It helps to inform about the product and services.
- It helps to save from the Trojan attacks, spamming and virus threats etc.
- It helps to understand the process of collecting personal details from the user.
- There is no advantage of a privacy policy on service operator website.
- Other _____

9. To what extent do you feel any disadvantage of having a complete privacy policy on service operator's website?

- There is a great chance of phishing or harassing the user.
- User's personal information can easily be hacked or theft by a hacker.
- User would not know that what service provider is doing with his / her personal data.
- There is no disadvantage of a privacy policy on service operator website.
- Other _____

10. Before registering as a new subscriber with the website. Have you ever read the policy contents?

- YES, I have read them whenever I registered as a new subscriber.
- NO, I have not read them whenever I registered as a new subscriber.
- I have not ever tried to read the policy contents because I don't have time.

11. To what extent you feel difficulty in understanding the context of the privacy policies?

- YES, I feel very difficulty in understanding the context of the privacy policy.
- NO, I don't feel any difficulty in understanding the context of the privacy policy.
- I have not ever read and understand the privacy policy contents before using the services from the service provider.

12. To what extent do you feel that these policies are relevant for you as a subscriber?

- YES, they are very relevant for us.
- NO, they are not at all relevant.
- I don't have any idea about relevancy of policies.

13. To what extent are you confident to give your personal information (*e.g. date of birth, address, telephone, social security number etc*) to your service provider?

- | | |
|---------------------------------------------------------|---------------------------------------------------------|
| <input type="checkbox"/> YES for Social Security number | <input type="checkbox"/> NO, for Social Security number |
| <input type="checkbox"/> YES for Date of Birth | <input type="checkbox"/> NO, for Date of Birth |
| <input type="checkbox"/> YES for address | <input type="checkbox"/> NO, for address |
| <input type="checkbox"/> YES for Telephone | <input type="checkbox"/> NO, for Telephone |

14. To what extend are you aware, when ever your service provider amends the privacy policy?

- YES, I am aware when there are any changes/ amendment from the service provider.
- YES, But when some other user inform me about any changes/amendment from the service provider.
- NO, I am not aware about any changes / amendments from the service provider.

15. To what extend you send request to review or update your personal information from the service provider?

- Once in a week.
- Once in a month.
- Twice in a month.
- Once in every 6 month.
- Twice in every 6 month.
- Once a year.
- Twice a year.
- I have not ever sent any request to update or review my personal information.

THE END

Appendix D

Questionnaires for the Organization (*total 13 questions*)

1. In which category does your organization belongs?

- Internet organization.
- Telecommunication organization.
- Scientific / Research / Academia organization.
- Financial institution / Banking organization.
- Trade / Business/ Commerce organization.
- Marketing / Advertisement organization.
- Other _____

2. Does your organization operate inside the territory of Norway?

- YES, it is operate inside Norway.
- NO, it does not operate inside Norway.

3. Approximately how many the numbers of registered users are getting your service?

- Below 10,000 registered users.
- 10,000 – 40,000 registered users.
- 40,000 – 50,000 registered users.
- 50,000 – 1, 00000 registered users.
- 1, 00000 – 1, 50000 registered users.
- 15, 0000 – 2, 00000 registered users.
- 2, 00000 -250, 0000 registered users.
- More than 300, 0000 registered users.

4. To what extent does the organization gives importance on Privacy Policy?

- The organization gives STRONG importance.
- The organization gives AVERAGE importance.
- The organization gives LOW importance.
- The organization gives NO importance.

5. Does your organization follow any Privacy Standards and Law?

- NO, the organization do not follows a privacy standard and Law.

If “Yes” Identify them?

- Norwegian personal data Act of [2000]
- European Union personal data directive of [1995]
- Privacy safe harbor framework of [2000]
- OECD privacy principles of [2000]
- United States privacy Act of [1974]
- United States COPPA Act of [1999]
- Canada personal information protection & electronic documents Act of [2009]
- New Zealand data privacy Act of [1993]
- Australia data privacy law of [2008]
- Other _____

6. Approximately how many users read the organization`s privacy policy, before registering as a new user?

- Below 10 percent users.
- Approximately 10-30 percent users.
- Approximately 30- 60 percent users.
- Approximately 60-90 percent users.
- Above 90 percent users.

7. To what extent does an organization think that privacy statements presented to a registered subscriber are understandable?

- YES, because it determines the user`s operational limitation and domain company`s procedures.
- Some of contents of privacy policy deal with the legislation & regulations and that are not inconsideration for user.
- NO, it is not completely understandable for the users because it just explains terms of business, procedure and other unnecessary text etc.

8. Does an organization have a review body / committee on setting up privacy policies?

- No, the organization does not have any review body /committee on privacy policies.

If “Yes” how frequent does the policy contents are amended by review body/committee?

- It amends in every one month.
- It amends in every six month.
- It amends in every one year.
- It amends in every two years.
- It amends in more than two year.
- Other _____

9. Does the organization follow the retention regulation in their privacy policy?

- YES, the organization strictly follows the retention regulation in its privacy policy.
- YES, But sometimes but there is a pre-defined time frame to follow the retention regulation.
- NO, the organization does not follow any retention regulation.

10. Does the organization disclose the subscriber`s personal data to any 3rd vendor or 3rd parties?

- YES, it is the policy of the organization to disclose data to any organization for marketing, promotions, advertisement purposes etc.
- YES, it is the policy of the organization to disclose personal data, if the State / Country law enforcement agencies request.
- YES, it is the policy of the organization to disclose personal data with its allied partner, collaborated firm or it`s Subsidiary.
- NO, it is the policies of the organization not disclose personal data to any other organization what so ever.

11. How frequent does the service provider receive request from registered subscriber to update their personal details?

- Once in the month.
- Twice in a month.
- Once in every 6 months.
- Twice in every 6 months.
- Once in a year.
- Twice in a year.
- More than twice in a year.
- None of the above.
- Other _____

12. To what extent does the organization build a strong trust & confidence for a subscriber?

- By introducing the privacy protection seals on website.
- By providing the Https channel of communication in website.
- By following a stick policy statements and guidelines in website.
- Other standard protective measures taken up in website.
- Not necessary to build a trust and confidence for a subscriber in website.

13. How frequent does the service provider handle the privacy violation reports from the subscriber?

- Once in the month.
- Twice in a month.
- Once in every 6 months.
- Twice in every 6 months.
- Once in a year.
- Twice in a year.
- More than twice in a year.
- None of the above.
- Other _____

THE END

Glossary

In order to have a common understanding of a theme, it is good to have precise definitions of the terms used. This part provides a short list of the some commonly used terms in thesis.

Aggregate Information: The statistical information that may be collected by a web or other source, but is not personally identifiable.

Authentication: Process that establishes positive ID of a user, device, or other entity in a computer system.

Authorization: The process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system

Browser: A navigational program runs on a client's computer for viewing World Wide Web pages. An example includes Netscape & Microsoft's Internet Explorer.

Child: A child is identified, in accordance with the U.S. Children's Act of 1998 as under the age of thirteen.

Cookie: Small texts file of information that certain Web sites plant on a user's hard drive while the user is browsing the web site. A cookie can contain information such as user ID, user preferences, archive shopping cart information, etc. Cookies can contain personally Identifiable Information.

Compliance cost: A compliance cost is expenditure of time or money in conforming with government requirements such as legislation or regulation.

Data protection: The prevention of misuse of information stored on computers, particularly information about individual people.

Data inspectorate (*norske Datatilsynet*): A data inspectorate is a Norwegian Government agency responsible for managing the Personal Data Act of 2000, concerning privacy concerns.

Data quality: Acceptable standard of accuracy of personal data.

Data aggregation: The practice of collecting data from various sources and putting them together. In practice, data can be aggregated multiple times.

Data subject: The person whose personal data are collected, held or processed.

Data transfer: Data transfer refers to the transmission / communication of data to a recipient in whatever way it may be.

Data controller: The person or administrative entity that determines the purposes and means of the processing of personal data on behalf of an institution or body.

E-mail: Abbreviation for Electronic Mail. Messages sent from one person to another via computer.

Encryption: Scrambling data into a private code to ensure secure transmission.

Firewall: Specialized software and/or hardware designed to prohibit unauthorized access to information on a computer network.

Home Page: The first page of a web site. Also, the web site that automatically loads each time you launch your Browser.

Host: A computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services.

HTML: Abbreviation for Hypertext Markup Language, the World Wide Web's standard computer language.

Hyperlink: A hyperlink is a clickable link to another web page or site, a connection between two anchors. Clicking on one anchor will take you to the linked anchor.

Internet Protocol (IP) Address: The numbers that are translated into a domain name (*e.g. google.com*). The address is a string of four numbers separated by periods (*example, 111.22.3.444*) used to represent a computer or other device on the Internet.

Link: Another name for a hyperlink.

Log Files: A record of Web activity that automatically saves use and information such as the date, time, IP address, HTTP status, bytes sent, and bytes received.

Openness: The policy of openness about developments, practices and policies with respect to personal data.

Outweigh: It is a verb used with an object and it means to exceed in value, importance, influence, etc.

Opt-In: The option giving the consumer complete control over the collection and dissemination of his/her personal information. A site that provides this option is stating that it will not gather or track personally identifiable information about the consumer unless he/she knowingly provides such information and consents to the collection and use of such information. The company must have the consumer's permission prior to collecting or using the information.

Opt-Out: The option whereby consumer must actively chose to prevent personally identifiable information from being used by a particular Web site or shared with third parties. Typically, the consumer is asked to choose to Opt Out to prevent the Host from using his/her information.

Personally Identifiable Information (PII): Information that can be traced back to a specific individual user, e.g., name, postal address, e-mail address, telephone number, or Social Security number. Personal user preferences tracked by a Web site via a cookie are also considered personally identifiable when linked to other personally identifiable information provided by the user.

Privacy Officer: Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable privacy and security directives are implemented throughout the life cycle of an automated information system network.

Privacy Policy: The statement on a web site of what personal information is collected by the site, how it will be used, who it will be shared with, and what options there are for controlling how the information will be used.

Recurring informational/promotional E-mail: An E-mail sent from time to time to give individuals information or advise them of product offerings.

Sweepstake: sweepstakes is an advertising or promotional tactic through which incentive or prizes are given in order to participate an event by lucky draw etc.

Security policies: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Service provider: A service provider is an entity that provides services to other entities. Usually this refers to a business that provides subscription or web service to other businesses or individuals.

Subsidiary: A wholly controlled part of the company.

Service operators: A service operator (SO) is also known as a mobile phone operator that provides carrier service, wireless service or cellular signals to subscribers.

Third Party: A natural or legal person, public authority, agency or body, other than the data subject, the controller, the processor and the persons who, under the direct authority of controller or processor are authorized to process the data.

Trace: The path revealing an end user movement over the internet.

Untraceability: Untraceability aims at making it difficult for the adversary to identify that a given set of actions were performed by the same subject.

Undetectability: Undetectability of an item of interest from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.

URL: Uniform Resource Locator, the address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the domain name where the resource is located.

Web Bug: A small image in an HTML page with all dimensions. Because of its insignificant size, it is not visible but it is used to pass information anonymously to third party sites.

Webmaster: The person responsible for maintaining and updating a web site.

Web site: A collection of pages or files on the World Wide Web that are linked together and maintained by a company, organization, or individual.

Bibliography

- [1] Warren, Samuel and Louis D.Brandeis, "*The Right to Privacy*", Harvard Law Review Association. Vol.IV, No: 5.
- [2] David.W, Serge. G, Michael. F,(2009) "*Privacy, trust and policy-making: Challenges & Responses* ", Computer Law & Security Review 25- 2009. Elsevier Ltd Publication. Vol, 69-83.
- [3] Wham., T (2001) "*Transcript of the Federal Trade Commission USA Workshop on Information Privacy. Measuring individuals Concerns about Organization Practices*". Available online at <http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm>
- [4] Karat, J., Karat, C.-M., Brodie, C., Feng, J (2005)" *Privacy in information technology: Designing to enable privacy policy management in organizations*". International Journal of Human-Computer Studies (2005)
- [5]Cao, X., Iverson, L: Intentional access management: "*Making access control usable for End-users*". In: Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS 2006), New York, NY, pp. 20–31. ACM Press, New York (2006)
- [6] C.Brodie, C.M.Karat, J.Karat and J.Feng. Usable Security and Privacy: "*A case study of Developing privacy management tools*". In SOUPS `05: proceeding of the 2005 Symposium on usable privacy and security ACM, New York, 2006.
- [7] Kelley,P.G., Bresee,J., Cranor,L. F., and Reeser,R.W (2009)"*A nutrition label for Privacy*". In proceedings of the 5th Symposium on usable privacy and security SOUPS 09-2009. Available online at <http://www.portal.acm.org/citation.cfm?doid=1572532> [accessed on May 27th, 2010]
- [8] S. E. Schecter(2004) "*Computer Security Strength & Risks: A Quantitative Approach*". PhD- Thesis, Harvard Unviersity, Cambridge, Massachusetts, May-2004.
- [9] Culnan,M.(1993) "*How did they get my name? An Exploratory Investigation of Consumer Attitudes towards Secondary Information Use*". MIS Quarterly, 17(3), 341.
- [10] Chung.W,Paynter.J (2002) "*Privacy Issues on the Internet*", 35th Hawaii International Conference on System Sciences, USA 2002.
-

-
- [11] James Waldo, Herbert Lin, Lynette I. Millett (2007) " *Engaging privacy and information Technology in a digital age*". National Academies Press. Washington DC USA.
- [12] United states Federal Trade Commission. *Federal Trade Commission (FTC) (1999 yearly report)*. Available online at <http://www.ftc.gov.us> . USA
- [13] Wikipedia the Free Encyclopedia " *Privacy Policy*" URL <http://www.wikipedia.org>
Available online & accessed on Spetember, 26th, 2010.
- [14] Answers.com: Internet Privacy: URL <http://www.answers.com>
[accessed on September 26th , 2010].
- [15] Slane,B(2000)." *Killing the goose? Information Privacy issues on the web*". Available online
At <http://privacy.org.nz/media/killgoos.html>
- [16] Hancock,W.(1997) " *Cookies on your hard-drive*". American Agent & Broker.69 (6):
8-10. June 1997, USA
- [17] Krauss,M.(2000) " *Don't kid yourself-consumers do pay attention to privacy*". Marketing
News.34 (5); 13.February 28th ,2000 USA
- [18] TrustE (2001). Available online at <http://www.truste.org>
- [19] Matt Bishop (2002) " *Computer security: art and science.*" Addison-Wesley Professional
Publication December12th, 2002, USA
- [20] Gary,S, Alice.G, Alexis.F, NIST (2002)" *Risk Management Guide for Information
Technology Systems*" .NIST Special Publication, July 2002. USA
- [21] Wikipedia the Free Encyclopedia " *Security Policies*" .Available online at
<http://www.wikipedia.org> [accessed on September 26th, 2010].
- [22]Oates.B.J (2006) " *Researching Information Systems and Computing*", Saga publications,
London, United Kingdom 2006.
- [23] Brehm J. (1993) " *The Phantom Respondents*". Ann Arbor: University of Michigan.
Press. USA 1993.
- [24] Francis J.D, Busch L (1975) " *What we don't know about "I don't knows*", Public Opinion.
Q. 34:207-18. 1975, USA
-

-
- [25] Cronbach L.J (1950) "*Further evidence on response sets and test design*". Educational Psychology. 10:3-31. USA
- [26] Fonda C.P, (1951) "*The nature and meaning of the Rorschach white space response*". J. Abnorm. Social Psychology. 46:367- 77. USA
- [27] Mark Kasunic (2005) "*Designing an Effective Survey* ", Carnegie Mellon University. September 2005. USA
- [28] Backstrom, C. H., Hursh-César,. G (1981) "*Survey Research*", 2nd Ed. New York, NY: Macmillan Publishing Company, USA
- [29] Yuji Sato (2003), "*Questionnaire Design for survey Research: Employing Weighting Method*", July -2003 .Honolulu, Hawaii, USA
- [30] karahasanovic, A.; Brandtzeag,P.;Vanattenhoven,J;Lievens,B.;Nielsen,K; and Pierson,J.(2009) "*Ensuring Trust, Privacy and Etiquette in web 2.0 Application* ". Computer, 42(6):42-49.
- [31] McDonald, A. and Cranor, L. (2009) "*The agenda setting function of mass media*". Public opinion quarterly, 36(2):176.
- [32] NCJA (2002) "*Report by justice information privacy guideline*". Available online at [http://www.ncja.org/ Content/NavigationMenu/ PoliciesPractices/ JusitceInformation privacyGuideline/PrivacyGuideline.pdf](http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusitceInformationprivacyGuideline/PrivacyGuideline.pdf) [accessed on May 26th , 2010].
- [33] Gellman.R (2010) "*Fair Information Practices. Brief History*". Available online at <http://www.tardis.ed.ac.uk/simkate/qmcweb/scont.htm> [accessed on June 7th, 2010].
- [34] Organization for Economic Cooperation and Development (OECD) (1980) "*OECD Guidelines on the Protection of Privacy and Trans-border flows of Personal Data*". Available online at http://www.oecd.org/pages/0,3417,en_3673052_1_privacy.html [accessed on June 7th , 2010].
- [35] Organization for Economic Cooperation and Development (OECD) (2010) "*About the Organization for Economic Cooperation and Development OECD Guidelines*". Available online at http://www.oecd.org/pages/0,3417,en_3673052_1_privacy.htm [accessed on June 7th , 2010].
-

-
- [36] Carron,C. (2009) " *Privacy Laws and regulations around the Globe. The impact of doing business Internationally*". Available online at <http://www.thefreelibrary.com/Privacy%20lawsand%20Regulations%20Around%20the%20Globe%20The20%Impact%20on%20Business/a0211183336.htm> [accessed on June 7th, 2010].
- [37] Wang,Y and Kobsa,A (2008) "*Privacy-Enhancing Technologies*", pages 352-375.Idea Group Inc (IGI). USA
- [38] Schartum, D. W. and Bygrave, L. A. (2004)" *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger*", Fagbokforlaget, Norway.
- [39] Fischer-Hübner, S. (2001)" *IT-Security and Privacy*", Springer-Verlag, Berlin, Germany.
- [40] HRL (2001) Act of 18 May 2001 on "*Personal Data Filing Systems and the Processing of Personal Health Data*", Vol. LOV-2001-05-18-24.
- [41] The Norwegian Personal Data Act POL (2000)"*Lov om behandling av personopplysninger*" Vol. LOV-2000-04-14-31 Norway.
- [42] EUDPD (1995) " *The EU directive on the protection of individuals with regard to the Processing of personal data and on the free movement of such data*". Vol. 95/46/EC.
- [43] United States of America Privacy Act of 1974. Available online at: http://www.usaid.gov/policy/egov/pa_1974.pdf [accessed on February 9th, 2011].
- [44] The Data Protection Act 1998. Available online at <http://www.dataprotectionact.org/index.html> [accessed on February 10th, 2011].
- [45] National Export Initiative US Government. Available online at http://www.export.gov/about/eg_main_016803.asp [accessed on February 10th, 2011].
- [46] Van Blarkom, G. W., Borking, J. J. and Olk, J. G. E. (2003)" *Handbook of Privacy and Privacy-Enhancing Technologies - The Case of Intelligent Software Agents*", Colledge Besherming persoongegevens, Haag.
- [47] Hoofnagle,C (2005)" *Privacy self regulation: A decade of disappointment* ". Available online at <http://epic.org/reports/decadedisappoint.html> [accessed on February 11th, 2011].
-

-
- [48] United States Government. Federal Trade Commission (FTC) (2009 yearly report). Available online at <http://www.ftc.gov.us> USA.
- [49] Children's Online Privacy Protection Act (COPPA 1999). Available online at <http://www.coppa.org/coppa.htm> [accessed on February 11th, 2011].
- [50] United States Government. Federal Trade Commission (FTC) (2008 yearly report). Available online at <http://www.ftc.gov.us> . USA.
- [51] United States department of Commerce (2010) "*International safe harbor privacy Principles overview*". Export.gov.us .Available online at http://www.export.gov/Safeharbor/eg_main_018236.asp [accessed on June 26th, 2010].
- [52] Simth., H. Milberg,S., Burke,S (1996)"*Information privacy. Measuring individuals concerns about organization practice.*" MIS Quarterly, 20(2): 167-196.
- [53] Harris Interactive (2001)"*Identity Theft: New Survey & Trend Report*". Available online at <http://identitytheft.lifetips.com/cat/65329/identity-theft-statistics/index.html>.
- [54] Milne,M.J (2001)" *The Culnan-Milne Survey on consumers & online privacy notices: Summary of Responses*". In Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices, Pages 47-54.
- [55] Anton, A., Earp,J., He , Q., Stufflebeam, W., Blochini , D., and Jensen, C. (2004) "*Financial privacy policies and the need for Standardization*". IEEE Security & privacy, 2(2):36-45.
- [56] Bonneau,J. and Preibusch,S. (2009) "*The privacy jungle: On the market for data protection in social networks*". In the Eight Workshop on the Economics of Information Security (WEIS-2009).
- [57] Jensen,C. Potts,C. (2004) "*Privacy policies as decision-making tools. An evaluation of online privacy notices*". In proceedings SIGCHI conference on Human factor in computing systems ACM .Pages 471-478.
- [58] Bolchini,D., He,Q., Anton A.L ,Stufflebeam,W.H (2004) "*I need it now ! Improving Websites usability by contextualization privacy policies*". In ICWE, pages 31-44.
-

-
- [59] Earp,J.,Anton,A. Aiman Simth,L., Stufflebeam,W (2005) " *Examining Internet privacy policies within the context of user privacy values* ". IEEE Transaction on Engineering Management, 52 (2):227-237.
- [60] Pollaach,L.(2007)" *What`s wrong with online privacy policies?*". Communication of ACM. 50(9):108.
- [61] Stufflebeam,W., Anton.A, He,Q., and Jain,N (2004) " *Specifying privacy policies with P3P and EPAL: Lessons Learned*". The ACM Workshop on Privacy.
- [62] Kleimann Communication Group (2006) " *Evolution of a Prototype Financial Privacy Notice*". Available online at <http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf> [accessed on August 8th , 2010].
- [63] Cranor,L., Guduru,P., and Arjula,M(2006)" *User interfaces for privacy agents*". ACM Transactions on Computer-Human Interaction (TOCHI), 13(2):178.
- [64] Mayer,R., Davis,J., and Schoorman, F (1995) " *An integrative model of organization trust*". Academy of management review. Available online at <http://www.jstor.org/stable/258792> [accessed on February 14th, 2011].
- [65] Metzger,M. (2004)" *Privacy, trust and disclosure: Exploring barriers to electronic Commerce*". Journal of Computer Mediated Communication. Available online at <http://www.jcmc.indiana.edu/vol19/issue4/metzger/html> [accessed on Feb 14th, 2011].
- [66] Kolsaker, A., Payne (2002)" *Engendering trust in e-commerce. A study of gender based concerns*". Marketing Intelligence and Planning.
- [67] Miyazaki,A. Fernandez,A (2000) " *Internet privacy and security. An examination of online retailer disclosures*". Journal of Public Policy & Marketing.
- [68] CDATA Jarvenpaa,S., Tractinsky,N., Saarinen.L., and Vitale,M. (1999) " *Consumer trust in an Internet store. A cross cultural validation*". Journal of Computer mediated Communication, 5(2):1-35.
- [69] Meinert,D., Peterson,D., Criswell,J., Crossland,M (2006)" *privacy policy statements and consumer willingness to provide personal information*". Journal of Electronic Commerce in Organizations. 4:1-17.
-

-
- [70] Gideon,J.,Cranor,L.,Egelman,S., Acquisti,A (2006) "*Power strips, prophylactics and privacy*".In proceedings of the second symposium on Usable privacy and Security. ACM.
- [71] Harris Interactive (2003)"*Identify Theft*". New Survey & Trend Report.
- [72] Awad,N., Krishnan,M (2006) "*The personalization privacy paradox. An empirical evaluation of information transparency and the willingness to be profiled online for personalization*". MIS Quarterly, 30(1):13-28.
- [73] Spiekermann,S., Grossklags,J., Berendt,B (2001)"*E-privacy in 2nd generation E-commerce*". In proceedings of ACM conference on Electronic Commerce-EC 01, Pages 38-47.
- [74] Leathern,R. (2002) "*FTC Security Workshop. Security and privacy data*". Available online at <http://www.ftc.gov/bcp/workshops/security/020520Leathern.pfd> [accessed on September 27th , 2010].
- [75] Milne,G., Culnan,M.J (2004) "*Strategies for reducing online privacy risks. Why consumers read, online privacy notices*". Journal of Interactive Marketing, 18(3).
- [76] Belanger,F., Hiller,J., Smith,W (2002) "*Trustworthiness in electronic commerce. The role of privacy, security and site attributes*". The journal of strategic Information Systems, 11 (3-4):245-270.
- [77] Cranor,L.,Reagle,J., Ackerman,M (2000) "*Beyond concern. Understanding net user`s attitudes about online privacy*".The internet Upheaval: Raising Questions, seeking Answers in Communication Policy, Pages 47-70.
- [78] Ackerman,M.,Cranor,L., Reagle,J (1999) "*Privacy in E-Commerce. Examining User scenarios and privacy preferences*". In Proceedings of 1st ACM Conference on E-Commerce ACM, Page 8.
- [79] McCombs,M., Shaw,D (1972) "*The agenda setting function of mass media*". Public opinion Quarterly, 36 (2):176.
- [80] Iarossi, G. (2006)"*The Power of Survey Design: A User's Guide for Managing Surveys, Interpreting Results and Influencing Respondents*". Washington, D.C. The World Bank, USA.
-

-
- [81] Moser, C.A. & G. Kalton. (1971) " *Survey Methods in Social Investigations*". London: Heinemann Educational Book Limited. UK
- [82] Survey-Monkey. (2009) " *Response Rates & Surveying Techniques: Tips to Enhance Survey Respondent Participation*". Available online at: http://www.amazonaws.com/SurveyMonkeyFiles/Response_rates.pdf [accessed on February 17th, 2011].
- [83] Brace, I. (2004) " *Questionnaire Design: How to Plan, Structure and Write Survey Material for Effective Market Research*". London: Market Research in Practice Series.UK
- [84] Yun, G.W., C.W. Trumbo (2000)" *Comparative Response to a Survey Executed by Post, E-mail and Web Form*". Journal of Computer Mediated Communications 6(2).
- [85] University of Texas at Austin USA (2007)" *Instructional Assessment Resources*". Available online at <http://www.utexas.edu/academic/ctl/assessment/iar/teaching/gather/method/survey-Response.php?task=research> [accessed on February 4th, 2011].
- [86] Creech, S.,(2007) " *Sample Size*". From Statistical Consultant for Doctoral Students and Researchers. Available online at <http://www.statisticallysignificantconsulting.com/Sample-Size-Help.htm> [accessed on February 19th, 2011].
- [87] Jon A. Krosnick (1999) " *SURVEY RESEARCH* ", Annu. Rev. Psychol. 1999. 50:537–67.
- [88] Book rages (*Famous Quotes by Benjamin Franklin*). Available online at http://www.bookrags.com/quotes/Benjamin_Franklin [accessed on March 3rd, 2011].
- [89] Piero A., Juri L., Daniel O., Luigi S.,(2007) " *Rule-based policy representations and reasoning*". Springer.USA.
- [90] Shaikh M., (2011)" *Analyzing the Privacy Policy: Responses and Challenges* ".TDT4520-Information Systems Specialization Project. Norwegian University of Science and Technology (NTNU), Trondheim - Norway.
-