



**NTNU – Trondheim**  
Norwegian University of  
Science and Technology

# User Interface Design for Privacy Enhancing Technology

**Nina Ripmann**

Master of Science in Communication Technology

Submission date: June 2012

Supervisor: Svein Johan Knapskog, ITEM

Co-supervisor: Karin Bernsmed, SINTEF ICT

Norwegian University of Science and Technology  
Department of Telematics



# Problem Description

**Name of student:** Nina Ripmann

Protecting your privacy has become increasingly difficult, as more and more personal information is shared through the use of social networks, mobile applications and location based services. While there are some implementations of privacy enhancing technology to protect personal information, we have yet to see widespread adoption by end-users.

SINTEF ICT is currently investigating new approaches to privacy protection of end-users. They have implemented a prototype Privacy Enhancing Technology (PET) that aims to learn the user's privacy preferences and to help by giving users advice on how to behave in different privacy contexts. The software is intended to run on for example a laptop or a smartphone.

For this project I will suggest a design for a graphical user interface for the PET, test it on users and evaluate it. The focus of the assignment will be on usability testing and evaluating the Graphical User Interface (GUI) based on the feedback from the tests and the systems learning process. A key aspect will be to find the right level of user involvement and what the interaction between the user and the system should consist of for further improvements of the system.

**Assignment given:** 13. Jan 2012

**Responsible Professor:** Svein J. Knapskog, ITEM

**Supervisor:** Karin Bernsmed, SINTEF ICT



# Sammendrag

En betydelig mengde informasjon er tilgjengelig om oss online på grunn av økt bruk av Internett og bruk av tjenester på nett. Det har blitt en tendens blant brukere å ikke lese nettsiders retningslinjer for personvern når man oppretter brukerkontoer, fordi de er kjent for å være lange og kompliserte dokumenter som er vanskelig å forstå. Brukerne føler også ofte at de egentlig ikke har noe annet valg enn å godta retningslinjene hvis de vil bruke tjenestene. Dette har skapt bekymringer for personvernet og et behov for bedre personvernkontroll siden brukerne egentlig ikke vet hva slags retningslinjer de har godtatt.

SINTEF IKT har utviklet et personvernsprogram kalt Privacy Advisor hvis hensikt er å hjelpe brukerne å tenke på personvern og deling av informasjon på Internett. Dette gjøres ved at programmet tolker nettsiders retningslinjer for brukerne og gi dem råd om hvorvidt nettsiden burde stoles på eller ikke. Brukerne blir da gitt muligheten til å gi tilbakemelding til Privacy Advisor om avgjørelsen sin og Privacy Advisor vil da tilpasse seg til brukerens preferanser til personvern.

Et grafisk brukergrensesnitt (GUI) ble utviklet til Privacy Advisor ved å benytte prototyping med iterativ forbedring av designet, basert på tilbakemeldinger fra SINTEF IKT og potensielle brukere. Tilbakemelding fra brukere ble samlet inn ved å utføre brukbarhetstesting med observasjon etterfulgt av et spørreskjema. Brukbarhetstesting ble også gjennomført for å bestemme designets brukbarhet og finne ”breakdowns” eller problemer i designet.

Tilbakemeldingene viste at det var noen problemer i designet. Disse var typisk presentasjon av tekst som var forvirrende for brukerne hvor de ikke skjønnte betydningen av teksten, eller knapper som ikke var intuitive nok. Disse ble fikset til det endelige designforslaget.

Brukerne navigerte også godt i prototypen og klarte å fullføre oppgavene de ble gitt. Systemet mottok også en del positive tilbakemeldinger om bruken og behovet av et slikt program, og på grunn av disse elementene er brukbarheten til systemet vurdert som god når de siste problemene i designet ble fikset.

Et endelig design for Privacy Advisor, implementert som en Google Chrome extension for Privacy Advisor ble så presentert for SINTEF IKT.



# Abstract

A significant amount of information is available of us online due to the increased use of the Internet and online services. It appears to be a tendency among users to not read privacy policies when creating user accounts online because policies are known to be long and complicated documents that are hard to understand. Users also feel like they don't really have a choice than to accept the policy if they want to use the service. This have created privacy concerns and a need for better privacy control for users, since the users usually don't know what they have agreed to when accepting policies.

SINTEF ICT have developed a Privacy Enhancing Technology (PET), named Privacy Advisor, whose purpose is to help users think about privacy and information sharing online. This is done by Privacy Advisor interpreting webpages privacy policies for the users and giving advices on whether the webpages should be trusted or not. The users are then given the opportunity to provide feedback to Privacy Advisor and the system will use this to adapt to the users privacy preferences.

A Graphical User Interface (GUI) for Privacy Advisor were developed using prototyping with iterative improvement of the design, based on feedback from SINTEF ICT and potential users. Feedback from users was collected by performing usability testing with observation, followed by a questionnaire. Usability testing was also conducted to determine the designs usability and find breakdowns in the design.

The feedback showed that there were some breakdowns in the system. These were presentation of text that was confusing for some users, where they did not understand the meaning of the text, or buttons that was not intuitive enough. These breakdowns were fixed for the final version of the design suggestion.

The users also navigated well in the prototype and managed to complete all the given tasks. The system also received positive feedback concerning further use and the need for a program like Privacy Advisor, and because of these elements, the usability were determined as good when the final improvements and fixing of breakdowns were completed. A final design for Privacy Advisor, implemented as a Google Chrome extension was then presented to SINTEF ICT.





# Preface

This thesis is the final product of my master's degree in Communication Technology, with Specialization in Information Security. The work has been carried out in the spring of 2012, at the Department of Telematics (ITEM), Norwegian University of Science and Technology (NTNU), Norway.

The assignment was proposed by SINTEF ICT and is a continuation of a project that started in SINTEF ICT in 2010 and was continued by students in the course TDT4290 - Customer Driven Project in the fall of 2011.

I would like to take this opportunity to express gratitude to my supervisor, Karin Bernsmed from SINTEF, for the guidance I have received throughout the work with this thesis. She has, since the beginning provided me with help, advices and feedback on my work and it is very much appreciated. Also, a great thank you to my professor Svein J. Knapskog for valuable input and constructive feedback on my work.

I also want to thank the people that helped me by participating in the usability tests and thus providing me with important data to work with.

Finally i want to thank my friends and family for support and my fellow students for five wonderful years at NTNU. A special thanks to Julianne, Maja, Silje, Line and Hanne who I have shared office with the last year and that has provided me with much motivation and many good memories.

June 7, 2012

Nina Ripmann



# Contents

<b>Sammendrag</b>	<b>i</b>
<b>Abstract</b>	<b>iii</b>
<b>Preface</b>	<b>v</b>
<b>Contents</b>	<b>vii</b>
<b>List of Figures</b>	<b>xiii</b>
<b>Acronyms and Abbreviations</b>	<b>xv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Background . . . . .	2
1.2.1 SINTEF ICT . . . . .	2
1.2.2 Privacy Advisor . . . . .	3
1.3 Problem Definition . . . . .	3
1.3.1 Contribution . . . . .	3
1.4 Existing Privacy Tools . . . . .	4
1.4.1 Privacy Bird . . . . .	4
1.4.2 Privacy Finder . . . . .	5
1.4.3 Ghostery . . . . .	5
1.4.4 Tor . . . . .	5
1.5 Completion of the Thesis . . . . .	6
1.5.1 Design Phase . . . . .	6
1.5.2 Testing Phase . . . . .	7
1.5.3 Evaluation Phase . . . . .	7
1.6 Outline . . . . .	7
<b>2 Theoretical Background</b>	<b>9</b>
2.1 Privacy . . . . .	9
2.1.1 Internet Privacy . . . . .	10

2.1.2	Privacy Concerns . . . . .	10
2.2	Privacy Policies . . . . .	11
2.2.1	P3P . . . . .	11
2.2.2	Other Standards for Privacy Representation . . . . .	12
2.3	Machine Learning . . . . .	13
2.3.1	Case Based Reasoning . . . . .	13
2.3.2	k-Nearest Neighbor Algorithm . . . . .	14
2.4	Human Computer Interaction . . . . .	15
2.4.1	User Interfaces . . . . .	15
2.5	Design Principles . . . . .	16
2.5.1	Usability . . . . .	16
2.5.2	Affordance and Constraints . . . . .	17
2.5.3	Ten Usability Heuristics . . . . .	17
2.5.4	KISS Principle . . . . .	18
<b>3</b>	<b>Methodology</b>	<b>19</b>
3.1	Methodology in Academic Work . . . . .	19
3.1.1	Qualitative and Quantitative methods . . . . .	19
3.2	Literature Review . . . . .	20
3.3	Design and Development methods . . . . .	20
3.3.1	Prototyping . . . . .	22
3.4	Testing the Design . . . . .	23
3.4.1	Usability Testing . . . . .	23
3.4.2	Observation . . . . .	24
3.4.3	Questionnaires . . . . .	24
3.5	Evaluation of Data . . . . .	25
3.5.1	Evaluating Quantitative Data . . . . .	26
3.5.2	Evaluating Qualitative Data . . . . .	26
<b>4</b>	<b>System Description</b>	<b>29</b>
4.1	Privacy Advisor . . . . .	29
4.2	The Advice Engine . . . . .	30
4.2.1	Finding Similar Cases . . . . .	30
4.2.2	Conclusion Algorithm . . . . .	31
4.3	Existing User Interfaces . . . . .	32
4.3.1	Command Line Interface . . . . .	32
4.3.2	Graphical User Interface . . . . .	33

---

<b>5</b>	<b>User Interface Design</b>	<b>35</b>
5.1	Browser Extension . . . . .	35
5.1.1	Google Chrome Extension . . . . .	35
5.1.2	Realizing an Extension . . . . .	36
5.2	User Scenarios . . . . .	36
5.2.1	Scenario 1 - Secure Online Surfing . . . . .	36
5.2.2	Scenario 2 - Unsecure Online Surfing . . . . .	37
5.2.3	Scenario 3 - Exploring Additional Functionality . . . . .	37
5.3	The Prototypes . . . . .	37
5.3.1	The First Prototype . . . . .	38
5.3.2	The Second Prototype . . . . .	38
5.4	The Design . . . . .	39
5.4.1	Main Menu . . . . .	40
5.4.2	Advices From Privacy Advisor . . . . .	40
5.4.3	Information . . . . .	42
5.4.4	Settings . . . . .	43
5.4.5	History . . . . .	43
5.4.6	Design Expansion . . . . .	44
5.5	Use of Design Principles . . . . .	44
5.5.1	Visibility of System Status . . . . .	45
5.5.2	Match With the Real World . . . . .	45
5.5.3	User Control and Freedom . . . . .	46
5.5.4	Consistency and Standards . . . . .	46
5.5.5	Error Prevention . . . . .	46
5.5.6	Recognition Rather than Recall . . . . .	46
5.5.7	Flexibility and Efficiency of Use . . . . .	46
5.5.8	Aesthetic and Minimalistic Design . . . . .	47
5.5.9	Recognize, Diagnose and Recover . . . . .	47
5.5.10	Help and Documentation . . . . .	47
<b>6</b>	<b>Usability Testing</b>	<b>49</b>
6.1	Test Plan . . . . .	49
6.1.1	Test Goals . . . . .	49
6.1.2	Test Subjects . . . . .	50
6.1.3	Test Introduction . . . . .	50
6.1.4	Execution . . . . .	50
6.1.5	Test Observations . . . . .	51
6.2	Testing . . . . .	51
6.2.1	The Pilot Test . . . . .	51

6.2.2	Usability Test Results . . . . .	52
6.3	Results from the Questionnaire . . . . .	54
6.3.1	User Statistics . . . . .	54
6.3.2	System Related Feedback . . . . .	55
6.3.3	Privacy Related Feedback . . . . .	58
<b>7</b>	<b>Evaluation and Discussion</b>	<b>61</b>
7.1	Test Results . . . . .	61
7.1.1	Functioning Design Elements . . . . .	61
7.1.2	Further GUI Improvements . . . . .	62
7.1.3	Information to Users . . . . .	64
7.1.4	The System's Learning Process . . . . .	65
7.2	The System's Usability . . . . .	65
7.2.1	Effectiveness . . . . .	66
7.2.2	Efficiency . . . . .	67
7.2.3	Satisfaction . . . . .	67
7.3	Validity of the Tests . . . . .	68
7.3.1	Selection of Participants . . . . .	68
7.3.2	Validity of the Results . . . . .	68
7.3.3	Tasks and Questions . . . . .	69
<b>8</b>	<b>Future Work</b>	<b>71</b>
8.1	System Improvements . . . . .	71
8.1.1	Additional Features . . . . .	71
8.1.2	GUI Improvements . . . . .	72
8.2	A Fully Functional Extension . . . . .	72
8.3	Support for Other Standards . . . . .	72
8.4	Additional Security Functionality . . . . .	73
8.4.1	Delete Cookies . . . . .	73
8.4.2	Erase History and Temporary Files . . . . .	73
8.4.3	Malware Scanning . . . . .	74
<b>9</b>	<b>Conclusion</b>	<b>75</b>
	<b>References</b>	<b>77</b>
<b>A</b>	<b>Testing Documents</b>	<b>81</b>
A.1	Tasks for Usability Testing . . . . .	81
A.2	Questionnaire . . . . .	82

<b>B Detailed Design</b>	<b>87</b>
B.1 The Google Chrome Extension . . . . .	87
B.2 Manifest . . . . .	87
B.3 Background Pages . . . . .	88
B.4 HTML Pages . . . . .	89
B.5 The CSS . . . . .	100
<b>C Running the Extension</b>	<b>103</b>
C.1 Installation and Execution . . . . .	103





# List of Figures

1.1	Privacy Bird . . . . .	4
1.2	Privacy Finder . . . . .	5
1.3	Ghostery. . . . .	6
2.1	Case based reasoning . . . . .	14
3.1	User-centered design . . . . .	22
4.1	High-level design of Privacy Advisor . . . . .	30
4.2	Data types in P3P . . . . .	31
4.3	The existing CLI . . . . .	32
4.4	Start page of existing GUI . . . . .	33
4.5	Settings in existing GUI . . . . .	33
5.1	The first prototype . . . . .	38
5.2	Navigation flow in extension. . . . .	39
5.3	Main menu of Privacy Advisor. . . . .	40
5.4	Advice to the user: reliable page. . . . .	41
5.5	Advice to the user: unreliable page . . . . .	41
5.6	Details on advices . . . . .	42
5.7	The information page in Privacy Advisor. . . . .	42
5.8	The settings page in Privacy Advisor. . . . .	43
5.9	The history page in Privacy Advisor . . . . .	44
5.10	Expansion of the main menu . . . . .	45
6.1	Gender of participants . . . . .	54
6.2	The age of participants . . . . .	55
6.3	Results on Internet shopping . . . . .	55
6.4	Results on using Google's services . . . . .	56
6.5	Results on navigation . . . . .	56
6.6	Opinions on the interface design . . . . .	56
6.7	Results on visibility. . . . .	57

6.8	Results on trusting the program . . . . .	57
6.9	Thoughts on information sharing . . . . .	58
6.10	Thoughts on shared information . . . . .	58
6.11	Results on reading privacy policies . . . . .	59
6.12	Thoughts on using Privacy Advisor . . . . .	59
7.1	The new advice window . . . . .	62
7.2	New history window . . . . .	63
7.3	Privacy policy in Privacy Advisor . . . . .	64
7.4	The new settings window. . . . .	66
7.5	The undetermined privacy window. . . . .	67

# Acronyms and Abbreviations

**AI** Artificial Intelligence

**APPEL** A Privacy Preference Exchange Language

**API** Application Programming Interface

**CBR** Case Based Reasoning

**CLI** Command Line Interface

**COPE** Comprehensible Privacy for End Users

**CSS** Cascading Style Sheets

**EPAL** Enterprise Privacy Authorization Language

**GUI** Graphical User Interface

**HCI** Human Computer Interaction

**HTML** Hypertext Markup Language

**HTTP** Hypertext Transfer Protocol

**ICT** Information and Communication Technology

**IE** Internet Explorer

**ISO** International Organization for Standardization

**ITEM** Department of Telematics

**JSON** JavaScript Object Notation

**KISS** Keep it Simple, Stupid.

**kNN** k-Nearest Neighbor

**NTNU** Norwegian University of Science and Technology

**P3P** Platform for Privacy Preferences Project

**PET** Privacy Enhancing Technology

**PPL** PrimeLife Policy Language

**PRIME** Privacy and Identity Management for Europe

**UI** User Interface

**URL** Uniform Resource Locator

**W3C** World Wide Web Consortium

**XACML** eXtensible Access Control Markup Language

**XML** Extensible Markup Language

**XP** eXtreme Programming

# Chapter 1

## Introduction

In this chapter I will give an introduction to the motivation and background for this thesis and also give a brief introduction to SINTEF ICT and the system this thesis is focused on. I will explain why privacy is an important concern on the Internet and why sharing personal information should be considered carefully. I will then give a short presentation of a few existing privacy tools. Last but not least I will also give a short description of how the work on this thesis has been carried out and the outline of this report.

### 1.1 Motivation

The increased use of the Internet and different services online has created a trail of information that we leave behind us. The use of social media, online banking services, email accounts and so on allows for many different details concerning our personal life to be stored and used online. In addition, we don't always control who has access to our data.

While accessible information about us is growing on the Internet, the potential ways to misuse or exploit them is likewise increasing. Because of this, online privacy has become an important and highly relevant topic on the Internet today. The type of information that is ok for sharing and with whom may vary with different people and situations. Sharing a phone number with friends and family on Facebook might be fine by some, but not everyone. Since there is no correct answer for what amount of information that is ok for sharing, everyone has to find their individual preferences.

When we start to use an online service, for example a social network, we have to accept the responsible service providers privacy policy, which contains information on how they will treat the information we provide to them. If we don't accept their policy, we will not be allowed to use the service. Such "take-it-or-leave-it" offers are considered a problem by many users who feel that they do not have a real choice.

Another problem is that most people don't read these policies, since they often

are long and complicated documents. The result is that most users accept privacy policies without reading them first, and are therefore unaware of what they have agreed to.

In order to deal with such privacy challenges there are many things one can do. For example we have tools or so called Privacy Enhancing Technology (PET) whose purpose is to help protect the privacy of end-users [1], either by helping them be more aware of privacy and information sharing or to avoid privacy risks and problems. PETs include a variety of tools and processes, but one way to help users with privacy is to help them understand privacy policy statements and give advice on what consequences accepting such privacy policies will have for them. This report deals with a PET named Privacy Advisor [2], whose purpose is exactly this.

## 1.2 Background

The background and idea for this thesis originated from SINTEF ICT and some of the research they have been conducting in the previous years.

### 1.2.1 SINTEF ICT

SINTEF is the largest independent, non-commercial research organization in Scandinavia [3]. They mainly work with research, innovation, developing technological solutions and generate knowledge. SINTEF possess high expertise in different disciplines like technology, medicine and social sciences.

SINTEF ICT is one of the subdivisions within SINTEF, mainly concentrating on research, services and products ranging from micro technology, communication and software technology, computational software to information systems and security [3].

In 2010 SINTEF ICT started the Comprehensible Privacy for End Users (COPE) project whose aim was to develop new technology to support users in their privacy decisions on the Internet. SINTEF ICT developed a system whose purpose was to enable users to better control how their personal information is collected and used online.

One of the most concrete outcomes of COPE is Privacy Advisor, where the system design and the underlying algorithms were developed by SINTEF ICT. As a result of close cooperation with NTNU the first version of Privacy Advisor was implemented in the fall of 2011. This implementation is further described in Chapter 4.

The COPE project were formally ended at SINTEF ICT in 2011, but some work on the topic is still being conducted by master students at NTNU.

## 1.2.2 Privacy Advisor

Privacy Advisor is a program intended to be used while surfing on the Internet. When the user access a webpage, its privacy policy will be interpreted by Privacy Advisor, matched with the user's privacy preferences and the user will be provided with an advice on whether the page should be trusted or not. The advice will be based on the way the webpage collects, processes and share the users' data and how the user's preferences upon these are.

The user will then be given the opportunity to provide feedback on the advice, upon which Privacy Advisor will learn from the feedback for future advices. Details upon the system and how it works is further described later in this report.

## 1.3 Problem Definition

In accordance to the above described motivation and background for the thesis, the problem definition of the project were defined as creating a user interface design for Privacy Advisor. The suggested design should be more usable and focused on the user and a suitable level of user involvement should also be determined. The focus of the project were decided to be on usability testing of the suggested design and also to evaluate it, based on the results from the test and how the mechanism of the system's learning process works.

### 1.3.1 Contribution

The main contribution of this thesis has been to take the system one step further in becoming a usable product. It will also be possible to directly use the design suggested in this thesis for further work and improvements of the program.

Issues concerning how the user think about the system and should interact with the program is determined, which is valuable information when further developing the product. What functionalities the system should have is also evaluated and implemented in the design. The suggested design is adapted to the users' knowledge on privacy and allows them to learn even more.

This work is valuable in order to determine the value and potential of Privacy Advisor and to ease the process of completing Privacy Advisor as a finished product since SINTEF ICT don't have the resources to continue working on this at the current time.

## 1.4 Existing Privacy Tools

Today there exists several security applications and programs whose purpose is to help the user think about their privacy and security while surfing on the Internet. These tools have different purposes, functionalities and run on different devices. One can find security applications for smart phones, programs that runs locally on your computer scanning for malware or programs that runs in your browser. There are programs to suit most needs and preferences. In this section a few privacy tools, somewhat similar to Privacy Advisor and whose purpose is to protect the user's privacy are briefly introduced and described.

### 1.4.1 Privacy Bird

Privacy Bird [4] is a tool that is quite similar to Privacy Advisor. Privacy Bird is a tool that was originally developed as a plug-in in the Internet Explorer (IE) browser, but is now also available in other browsers such as Google Chrome. The purpose of Privacy Finder is to help users make wiser decisions on privacy online based on their preferences. The difference between Privacy Advisor and Privacy Bird is that Privacy Bird needs the user's preferences before the program can be used, which is a rather time-consuming job, while Privacy Advisor tries to learn the user's preferences continuously.

Privacy Bird gives advices to the users by using changing visual symbols and optional sounds in the browser. A figure illustrating how Privacy Bird works can be seen in Figure 1.1. The program is based on the Platform for Privacy Preferences Project (P3P) technology, described further in Chapter 2.2.1.

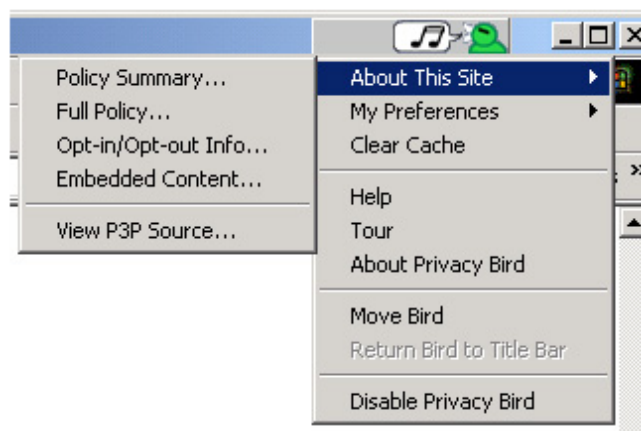


Figure 1.1: Privacy Bird, from [4].



## 1.4.2 Privacy Finder

Privacy Finder [5] is a P3P based search engine which marks or labels the search results with privacy information derived from the pages privacy policies. The labels indicate how well the search result matches with the user's privacy preferences. This tool is developed by the same people as Privacy Bird, but it is now an outdated software no longer in use. An example of how Privacy Finder worked can be seen in figure 1.2.

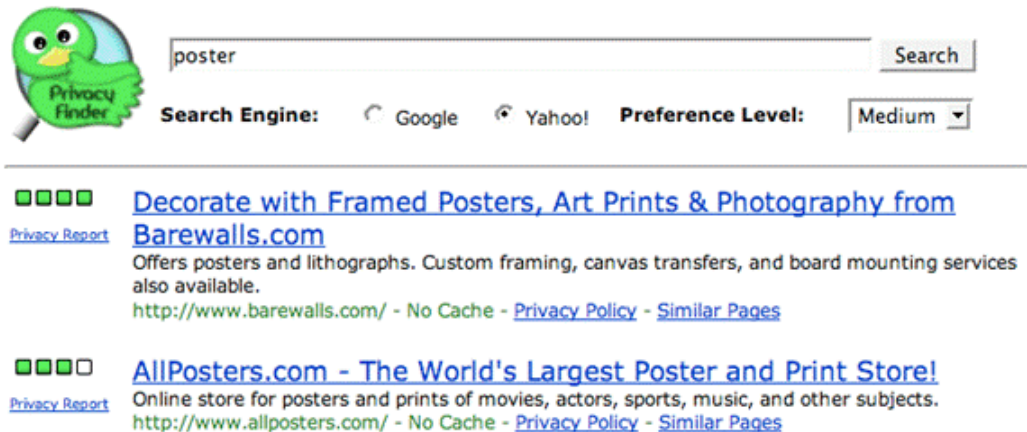


Figure 1.2: Privacy Finder, from [5].

## 1.4.3 Ghostery

Ghostery [6] is an extension for the Google Chrome browser. Its purpose is to alert the user of parties that operate in the background of webpages and learn more about them. It also includes links to the webpages' privacy policies. Ghostery also allows the users to block scripts, images, iframes and other objects from companies the user don't trust, but in order to do this the user has to provide the extension with several settings information on the user's preferences. One example on how the Ghostery interface can look like can be seen in Figure 1.3.

## 1.4.4 Tor

Tor [7] is a somewhat different tool than the ones already described, but is included in order to illustrate other privacy options. Tor is a free software and open network that helps to protect the user's privacy by mainly defending against network surveillance and traffic analysis. It was originally developed with the U.S. Navy in mind, but today it is used by normal people and other institutions as well. The Tor Project has several projects going on privacy and security, like Tor for Google Android devices and Browser protection.

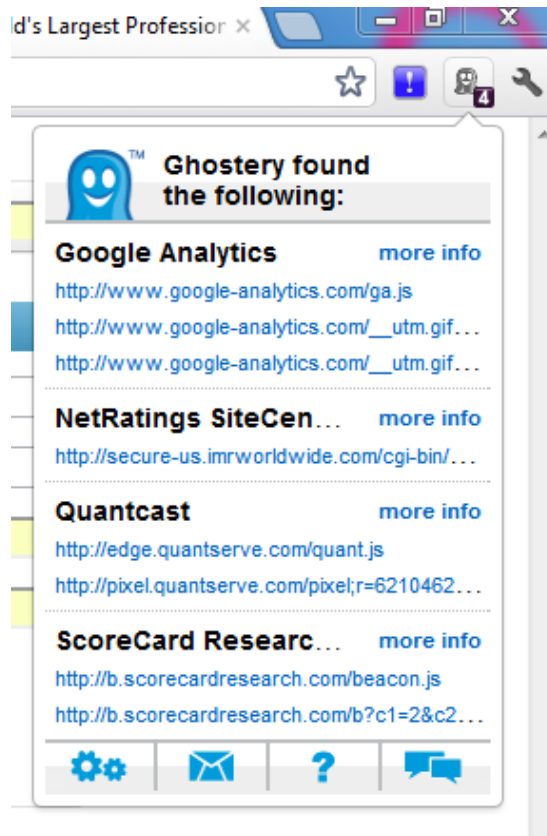


Figure 1.3: Ghostery.

## 1.5 Completion of the Thesis

The work done in this thesis has essentially been carried out in 3 main phases, each presented here. In addition, all methodologies used throughout all the phases are described in detail in Chapter 3.

### 1.5.1 Design Phase

The first phase was the Design phase, a phase that consisted of developing a design for the actual system. This phase also consisted of obtaining knowledge about the system and also relevant theory such as design principles, usability, privacy and relevant technologies that would be used in developing the design. This phase was considered over when a satisfying design was developed and a prototype for testing was ready. The relevant theory found can be found in Chapter 2 and the development of the design in Chapter 5.

### **1.5.2 Testing Phase**

The second phase was the testing phase. It started with planning usability testing of the developed interface design, by making a test plan with appropriate tasks as well as finding suitable users for the tests. This phase also contained the actual testing on the users and registering the results. The phase is described in detail in Chapter 6.

### **1.5.3 Evaluation Phase**

The third and last phase was the evaluation phase which consisted of evaluating the design, based on the results from the testing phase and the system's learning process. Based on the evaluation, the interface design was improved into a final interface design. This can all be further studied in Chapter 7.

## **1.6 Outline**

The outline of the rest of this report is as follows.

First Chapter 2 presents the relevant theory related to the work done in this thesis. This includes an introduction to privacy issues, privacy technologies, machine learning and also graphical user interfaces and usability principles. If you have a background from some of these topics you might want to skip this chapter, or parts of it.

Chapter 3 describes the methods used to conduct the work described throughout this report, and also explain why the methods were chosen. Chapter 4 follows with a description of Privacy Advisor and details on how it works.

Chapter 5 then presents the interface design suggested for Privacy Advisor and an explanation of the choices made. I also give an explanation of assumptions and changes made to the system in order to make the system work as desirable.

After this, Chapter 6 presents the plans made for the testing process and summarizes the results from it. Chapter 7 then follows with the evaluation, which discusses the suggested GUI, the user involvement and the results from the tests. The final design suggestion is then presented.

Chapter 8 then describe some suggestions and ideas for future work on this topic. In the end Chapter 9 concludes the work done.



# Chapter 2

## Theoretical Background

In this chapter I will provide the theoretical background necessary to understand the base of this report and the concepts and technologies presented throughout this thesis. I will start with a description of privacy and privacy policies. I will then give a brief introduction to machine learning and Case Based Reasoning (CBR). Further, I will explain what is meant by privacy enhancing technology, and in the end I will give an introduction to GUIs, Human Computer Interaction (HCI) and usability.

### 2.1 Privacy

The term privacy is a large and somewhat nuanced concept, with many definitions. Most people would however agree that it concerns the ownership of personal information<sup>1</sup> and also the owner's right to decide over it.

The Norwegian Data Inspectorate (Datatilsynet) state that the concept of privacy refers not only to the protection of the private life or the individual's personal integrity, but also to the protection of the individual's right to influence the use and dissemination of personal information about themselves. The individuals should to the greatest extent possible, be able to decide over their own personal information [8].

Privacy is also recognized as a human right. It is in the European Human Rights Convention [9] stated that:

*"Everyone has the right to respect for his private and family life, his home and his correspondence."*

There are many laws and regulations whose intent is to secure our privacy, but to what extent it is applicable and maintained depend on the country you're in.

---

<sup>1</sup>Personal information is here considered as information that can be used to identify an individual with reasonable means, such as name, address, contact information, social security number, financial information and so forth.

However, privacy has become a concern due to the development of information technologies as the information is more available and the countries border where different laws apply is erased on the Internet.

### 2.1.1 Internet Privacy

The term Internet privacy involves the right to privacy concerning storing, repurposing, disclosure and display of information pertained to a person via the Internet. This has, as explained in Chapter 1.1 become an important topic and challenge, due to all the information left and shared on the Internet and also because of how easy it has become to collect this information about a person, with or without the persons consent.

The Internet is international and largely unregulated [10] which means that users from all over the world is at risk for privacy violations. Many countries have laws and regulations in order to maintain a certain level of privacy, but when using a service online it is not given that the same laws as your home country applies when the service originates from somewhere else.

### 2.1.2 Privacy Concerns

Privacy concerns are situations that arise when individuals can no longer maintain a substantial degree of control over their personal information or the use of them. According to Chung and Paytner [10] the threats that people are most concerned about include:

- Visiting webpages that will be secretly tracked.
- Get e-mail addresses and other personal information captured and used for marketing or other purposes without their consent.
- That their personal information will be sold to third parties without their permission.
- Credit card thefts.

The way information is gathered on the Internet might not always be so obvious. Sometimes the user is asked to provide the information by himself by filling out forms and sometimes cookies<sup>2</sup> are used to gather information about users automatically. This creates different concerns for the user, both that information can be misused and that their surfing and activities can be tracked.

---

<sup>2</sup>Also known as Hypertext Transfer Protocol (HTTP) cookies, is a piece of data stored in the browser that can be used to identify a user. Often used by webpages to recognize users and their settings and preferences [10].

## 2.2 Privacy Policies

Most public websites have a privacy policy describing how users or visitors information is used and stored.

Webpages like `www.facebook.com` have a privacy policy containing information about how their registered user's information is collected, stored and shared with others. In order to make use of the services Facebook provide you have to accept their privacy policy and then give your information to them [11].

We also have other types of pages like `www.vg.no`, which is a Norwegian newspaper's webpage, who has a privacy policy describing how they collect information about their visitors and for what purpose they do. In this case it is enough to visit the webpage in order for them to receive information about visitors [12]. This information is not likely to identify you as a person, but is usually enough to recognize your user agent<sup>3</sup>.

There is also a difference in what a good privacy policy is and what a good policy is for a specific user. A good policy is structured and clear and provide information on what kind of information is gathered, how it's used, to whom it is made available, what security is provided, how users are updated on changes in the policy and contact information to the company [13]. If a policy leaves out important factors it is no longer considered as a good policy and one should think twice before accepting it. When it comes to what is a good policy for a user, one have to look at the particular user's own preferences and compare it to how the policy suits them.

Privacy policies can be found in different forms and contexts, and is typically specific for a certain environment or context. They can be interpreted manually by humans or automatically by computer systems and programs. There are also various ways of representing privacy policies in a machine-readable way, which can be used for automatic interpretation of policies. The existence of these standards would hopefully create incentives for websites to make their privacy practices more available to the public and therefore influence them to represent their privacy practices using these standards.

### 2.2.1 P3P

One way to represent a privacy policy online is by using the Platform for Privacy Preferences Project (P3P) standard. P3P were developed by the World Wide Web Consortium (W3C) in 2007 and its goal was to increase the transparency of webpages public privacy practices in an understandable way [14].

The Platform for Privacy Preferences Project (P3P) standards purpose is to

---

<sup>3</sup>A user agent is typically the device you use for surfing the Internet, for example your computer or smartphone

enable websites to represent their policies in a standard machine readable format that can be retrieved automatically by user agents and further interpreted. With the help of P3P, user agents can inform the users of important issues and risks in the policies in a faster and easier way than by manually inspecting the privacy documents.

Technically, P3P consist of two parts. First a standard machine readable syntax that uses Extensible Markup Language (XML). This allows websites to describe their privacy practices regarding the collection, use, purpose and distribution of personal information. Second, it contains a "handshake"-protocol built on top of the HTTP protocol that enables user agents to retrieve websites policies automatically when entering the webpage. The P3P standard is the one used by Privacy Advisor and the behavior of it will be further described later in this report.

### 2.2.2 Other Standards for Privacy Representation

There are also other standards, in addition to P3P that defines ways of representing machine-readable privacy policies. Two of these standards are very briefly presented here in order to show differences and similarities.

One standard is the PrimeLife Policy Language (PPL) that were developed based on the scenario that a user wants to access a resource hosted by a data controller, but has to reveal some personal data in order to do it. The standard allows the data controller to express what personal data he needs from the user, how he will treat this and allows the user to decide to whom he is willing to share it and how it should be treated [15, p. 10]. This standard also allows for two-sided data handling preferences with automated matching, credential-based access control, language symmetry and downstream usage.

We also have the Enterprise Privacy Authorization Language (EPAL) and the eXtensible Access Control Markup Language (XACML) standard. Both are independent of platforms and are somewhat more fine-grained and expressive than the P3P standard [16]. EPAL and XACML are both quite similar and share the same authorization model. At the same time, they are also very different in several ways. While XACML supports the ability to specify conditions, handling error conditions and missing attributes and provides support of additional primitive data types, EPAL does not. EPAL in turn supports the concept of a policy vocabulary and hierarchical categories with defined inheritance [16].

There are also several other privacy policy standards, all with somewhat different properties. What is the most suitable standard depends on the service you want to provide.



## 2.3 Machine Learning

*"A computer program is said to learn from experience  $E$  with respect to some class of tasks  $T$  and performance measure  $P$ , if its performance at tasks in  $T$ , as measured by  $P$ , improves with experience  $E$ ."*

This is the definition of machine learning presented by Russel and Norvig [17]. The concept addresses the question of how to build software that improves its performance at some task through experience. Machine Learning draws ideas from a diverse set of disciplines, including artificial intelligence, probability and statistics, computational complexity, information theory, psychology and neurobiology, control theory and philosophy [17].

Machine learning is a subdivision of artificial intelligence, which is a branch in computer science whose aim is to make intelligent machines. This often includes the ability to make the machine work and behave as human beings.

In order for the machine to be able to act as a human, it would need to have functionalities that allow it to process natural language, store information it learns, have automatic reasoning and of course have the abilities of machine learning [18].

To make a machine or a program learn from experience, a learning problem needs to be defined. The problem would also need a well specified task, concrete performance metrics and a source of training experience.

### 2.3.1 Case Based Reasoning

Case Based Reasoning (CBR) is a technique used for solving problems based on previous experiences, and is a method familiar within machine learning. The technique tries to emulate human reasoning where previously experienced situations, recognized as cases, are used to solve new ones [19]. CBR is also a lazy learning method because it defers the decision of how to generalize beyond the training data until a new instances is observed [18].

The main purpose of CBR is to find a set of stored cases, called a ballpark solution [19], that is similar to the problem at hand and then suggest a solution to it based on the similar cases. A case that is not a part of the ballpark solution is ignored. This method is similar to the way human beings solve problems, as we often use our experiences to solve new similar problems.

Figure 2.1 illustrates the main flow in the CBR process. The process consists mainly of the following four steps:

- Retrieve: consists of finding previous cases that is closely related or similar to the one at hand.

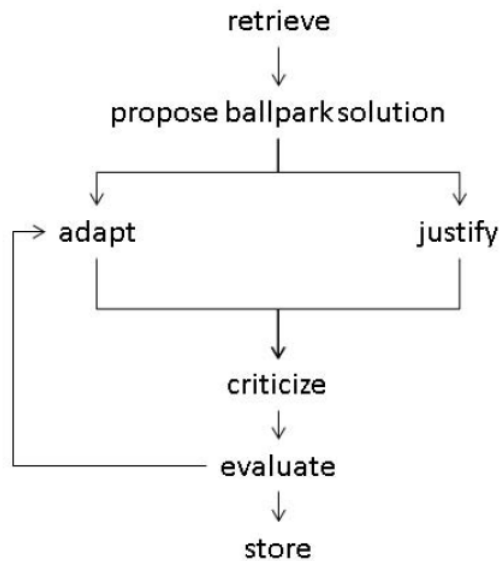


Figure 2.1: Case based reasoning, from [19].

- Reuse: looking at the previous cases and adapting the solution to them in order to solve the current case.
- Revise: presenting the solution to the user and waiting for feedback.
- Retain: store the feedback for use in future problem solving.

When implementing CBR, different algorithms can be used for conducting the different phases and functions of the technique. CBR is the technique used for Privacy Advisor, and the specific implementation of it can be further studied in Chapter 4.2.

### 2.3.2 k-Nearest Neighbor Algorithm

The k-Nearest Neighbor (kNN) algorithm is an instance based learning algorithm. It is one of the most thoroughly analyzed algorithms within machine learning, mainly because of its age and simplicity [18]. It is also an algorithm that can be used as part of the CBR process.

kNN is used to find the  $k$  nearest neighbors of an element when sorted on a predetermined property. This is done by using a distance metric, for example the Hamming distance<sup>4</sup>, depending on the dataset being evaluated. When looking at another property, the set of nearest neighbors changes. The word nearest is in this

---

<sup>4</sup>Is the process of finding out how many operations is required to change one element into another [20].

context equal to similar, and the neighbors are the most similar elements when ordered by the property.

The algorithm works quite well and is very simple to implement. For larger data sets however, kNN is not very effective because the distance to all neighbors would take too much time [17]. Additional mechanisms should therefore be implemented to make it more efficient to calculate in such cases, for example by preprocessing the training data.

## 2.4 Human Computer Interaction

Human Computer Interaction (HCI) is an interdisciplinary science which concerns how the interaction between the user and the product design should be [21, p. 4]. It is considered as interdisciplinary because knowledge from different fields are used to build knowledge within HCI. User experience and performance with computers will remain a rapidly expanding field, because the technology is constantly changing and the HCI has to follow and adapt to these changes.

### 2.4.1 User Interfaces

When a user interacts with a product or a machine, we say that they interact through a user interface. User interfaces comes in many different shapes and colors, all suitable for different situations, programs and users. Whether to choose one interface over another should be considered in each and every case individually. What distinguish the interfaces from each other is mostly how the user interacts with the system, and how the information from the system is presented for the user. Some of the most common interaction styles are listed below [21, p. 71].

**Command Line** Interfaces based on command lines are most suitable for frequent or trained users. The interface type allows the user to be in control of the system by using commands, but it also requires the user to learn the commands and the syntax. The error rates with these interfaces are also quite high, often due to syntax errors in commands. The error messages might also be quite confusing for inexperienced users.

**Natural Language** Is based on the ability the system has to respond to natural language like full sentences and phrases. This style would likely work a bit slower than others, because the users have to write out complete sentences to interact with the system. The users might also be asked to reformulate sentences in order for the system to understand the meaning of them.

**Form Filling** Form filling is as simple interface which uses forms that the user need to fill in with required information. This requires that the user understands the labels of the fields in the form and the valid data input. The user is also required to understand error messages and respond to them. Such a style is probably most suitable for experienced users or users with some training.

**Menu Selection** With this style users are presented the different options from a menu where they can select the one most appropriate for their intention with the system. This approach requires little memorization from the users and is also easy to learn, so it would be suitable for new inexperienced users. It could also work well for the more experienced ones, as long as the menu navigation is effective.

**Direct Manipulation** Direct Manipulation allows the user to interact with the system by directly manipulating the system by pointing at visual representation of objects and actions. This gives fast feedback to the user. This style, if done properly and effectively could be suitable for both the experienced and the less experienced users. Examples of direct manipulation can be touch-screens or drag and drop.

## 2.5 Design Principles

When designing a Graphical User Interface (GUI) there are several things one should keep in mind in order to create effective HCI and a good user experience. Several guidelines and principles have been developed in order to help designers in creating better systems and some used in this thesis will be presented here.

### 2.5.1 Usability

One important thing to focus on is the usability of a system. Usability is defined by the International Organization for Standardization (ISO) as:

*“the effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments”* [22].

In other words, if a system provides good usability it lets the users perform their tasks in a good and efficient way, which in turn makes the system more attractive to use. Jakob Nielsen, one of the pioneers in usability and HCI stated that usability consists of 5 elements, namely learnability, efficiency, memorability and satisfaction [23]. These all indicate that the system and design should be intuitive in order to give a good user experience.

## 2.5.2 Affordance and Constraints

When creating a new system or a new design we want to make sure the users understand what to do, what buttons to push and where to find the desired information. The idea that something is "the obvious thing to do" or that an object allows for a certain action is closely related to the term affordance. Affordance, or the perceived affordance is considered as the relationship between a user and an objects physical property [24]. As designers we want the user to perceive that some action is possible (or not possible).

Some things can not be done with an object and are recognized, using terminology, as constraints [22] and should be just as obvious for the users as affordance. If both these terms are well taken care of, the users avoid being confused and the system should be easier to use.

## 2.5.3 Ten Usability Heuristics

Jakob Nielsen has defined some principles, or heuristics, that apply for interaction design [25]. These principles is intended to work as guidelines on how to think when developing a GUI. The principles have their limitations and should be considered in a larger context, and also needs to be interpreted and shaped for each environment individually. Either way, these principles give a starting point for designers to avoid the biggest mistakes.

The Usability Heuristics and what they mean are listed below:

### 1. Visibility of system status

The user should always be informed about what is going on with appropriate feedback within reasonable time.

### 2. Match between the system and the real world

The user should be presented with familiar words and concepts, and be given information in a natural and logical order.

### 3. User control and freedom

Users should have the option to regret an action, in case of mistakes, to leave unwanted states. Support undo and redo functions.

### 4. Consistency and standards

Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions and strive for consistency.

### 5. Error prevention

Try to avoid error messages, eliminate error-prone conditions and present users with a confirmation before they commit to the action.

### **6. Recognition rather than recall**

The users should not have to memorize information, actions and options. Instructions for use of the system should be visible or easily retrievable whenever appropriate.

### **7. Flexibility and efficiency of use**

Allow users to tailor frequent actions, by giving experienced users the option to use shortcuts.

### **8. Aesthetic and minimalist design**

Don't include irrelevant information or objects in the design, because it diminishes their relative visibility.

### **9. Help users recognize, diagnose and recover from errors**

Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.

### **10. Help and documentation**

Provide the opportunity to give help and information for the user who needs it. It should be easy to search for, focus on the user's task and should not be too long or complex.

## **2.5.4 KISS Principle**

The KISS principle [26], "*Keep it Simple, Stupid*", refers to the idea that an easy solution is normally better than a harder and more advanced one. This principle is being used in, and applies to many different areas of expertise, including interface design. The principle is supposed to be a reminder that usability often comes with a simple design solution. It would also imply that design elements that are unimportant or complicated should be avoided or simplified. The principle have different interpretations, like "*Keep it simple and stupid*" or "*Keep it short and simple*". Common for all the interpretations is the focus on simplicity.

# Chapter 3

## Methodology

In this chapter I will present the methodologies used throughout the work described in this report. I will present the methods stepwise for each phase of the process and also try to explain and justify why the different methods were chosen. All theory described in this chapter is taken from Oates [27] unless other is stated.

### 3.1 Methodology in Academic Work

When conducting academic work or research in particular, it is important to follow methods. This is because the choice of methods will influence researchers in how they gather and evaluate their data, and therefore also the quality of the research. Research is in Oates described in the following way:

*Research is the creation of new knowledge, using an appropriate process, to the satisfaction of users of the research.*

He also says that doing good research is also about not taking shortcuts or jumping to conclusions, but rather taking the time to find the appropriate ways of finding data, recording them, analyzing, evaluating and presenting them. Further aspects such as purpose, product, process, participants, paradigm (pattern or model) and presentation have to be considered to present good academic work.

#### 3.1.1 Qualitative and Quantitative methods

When it comes to research methods, we usually divide between qualitative and quantitative methods. These are appropriate in different situations and have a bit different focus. While quantitative methods focus on bigger amounts of numbers to produce statistics, qualitative methods are more focused on data other than numbers.

Quantitative methods is typically based on activities such as questionnaires,

experiments, mathematical modeling or other methods where data is being analyzed in order to search for patterns that can lead to conclusions.

Qualitative methods on the other hand focus more on interviews, observation or documents. These data appears through ethnography <sup>1</sup>, action research or case studies. In action research, the researcher is actively involved and has to observe and participate in the phenomenon of the study. Case studies differ in that the researcher base his data collections on interviews supplemented with documents rather than observations.

When doing research on information systems and the context they appear in, qualitative methods are the most common because such studies often focus on the understanding and the use of the systems. Michael D. Myers [28] once said the following;

*"qualitative research methods are designed to help researchers understand people and the social and cultural context within which they live".*

The focus in information system research is therefore the understanding of the use and because of this, qualitative methods are appropriate choices.

## 3.2 Literature Review

When doing research one should perform a literature study in order to gather and present evidence supporting your work. The literature will in other words provide the foundation of the research work.

A literature study was conducted mainly in the beginning of the project period, finding literature describing design principles and system related technologies and standards. There was also some literature reviewing during other phases on minor topics. The literature was typically found by searching on the Internet or the NTNU library database with predetermined keywords, but also books that had been presented as curriculum in relevant subjects.

A quick assessment of the literature were also done to check the credibility of the content, by considering where it was found, who wrote it and where and by whom it was published.

## 3.3 Design and Development methods

When developing new IT-systems one should plan the processes carefully and make use of established principles of systems development for the system to be delivered

---

<sup>1</sup>research methods based on firsthand observation, i.e. experienced by the researcher.



within the specified time and cost for the project. If there in addition is a customer, the methods chosen will help to assure that there is accordance between the customers' requirements and the product.

There are many methods and project management methodologies to choose from, where different methodologies are more suitable depending on the resources available, time, costs and whether there is a customer. One can choose sequential processes, like the waterfall model where every phase of the project are finished before continuing to a new one.

A more flexible way is to choose a method based on iterative thinking like agile development or eXtreme Programming (XP). These approaches allows for going back to previous phases and reconsidering the decisions made. An iterative approach is typically a five step process that is revisited until the product is satisfying. These five steps are:

**Awareness** Involves the recognition of a problem that needs to be solved and identify the needs.

**Suggestion** Involves finding and then suggesting a solution for problems pointed out.

**Development** Is where the ideas are implemented. How this step is conducted depends on the type of product being developed.

**Evaluation** The product is being examined and evaluated, and the deviation from the expectation assessed.

**Conclusion** The results are determined and knowledge are gained and identified.

As the focus of this thesis is to suggest a design rather than developing the actual software, an iterative approach was chosen. Since there also is a "customer" involved, this seemed to be the most suitable approach since it allows the product to continuously be improved, until reaching a satisfying result. Prototyping were further chosen as the method for developing the design.

As the feedback from SINTEF ICT and users were used for further improvements of the design suggestion, the specific iterative method used is recognized as user-centered design and is defined by ISO 9241. The phases seen in Figure 3.1 almost exactly match to the phases listed above for iterative processes.

In this case would the method be used in two main iterations, where feedback from SINTEF ICT would be used for the first iteration and feedback from potential users in the second. This would be the results of activities performed in the box concerning evaluation of design against requirements from the figure.

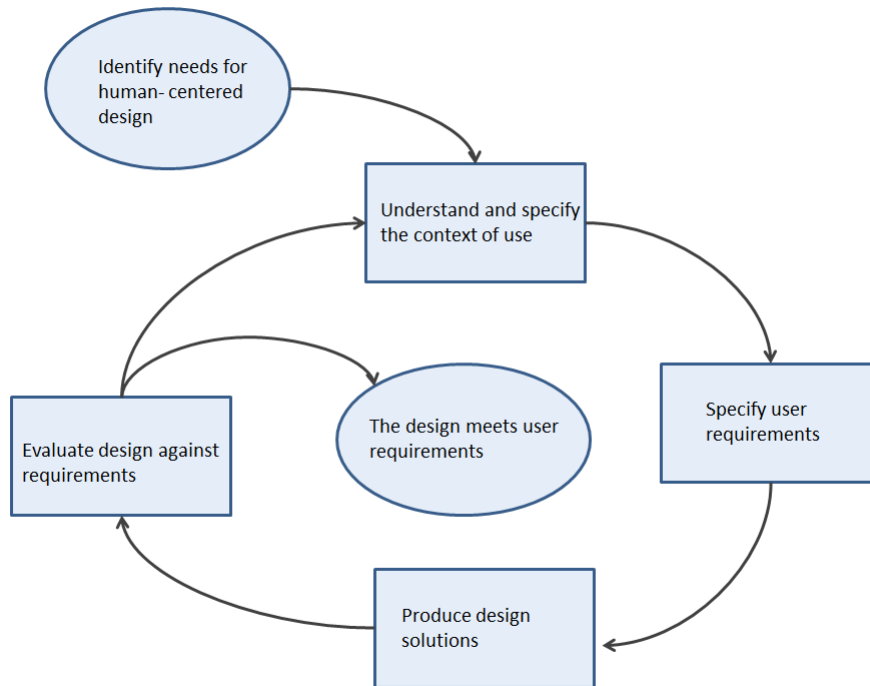


Figure 3.1: User-centered design, improved from [29].

### 3.3.1 Prototyping

For an iterative approach as described above, prototyping is a very suitable approach. A prototype can be seen as an experimental, incomplete design or program developed to test design ideas [30]. In other words, it is not a finished product.

A "low-fidelity" prototype is a prototype that is far from the finished product, typically the first draft and often made in paper or wood rather than being programmed. Such a prototype does not necessarily include all the intended functionality, but is used more to present the main design principles of the product.

In contrast, a "high-fidelity" prototype is more similar to the finished product and might also include more functionality. If the prototype's purpose is to illustrate some kind of software, it is usually programmed, but typically in a simpler way or programming language than the finished product.

The prototypes can also be seen as either vertical or horizontal, whereas the horizontal looks like a finished product without all the functionality, the vertical has some of the functionality in place [30].

The method of prototyping consists of developing a prototype that is designed and analyzed. The understanding gained from the first version is used to modify the design and create a revised system prototype, also by adding more functionality to it. These steps can be repeated several times in order to further develop the prototype into a satisfying implementation or product.

In other words, prototypes allows for pointing out opportunities. They also give the people involved a chance to provide feedback and explore different designs without using too many resources on it.

The advantage with prototyping is that it's not necessary to have a full understanding of the problem or all the details before trying out tentative solutions and ideas. In addition to this the method were also chosen because it seemed like a natural choice, as the design would gradually improve during the process due to own ideas and feedback from both SINTEF ICT and usability tests.

## 3.4 Testing the Design

Testing of the design was chosen in order to receive additional feedback on the system to reveal potential constraints that neither I nor SINTEF ICT had thought of. The method used for the tests were usability tests on users, observation of the tests and feedback in form of a questionnaire.

### 3.4.1 Usability Testing

According to ISO 13407 usability testing are defined as the process *"to ensure that the delivered product reaches a minimum required level of usability, to provide feedback during the design on the extent to which the objectives are being met, and to identify potential usability defects in the product"* [22]. We perform usability testing in order to see if our products have potential in the market.

In usability testing you typically want to determine the system's usability. Usability was in Chapter 2 defined to consist of the following three things, as are to be measured in the tests:

**Effectiveness** The extent to which tasks allows themselves to be performed is considered as the effectiveness of a product. This will give answer to whether the system covers the relevant functions, and whether the users are able to use them.

**Efficiency** Efficiency is a measure on how efficient a task allows itself to be performed. This would require a quantitative measure on the time spent on obstacles compared to actual performing the exercises.

**Satisfaction** Satisfaction is the experienced usability of the product or system. This requires tests, interviews, field studies, questionnaires etc. in order to determine every individual user's experience of the system.

All the three measures are important ones in the planned test, and will be measured. The test is both formative and summative. Formative because the feedback will be used with the purpose of improving the design further, with focus on discovering faults and elements that does not work. Summative because the usability of the product will be measured and checked, where the focus will be on performance of the tasks and the feedback from the questionnaire. Usability testing were also chosen because it was considered a practical way to gain feedback, since it would not require to many resources to conduct and potential participants were considered easy to recruit.

#### 3.4.2 Observation

Observation is by Oates described as the action of "watching" or "paying attention to" events.

In this case observation will be equal to paying attention what the users are doing during the tests as a complete observer<sup>2</sup>.

Observation also involves looking, but can also include use of other senses as well. For example hearing is an important factor, since the users can make sounds to emphasize a feeling, for example by a sigh if bothered. Findings will therefore be noted during the tests for further analysis later.

The goal of the observation is to get an accurate and complete overview of the test. The advantage is that it can create an insight into how things work in social surroundings, without people noticing their own practices or being able to report it. The observer will then gain knowledge on how people actually behave in specific situations.

Being under observation can also affect the outcome of test for the person being observed. This is recognized as the "Hawthorn-effect" [31] and indicates that people can change behavior (consciously or unconsciously) because they know they are being observed. This is something that can easily affect the results of the observations, and it is important to take this into consideration when conducting the tests and evaluating the results.

This method were chosen because it works well together with usability testing, and also don't require that many resources to conduct, in addition to the advantages already mentioned above.

#### 3.4.3 Questionnaires

A Questionnaire is a list with a pre-defined set of questions placed in a specific order. The users were asked to answer the questions, thus providing data for further

---

<sup>2</sup>a complete observer is present only as an observer and is not participating.

analysis and interpretation. The questionnaire was self-administered by the user, meaning that they answered the questions without observation or supervising. I was still present in the same room in case of questions or clarifications.

The method is well suited in cases where you need specific information and know which questions you want to ask. It is important that the questionnaire is carefully prepared in order to successfully collect the desired and reliable data. It is in Oates cited that:

*"Simply stated, the quality of the information obtained from a questionnaire is directly proportional to the quality of the questionnaire, which in turn is directly proportional to the quality of the construction process."*

Also the interpretation of the questions can have a huge impact on the results of the questionnaire. It is therefore important to formulate the questions so that they are always interpreted in the same way. Further, the type of questions chosen will also influence the results and also how the data will be evaluated and analyzed afterwards, whether it be yes/no questions, plain text, multiple choice or a Likert Scale<sup>3</sup>.

Questionnaires have its advantages and disadvantages. Some of the disadvantages worth mentioning are that you can not correct misconceptions or confusions that the respondents had while filling the form. The way the questionnaire is presented is therefore very important for the outcome. The quality of the data gained from questionnaires has a direct link with the quality of the questionnaire.

This method was chosen because it was considered feasible with the available resources, and also would seem more harmless for the users than the observed tests. The questionnaire would then allow for more honest feedback from the user, even though there was still a danger that they might answer what they thought I wanted them to. I also had quite a clear vision of what I wanted to ask and find out from the users.

## 3.5 Evaluation of Data

When collecting data for research purposes one should evaluate the results using structured methods to reach reliable conclusions. Recommended methods for evaluation depend on the type of data being analyzed, whether it is qualitative or quantitative data. Both types of data are collected during the planned test phase and methods for evaluation of both types should therefore be determined.

Regardless of the type of data being evaluated, one should always be aware of

---

<sup>3</sup>A Likert Scale is a scale where you are asked to place your opinion, for example on the scale from 1 to 5, how much do you agree with the following statement.

potential sources of error and the validity of the data. Another thing to be aware of is that different people might perceive questions, answers or observations differently, resulting in different interpretations of the same event.

#### 3.5.1 Evaluating Quantitative Data

Since quantitative data usually contains numbers, a normal approach for evaluation is using statistics to find the average mean and standard deviations to make further conclusions on them. Making graphs or other graphical presentations of the results is also a good way to illustrate the distribution of the data.

Statistical analysis of data collection would typically be seen as reliable presentations of results, but the analysis can only be as good as the data collected. The presentation of the results should therefore be suited for the data.

When looking at the amount of users who answered this or that, quantitative evaluation methods can be used. Since this will be the case for much of the feedback from the questionnaire, graphs or pie charts will be used to illustrate the proportions of the answers, together with a text based description. The actual evaluation will consist of finding out what the data mean and imply, what is important and what relevance they have for further work and improvements of the design. Since many of the results will reflect how many agreed with a statement, the meaning of the feedback should be easy to find. This method was therefore used to evaluate and interpret the quantitative data collected.

#### 3.5.2 Evaluating Qualitative Data

Evaluation of qualitative data includes interpretation of other data than numbers, typically observations, text, sound, pictures etc. This will in this work typically be collected from the text based questions from the questionnaire and observations from the usability testing. The methods chosen for this evaluation will therefore be the ones suggested by Oates and described here.

To prepare the data for evaluation, all the data should be gathered in one place, in one format to get a general impression and to identify key themes and relations within the data. It will then be an advantage to try to systemize and categorize the data to ease the work of evaluating them. It will also be important to find out what kind of data is irrelevant so that time is not wasted on them. This is important so that one is not overwhelmed by the amount of data to process. At the same time qualitative data might provide more useful data than quantitative data alone.

Evaluation of the qualitative data should therefore be conducted in a structured way. It will in this case be done categorically by the findings.

In qualitative data analysis it is also important to be aware that the interpretation of the data can be affected by the researcher evaluating them, and one should therefore try to make objective analysis and conclusions.





# Chapter 4

## System Description

This chapter contains a thorough description of Privacy Advisor and how it works. I will also go into detail on how the system learns the user's privacy preferences using Case Based Reasoning (CBR). All information mentioned in this chapter is taken from Bernsmed et al.[2] or provided by SINTEF ICT, unless others is specified.

### 4.1 Privacy Advisor

Privacy Advisor is as already explained a PET whose intention is to help the user make wise decision on privacy issues while browsing the Internet. It helps the user by providing advice on whether a user should trust a webpage with its personal information or not. Advices are given based on the websites privacy policies and how it compares to the users' privacy preferences.

The system uses the P3P technology to read and understand a websites privacy policy and CBR to compare it with similar policies. If Privacy Advisor finds that the current webpage's privacy policy is similar to other webpages that the user had already accepted, it will provide the user with the advice that the page can be trusted. The same applies for advices for pages that should not be trusted. The user is then asked to provide its opinion on how the page should be considered.

The programs purpose is in other words to give guidance to the user rather than to restrict its use. The CBR engine allows the system to learn from the feedback provided by the user, and to adapt to the specific user's preferences.

The first version of the system were developed by students at NTNU with guidance from SINTEF ICT, through a project in the subject TDT4290 - Customer Driven Project in the fall of 2011. The program was implemented using Java and associated libraries. The program has its own database where saves previous decisions to use for training data for future situations. The system also has to be run locally and manually attached to the privacy policy for comparison. The logic, functions and user interfaces implemented are described in the following subsections.

## 4.2 The Advice Engine

Privacy Advisor’s advice generator or engine is based on CBR as described in Chapter 2.3.1. This engine mimics human reasoning where previously experienced situations or cases are used as a basis for solving new ones. In addition, the system allows for adjustments in those cases where the user disagrees with the advice given and overrules the advice. A high level overview of the system’s learning process can be seen in Figure 4.1.

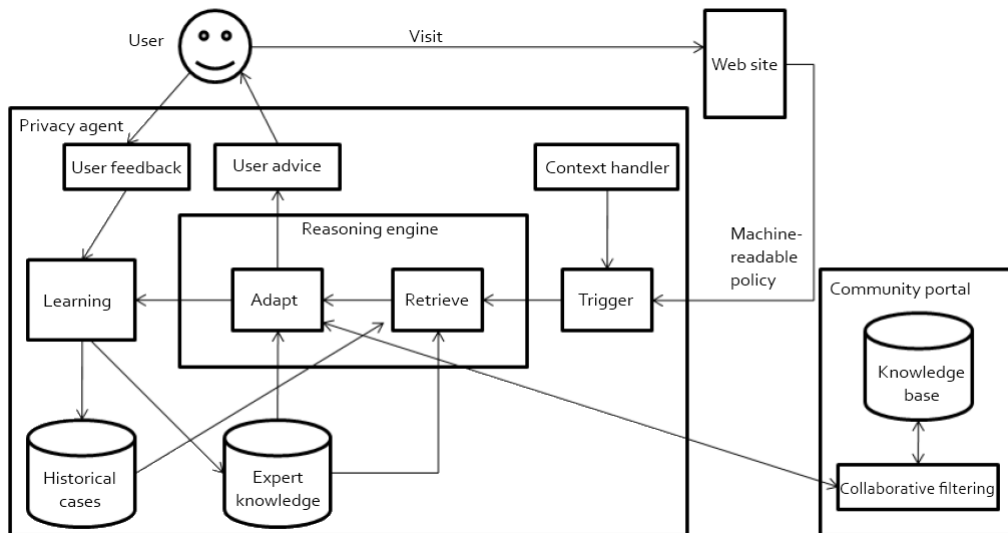


Figure 4.1: High-level design of Privacy Advisor, from [32].

In order to provide the user with meaningful advices, the system makes use of the algorithms and process described in the following subsections.

### 4.2.1 Finding Similar Cases

One very important function of Privacy Advisor is the ability to find cases that are similar to the current one. The engine is provided with a P3P privacy policy as input and based on parameters drawn from the policy, the system finds similar cases from the system’s database. If it finds an identical Uniform Resource Locator (URL) or privacy policy in the database, it’s treated as a duplicate and the decision from last time is used again.

All policies in the database are sorted by their distance to the current policy, and the  $k$  policies (where  $k$  is a configurable number) with the smallest distance are returned. This is done by using the  $k$ NN algorithm.

The policies are then transformed into statements, one statement for each data type in the policy, as can be seen in Figure 4.2. Privacy Advisor will then choose a subset of the statements, one from each of the  $k$  policies used for comparison.

Similar data types are decided by using ontology metrics, based on the implicit relationship defined through the naming of P3P data types.

When statements are paired the program will decide the similarity of the data. Each data type is given a value based on where in the list they are placed, again see Figure 4.2. The distance is then calculated as the absolute value of the difference between the two. These similarities are then combined as a measure for the total similarity of two statements.

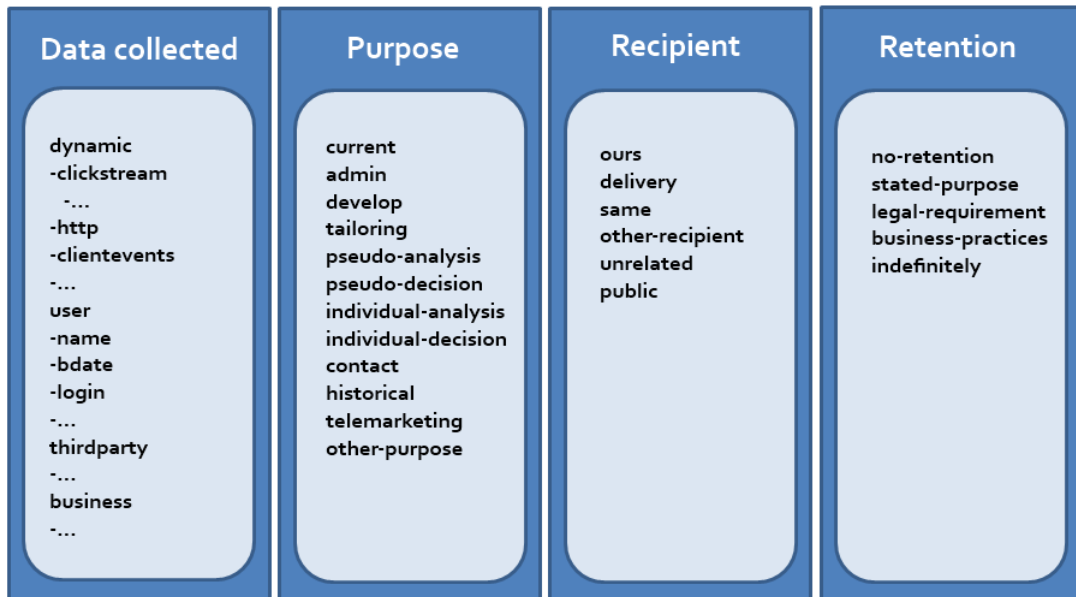


Figure 4.2: Data types in P3P, improved from [2].

There is also a configurable weight associated with every component that decides the importance of the statement. The similarities are therefore aggregated to determine a simple mean average. In the end, the system takes the  $k$  most similar policies and deliver them to the conclusion algorithm.

## 4.2.2 Conclusion Algorithm

In order to produce the advice, the algorithm sorts the  $k$  cases in two subsets according to whether they were accepted or rejected. Then the sum of each subset is calculated in order to determine their total similarity. Privacy Advisor then makes a decision based on the total similarity, i.e. the decision given most often in the  $k$  cases. A level of confidence is then calculated, which is done by taking the most cases with the same decision and divide it by the  $k$  cases to get a confidence level. For example, if 20 cases are selected as similar and 16 of them suggest the webpage should be trusted. The advice will be to trust the webpage with a confidence level of 16 divided by 20, and then converted to percentage.

Since there is a difference in how we would treat an advice with 51% and 99% certainty, Privacy Advisor also estimates a certainty indicator and presents it to the user. The indicator shows how many percentages of the  $k$  similar cases are consistent with the advice.

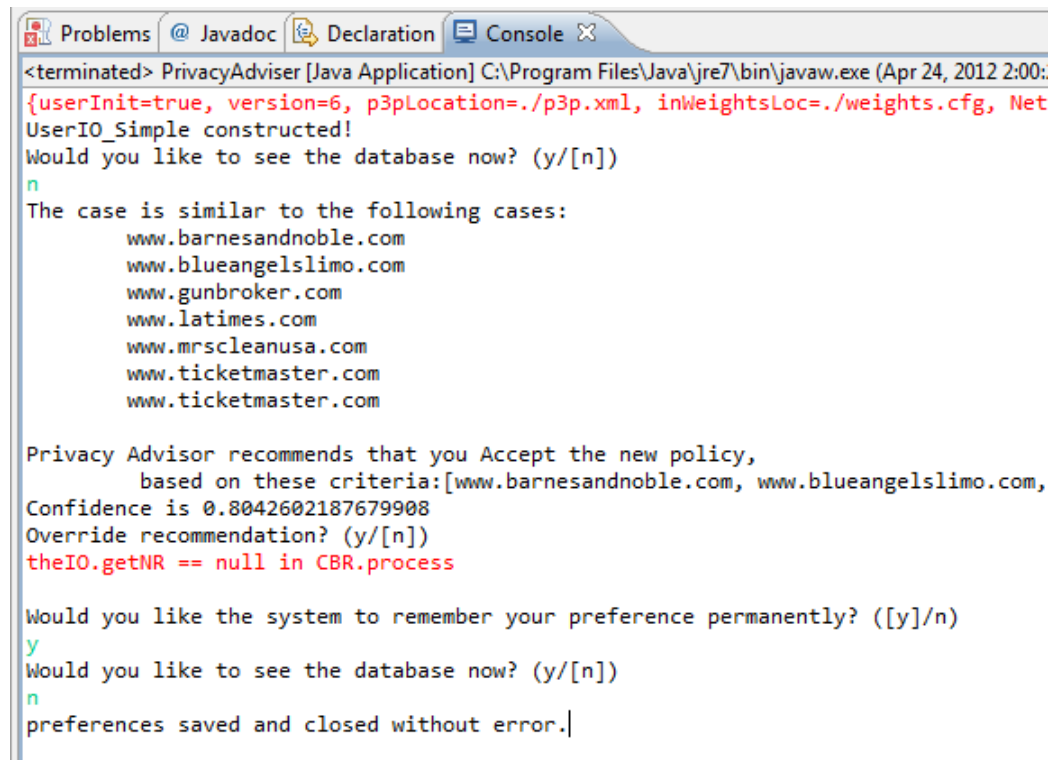
## 4.3 Existing User Interfaces

Privacy Advisor were developed with two different User Interfaces (UIs), one presented by a GUI and one Command Line Interface (CLI). Both are based on top of a general input/output module.

### 4.3.1 Command Line Interface

The CLI is a text based interface, running in the console of the development tool. It interacts with the user simply by text. This allows the user to control the program by using commands as described in Chapter 2.4.1.

A screenshot of the existing CLI and how it works can be seen in Figure 4.3.



```
<terminated> PrivacyAdvisor [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Apr 24, 2012 2:00:
{userInit=true, version=6, p3pLocation=./p3p.xml, inWeightsLoc=./weights.cfg, Net
UserIO_Simple constructed!
Would you like to see the database now? (y/[n])
n
The case is similar to the following cases:
  www.barnesandnoble.com
  www.blueangelslimo.com
  www.gunbroker.com
  www.latimes.com
  www.mrscleanusa.com
  www.ticketmaster.com
  www.ticketmaster.com

Privacy Advisor recommends that you Accept the new policy,
  based on these criteria:[www.barnesandnoble.com, www.blueangelslimo.com,
Confidence is 0.8042602187679908
Override recommendation? (y/[n])
theIO.getNR == null in CBR.process

Would you like the system to remember your preference permanently? ([y]/n)
y
Would you like to see the database now? (y/[n])
n
preferences saved and closed without error.
```

Figure 4.3: The existing CLI

### 4.3.2 Graphical User Interface

The graphical presentation of the program provides a simple interface with focus on functionality rather than usability. It can be used to get an overview of the database, change configurations and run the framework. All elements are implemented using Java SWING library elements.

The main window is split between the database on one side and the current privacy policy on the other. The menu has four options, reload database, configure, run and exit. Screenshots of the GUI can be seen in Figure 4.4 and Figure 4.5.

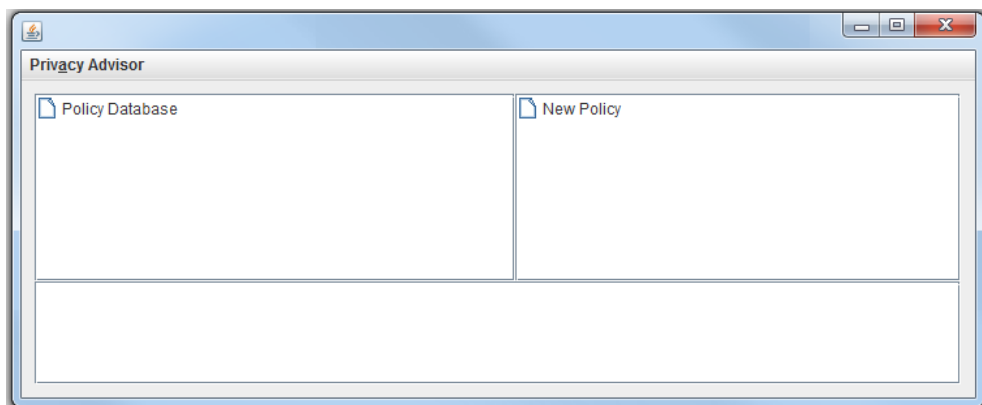


Figure 4.4: Start page of existing GUI

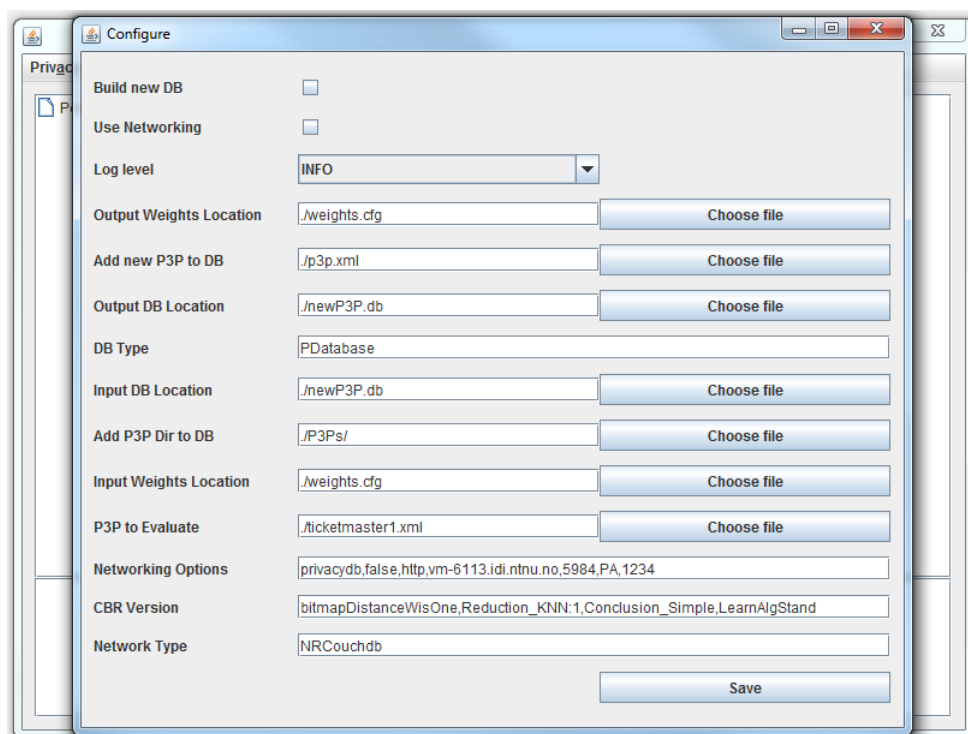


Figure 4.5: Settings in existing GUI



# Chapter 5

## User Interface Design

In this chapter I will present the suggested design for Privacy Advisor that will be used for usability testing. The chapter describes how the prototyping has worked and how the design has been developed through stepwise development of the prototypes. I will also present some user scenarios used as a basis for developing the design.

### 5.1 Browser Extension

The realization of the program was decided upon after careful consideration of how the system would work best for potential users. The conclusion fell on a browser extension as it was considered the most suitable for this kind of program. The idea of using a browser extension had also been suggested by SINTEF ICT and the students that developed the logic for Privacy Advisor.

The choice of using a browser extension were also made because it was considered as the solution that would require the least effort from the user in order to have it work as desired. If running in the browser, users would avoid doing extra work like manually downloading and running privacy policies for comparison as was the case in the existing version of the system.

#### 5.1.1 Google Chrome Extension

The choice of browser fell on Google Chrome. This seemed to be the obvious choice because in according to W3Schools [33] statistics Google Chrome is one of the most popular browsers currently in use, and one of the browsers that are still (in the time of writing) experiencing increasing usage. In addition to this, Google Chrome has an easy solution for adding extensions to the browser and their own Application Programming Interface (API) that allows for the desired functionality.

The API allows the program to run in the actual browser without disturbing the user in browsing the Internet. The program is at the same time visible to the user,

so that important information will be easily presented.

### 5.1.2 Realizing an Extension

Extensions for Google Chrome are mainly written in JavaScript, Hypertext Markup Language (HTML) and Cascading Style Sheets (CSS). The logic of the existing Privacy Advisor is implemented in Java, and therefore requires some extra work in order for the different components to work together.

This could for example be solved by deploying most of the logic as a web service that interacts with the extension. The extension would then mostly contain the graphical interface and navigation. Information fetched from the browser would be sent to the web service for processing and the response returned and presented to the user through the extension.

In addition, the logic would need some improvements in order to function properly or as desired. Realizing this as a working program would require an extra workload and is considered out of the scope of this thesis. The focus will therefore be on creating and suggesting a GUI for the program as a browser extension. This will be done by creating a simple Google Chrome extension simulating the logic and functionalities of the program.

## 5.2 User Scenarios

The suggested design for Privacy Advisor were developed based on some user scenarios describing the general usage of the program as it is intended to work. The scenarios describe the most important use and functions of the program and will therefore represent the SINTEF ICT's requirements for the design. These scenarios are further used as the basis for developing and suggesting the design and the test plan for Privacy Advisor.

### 5.2.1 Scenario 1 - Secure Online Surfing

Alice has already installed Privacy Advisor in her Google Chrome browser. When accessing the Internet Privacy Advisor starts, only running in the background without disturbing Alice in her browsing.

When she later browse into `www.twitter.com` considering to create a user account, Privacy Advisor changes its icon and provide Alice with information indicating that this page can be trusted, and Privacy Advisor is certain in its advice. The decision is based on the history of Alice's previous surfing, indicating that Twitter treats her information in a similar way as `www.youtube.com` as she previously accepted and trusted.



Alice decides to trust Twitter and accept it in Privacy Advisor. The program saves her decision and allows her to continue surfing without more interruptions. Privacy Advisor will not disturb her the next time she enters Twitter, since the decision is stored in the system's database.

### 5.2.2 Scenario 2 - Unsecure Online Surfing

At a later time, a friend of Alice named Bob recommends `www.paypal.com` as an easy service for Alice to use while shopping online. Alice visits the page, considering to start using it. Privacy Advisor reacts to PayPal's privacy policy and provides Alice with the advice that this page should not be trusted with her personal information. Privacy Advisor also presents her the level of certainty of the page, indicating a low percentage.

Alice checks the details of the advice which tells her that this page handles her information in a similar manner as `www.notgood.net` and `www.badbusiness.com` which she had already rejected.

Alice decides to reject PayPal, because she doesn't find it that important that she wants to risk her information being misused. Alice can then surf on without being disturbed by Privacy Advisor, but will receive a reminder the next time she enters this webpage.

### 5.2.3 Scenario 3 - Exploring Additional Functionality

Alice one day finds out that she wants to see what pages she has previously accepted and rejected. She opens Privacy Advisor and goes to the history of the system. Here she finds a list of all the pages that are stored in the database and the decisions related to them.

Alice finds that she had previously rejected Google's privacy policy for Gmail, and she now decides that she wants to change her mind. She then edits the decision by changing the pages status to accepted.

## 5.3 The Prototypes

The design suggestion for Privacy Advisor was developed in two main phases. I first started to develop a "low-fidelity" prototype on paper to present my ideas for the design. The other was to further develop the first design into a "high-fidelity" prototype including enough functionality to run usability tests on it.

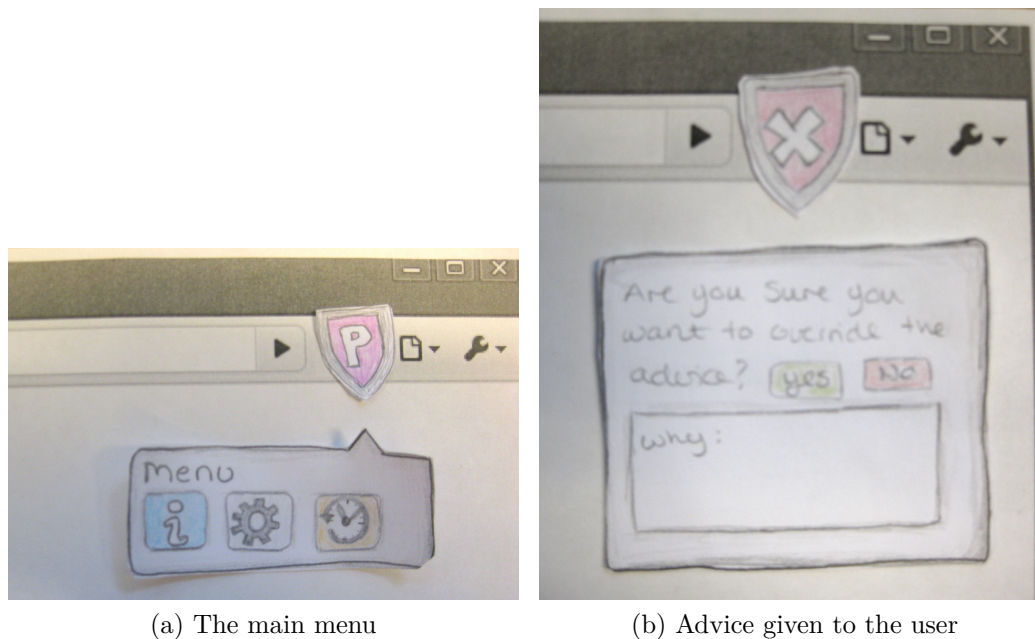


Figure 5.1: The first prototype

### 5.3.1 The First Prototype

The first ideas for the design were sketched on a piece of paper creating the "low-fidelity" prototype. The sketch illustrated the initial idea for the design. I had already been exploring existing solutions for privacy software and other existing extensions in Google Chrome.

Based on the existing solutions and the user scenarios described I decided how I thought Privacy Advisor should work. This prototype was created mostly to see how the ideas and design would work. The ideas were not tested on users, only shown to SINTEF ICT for feedback. Parts of the first prototype can be seen in Figure 5.1.

The ideas were well received by SINTEF ICT, and the work with the "high-fidelity" prototype was started. The design from the first prototype was used as the basis for the design on the second, only with small adjustments.

### 5.3.2 The Second Prototype

The second and improved prototype was developed as an extension in the Google Chrome browser. The prototype is a working program with most of the functionalities and navigation in place, only the system's CBR logic is simulated.

The prototype was developed using HTML, CSS and JavaScript in addition to Google Chromes own API for extensions which allows for interaction with the browser. In addition, most of the icons used were created using the program Paint.NET [34].

The first evaluation of this prototype was done by showing it to SINTEF ICT for feedback and comments. I also reviewed the design a few times by trying out different fonts, texts, icons, menu items and tables before determining which was most aesthetically looking. Comments from SINTEF ICT included different things that were added to the design, for example a suggestion for content in the settings.

When this prototype was considered finished, the design was taken to usability testing for further evaluation. The design from the second prototype is described in detail in the following section.

## 5.4 The Design

The final version of the prototype, ready for usability testing is quite different than the existing design and also provides some other functionalities. This GUI is more focused on the user and strives to provide user friendliness. The design is intended to be so intuitive that no training is necessary in order to use it, only a short introduction to the program.

The suggested design allows the user to receive advices on webpages, look at details for the provided advice and give feedback, look at the history of advices and the choices associated to them and also to edit them. The user can also read about the system and how it works and adjust some settings that affect how the program reaches the advices based on the user's preferences.

A simple diagram illustrating the navigation flow of the design and extension can be seen in Figure 5.2. A user can start the navigation either from the main menu or the advice. When navigating from the details you can only go back to the page you came from and not to a new page. In other words, you can not go from history to advice via the details or vice versa.

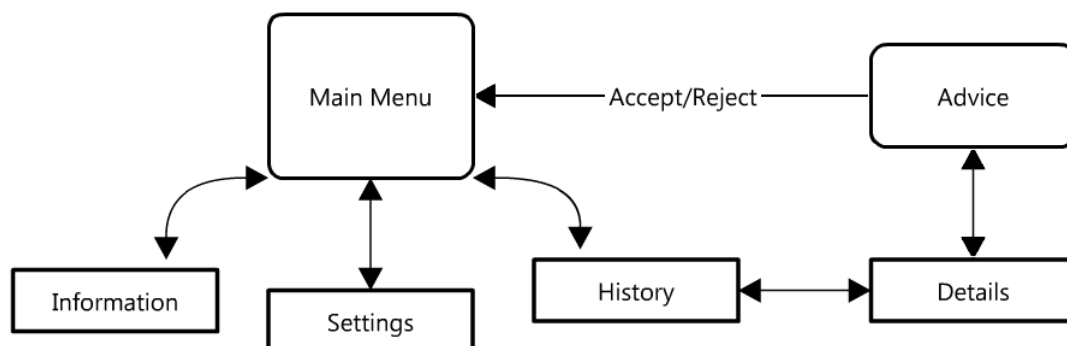


Figure 5.2: Navigation flow in extension.

### 5.4.1 Main Menu

When opening the proposed GUI for Privacy Advisor the main menu appears containing 3 icons; information, settings and history. The interface chosen is plain menu selection as described in Chapter 2.4.1, because it doesn't require much memorization and the different choices are presented once the user open the menu.

The graphical elements in the menu are constructed with the intent to be self-explanatory, using simple text and icons to indicate the selections, and buttons with well-known symbols. For example the settings button has a picture of gears and the text "settings" underneath it. This can be seen for all the choices in Privacy Advisor's main menu as shown in Figure 5.3.

The figure also shows Privacy Advisor's main icon in the browser. This icon is always present when the main menu is available.

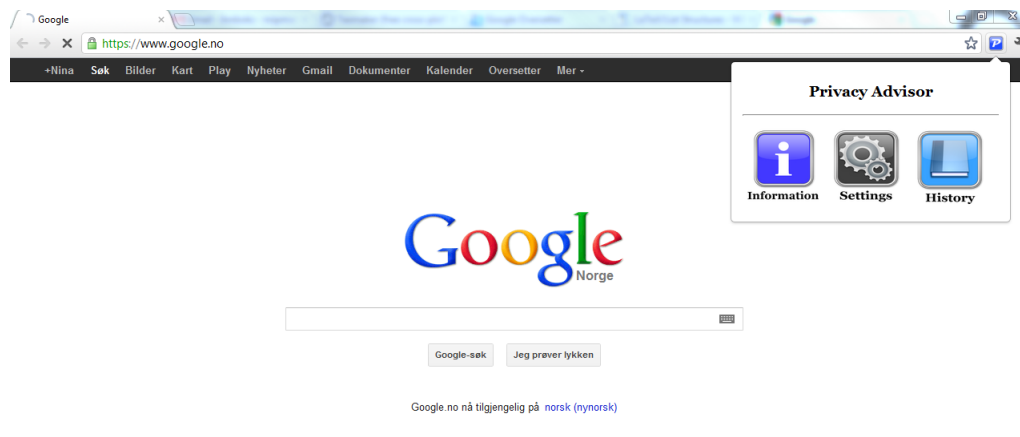


Figure 5.3: Main menu of Privacy Advisor.

### 5.4.2 Advices From Privacy Advisor

When the user is provided with an advice from the system, the icon in the browser is changed in accordance to the advice. An advice window can be opened by pressing the icon and the advice is then presented to the user. The user can then accept the advice by pressing a green button with the text "accept" or reject it by pushing the red button with the text "reject". Accepting means that the user agrees with the advice and vice versa.

The structure of the advice given to the user on different webpages is very similar for the "good pages" as for the "bad pages". This can be seen in Figure 5.4 and Figure 5.5. The advices also provide the user with the opportunity to leave a comment on the decision he or she makes on the page.

The user is also informed in the same way as with the advices when a privacy

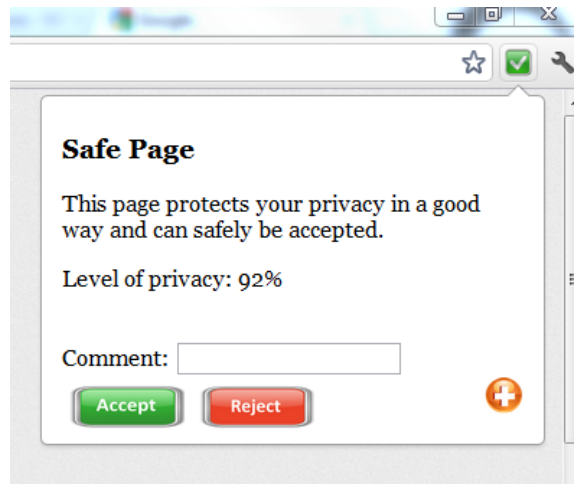


Figure 5.4: Advice to the user: reliable page.

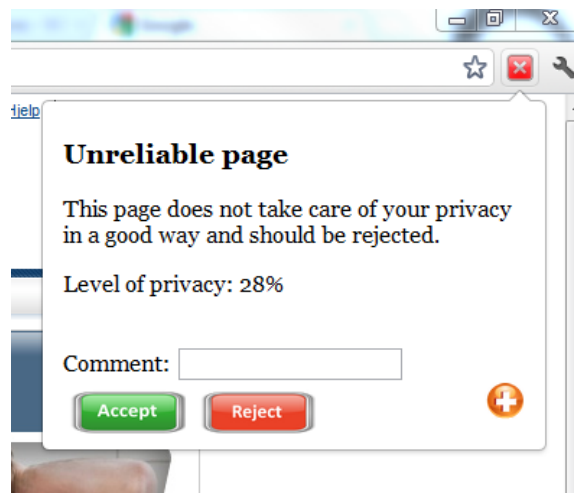


Figure 5.5: Advice to the user: unreliable page

policy for some reason can't be evaluated. The user is still encouraged to provide a decision on the page so the system can still learn from the event.

The user can also choose to see the details on the provided advice. This can be done by pushing the orange button in the advice window, and the details window will appear. The structure of the details page is also similar for all webpages, only the content will change according to the page visited.

The user can then navigate back to the advice by pressing the green return button as shown in Figure 5.6. When the user provides its decision to Privacy Advisor the window changes to the main menu window and the icon is replaced with Privacy Advisor's main icon.

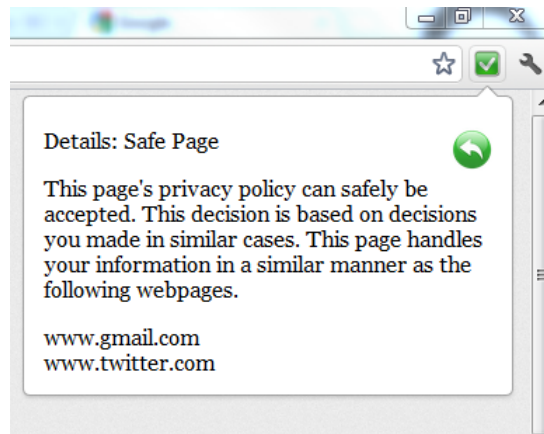


Figure 5.6: Details on advices

### 5.4.3 Information

From the main menu the user can choose to see the information. The user is then presented with a page describing the main functionality of the program and how the changing icons work. The intention with this page is that it can replace training of the users and give them a brief understanding of how the system works. The information page can be seen in Figure 5.7.

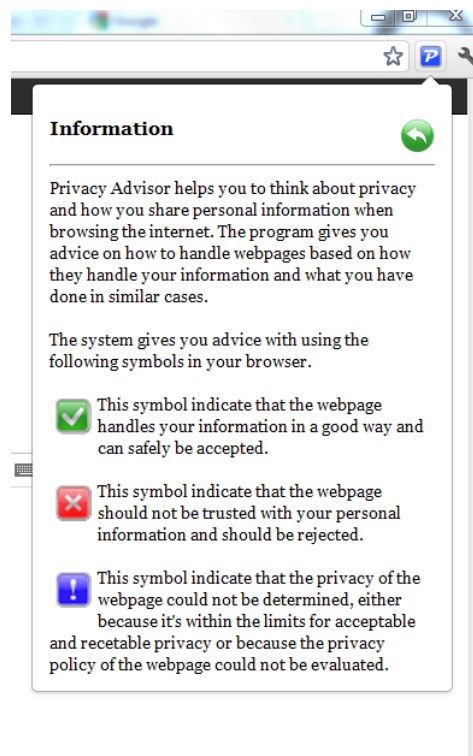


Figure 5.7: The information page in Privacy Advisor.

### 5.4.4 Settings

The user can also choose to go to the settings from the main menu. The settings allow the user to make adjustments on how the system emphasizes the advices. The user is given the opportunity to determine how many other similar privacy policies the program will use for comparison when determining an advice for the webpage. The user can also determine the level of privacy that he or she think is acceptable for a good page or a bad page, or in other the limits on when the pages privacy policy is considered ok or not ok.

Finally the user can also determine the weighting on which elements should be considered more important when comparing the privacy policies. The different elements that can be weighted is the type of data the user provide to the webpage, how the data is stored and handled, the reason the webpage gathers the data and who are given access to the information provided. The settings page can be seen in Figure 5.8.

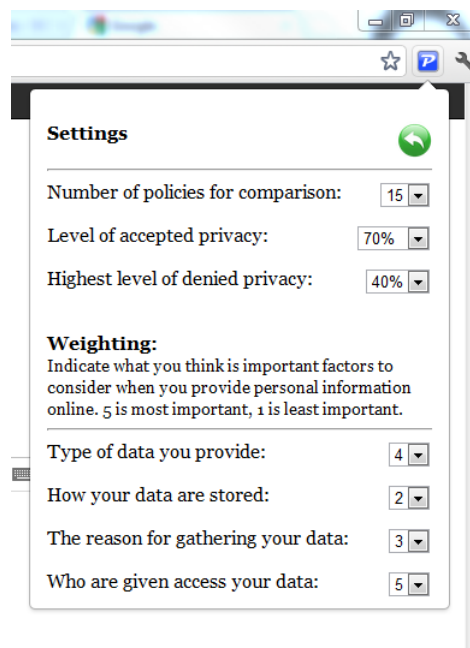


Figure 5.8: The settings page in Privacy Advisor.

### 5.4.5 History

The last choice in the main menu is the history option. The history page is an overview of the different webpages already evaluated and the decisions associated with them. Again the user is given the option to see the details of the webpages already evaluated (the same details as showed in Figure 5.6) and to change the decisions of the webpages if desired. The list should automatically be updated when

feedback is given to a new advice, even though the current list in the prototype is static. The history page can be seen in Figure 5.9.

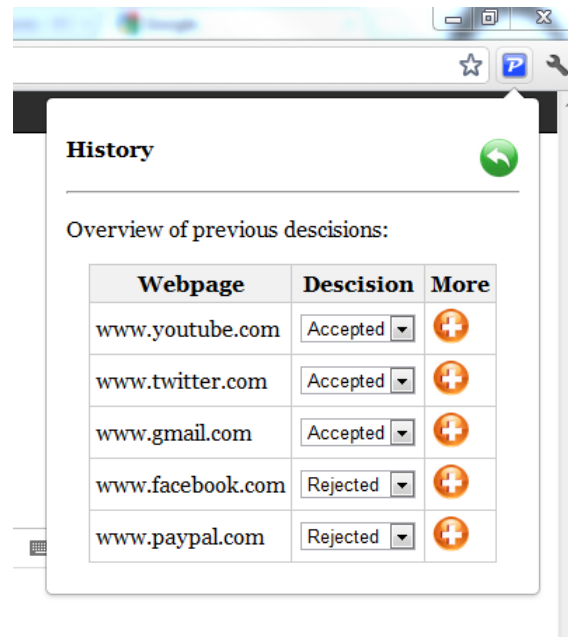


Figure 5.9: The history page in Privacy Advisor

### 5.4.6 Design Expansion

The design suggestion also allows for expansion for additional menu selections, text or functionalities. Additional text would to some extent stretch the popup window until it reaches a certain size. When the window reaches this size it could make use of a scrollbar to present additional information.

The main menu also allows for easy expansion with more choices, without changing the aesthetic structure of the menu. An example of the menu with an additional menu selection can be seen in Figure 5.10.

## 5.5 Use of Design Principles

The theoretic background presented in Chapter 2.5 was used as guidance when developing and making decisions on the design. This section will describe how each of the 10 usability heuristics from the theoretical background has been addressed in this design.



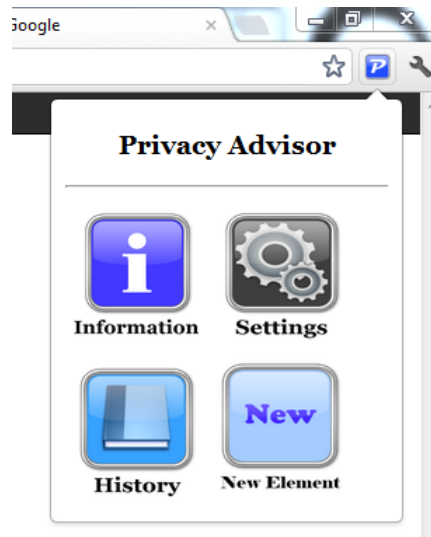


Figure 5.10: Expansion of the main menu

### 5.5.1 Visibility of System Status

The status of the system is presented to the user through the icons placed in the browser and when the system changes state, the icons change accordingly. Each icon also has its own window indicating the state of the system. For example when the system's logo is presented in the browser the main menu is present in the window, indicating that the system is in a general state. When the system is not able to evaluate a page or some error occurs, the system will show a message indicating this in the window and the icon changes to blue with an exclamation mark. The same applies for the advices where the advice decision is indicated with a icon.

In the settings in Google Chrome you can also see whether the system is active or inactive, and choose to change it. This affects whether you want Privacy Advisor to be running or not. Because of this the system status should be visible for the users.

### 5.5.2 Match With the Real World

The second usability heuristic states that there should be a match between the system and the real world, and that the user should be presented with familiar words and concepts. This is avoided by not using advanced language and offering a simple explanation on the system in the information window. The menu is also created by using self-explanatory words together with an icon with a descriptive image in order to make the menu intuitive.

### **5.5.3 User Control and Freedom**

User control is maintained by giving the user the opportunity to be able to always navigate backwards to the previous page if the wrong buttons is pushed. The user will also always be given the opportunity to change the decision made on a advice by going to the history of the program and change it there. The system then allows the user to change his mind several times, hence be in control of the system.

### **5.5.4 Consistency and Standards**

This point is maintained by having the different advices windows look similar. Consistency is also maintained by having the same graphical expression in the rest of the windows and having the different elements placed in the same place. The meaning of the buttons and icons are also always the same throughout all the different windows in the design. The same fonts and color schemes are used throughout the extension.

### **5.5.5 Error Prevention**

The most common error for Privacy Advisor as of now would be the general error message indicating that the system could not provide the user with an advice, for example because the webpage did not have a machine readable privacy policy. This is a short and simple error message indicating that the system could not fulfill its intended function.

Other possible error messages would be standard error messages controlled by Google Chrome when uploading the extension in the browsers settings, and this is not related to the actual program and can not be controlled by extension developers.

### **5.5.6 Recognition Rather than Recall**

Since the user should be spared from memorizing actions and options in the system, buttons, choices and words are chosen in order to try to make it intuitive. The different buttons have text or an icon that should be familiar for most people, to allow the user to recognize the right choice rather than memorizing it.

### **5.5.7 Flexibility and Efficiency of Use**

This point states that one should give experienced users shortcuts. Privacy Advisor does not provide that many functions, neither is the navigation big or complicated. The information and additional details for advices is placed behind a button, so the

extra information can be seen by the ones that wants to see them. This allows the ones that are not interested to not be bothered by it.

### **5.5.8 Aesthetic and Minimalistic Design**

Irrelevant information tried avoided and the design kept simple. The KISS principle is maintained throughout the design. No irrelevant images or details are used in the design and the color scheme is the same throughout the extension.

### **5.5.9 Recognize, Diagnose and Recover**

This point states that error messages should not be given in code and should be expressed in plain language precisely indicating the problem and suggest a solution to it. The handling of error messages are already described in Section 5.5.5. The solution for the failed evaluation of a webpage is solved by the user giving its opinion on the page so the program can still learn from it.

### **5.5.10 Help and Documentation**

The users who need extra help and documentation is guided to the information as described above. The details of the advices of the webpages are also given to the user that needs and wants it by looking at the details.



# Chapter 6

## Usability Testing

In this chapter I will explain the testing phase in terms of the test plan and execution. I will also present the results and observations done during the tests and render the results from the questionnaire.

### 6.1 Test Plan

The methods used for the usability tests are already described in Chapter 3. Here follows a more thorough description of the tests and the actual execution.

#### 6.1.1 Test Goals

There are two main reasons for performing usability tests on the prototype of the interface design for Privacy Advisor. One of them was to check the usability and to see if there were any problems in the design, or so called breakdowns [30].

Problems would typically be elements like buttons or representation of text that are not intuitive for the user and which the user would have problems understanding. Observing how the user navigates and communicates with the program was also important when evaluating the HCI of the system. Determining the usability of the design will consist of determining the efficiency, effectiveness and satisfaction of the design as explained in Chapter 2.5.1.

The second reason for testing was to see what relationship users have to privacy and information sharing online. The main objective was to identify how users act and think about privacy topics and their worries concerning them. These issues are important for assessing further realization and the potential of Privacy Advisor.

### 6.1.2 Test Subjects

According to Jakob Nielsen et al. [35], three to five test subjects is the optimal number for most usability studies. It is said that most faults or breakdowns in a system is found with this amount of test subjects, henceforth referred to as participants. In order to get more statistically correct feedback or to be able to say something about tendencies among the users, a bigger number should be used for the questionnaire.

After encouragement from my supervisor it was decided to try to reach 20 participants, since the answers could start to become normal distributed and more statistically reliable. In the end I reached 19 participants.

The participants were all people I already knew and mostly students. This might not be the optimal variety or number of people to make statistically accurate conclusions on quantitative data, but will still give some indication on tendencies. As for the usability part, 19 people would reveal most breakdowns in the prototype.

### 6.1.3 Test Introduction

Before the test was started, the participants were given a short introduction to the system and the procedure of the test and to build confidence. The participants were given a short introduction to the system, what it was supposed to do and where it could be found. Different terms like privacy policies were also clarified in order to increase the user's understanding.

They were also informed that the program they were going to test was still a prototype with certain limitations and not a finished product. For example, sometimes webpages had to be refreshed or loaded two times in order for Privacy Advisor to react.

Further the participants were instructed to think out loud and try to explain the choices they made and announce when they felt finished with a task. In order to prevent the users from becoming uncertain, they were told that they could press whatever buttons they wanted and would not damage anything by doing so. I explained that the intention were to test the system and not them.

I also explained my role during the test; that I was there for observing and could not help them complete the tasks, but rather to help solving ambiguities. In the end there were room to answer questions, and the participants were asked one more time if they wanted to go through with the test.

### 6.1.4 Execution

The tests were conducted during the month of April. Some of the tests were conducted at NTNU in Trondheim, and some in my hometown Tromsø. Each test took

approximately 20-30 minutes depending on the time the participant used on the tasks.

The test was performed in two parts. The first part concerned performing some practical tasks in the browser and with Privacy Advisor, and the second was to fill out a questionnaire which was available online. The practical tasks were chosen to reflect the user scenarios used for development of the design, including visits to relatively familiar webpages that offers or requires user accounts to fully use the service to try to make the tests somewhat realistic. The questions in the questionnaire were chosen to identify problems in the design and the need for both improvements in the design and the need of Privacy Advisor. Both the tasks and the questionnaire are represented in full detail in Appendix A.

The practical tasks were performed with me as an observer, making notes on observations. The participant were then let to fill out the questionnaire alone, still having me available to clarify if there were to be any questions, but not as an observer.

### **6.1.5 Test Observations**

Things that were noted during the execution tests where different problems the participants had during the tasks like reactions, decisions or comments they had during the test. For example if a participant commented that he or she did not know which buttons to push or did not understand something, that was noted. It could also be the time spent on a task, errors that appeared, comments from the participants or if the participant failed to complete a task in the intended way. The findings are presented later in this chapter and are then discussed and evaluated in Chapter 7.

## **6.2 Testing**

The executed tests are described in this section. This includes the results and observations from all the tests.

### **6.2.1 The Pilot Test**

Before the testing started a pilot test [22] was conducted. What distinguishes the pilot test from the others is that it allows for a final evaluation of the test plan, the system and the questionnaire before fully starting the actual tests. In other words, a pilot test is a "test of the test", the first one conducted. The point of the pilot test is to evaluate all the aspects of the test plan.

Conducting a pilot test allows for checking the clarification of questions, instructions and assignments to see if the participants will understand the meaning of the tasks given and the system. It also allows for the "tester" to practice one the execution and guidance. In addition, it is a golden opportunity to find and fix the last bugs in the system and design.

This test will in the end provide a better product for the actual testing and result in a more accurate and suitable test plan. Since the focus is on the users, you are more likely to improve the test plan to suit their needs.

In the pilot test for Privacy Advisor all of the mentioned aspects were evaluated and to some extent improved before further tests were performed. Some bugs in the software were discovered and fixed. For example Privacy Advisor did not react when entering `www.twitter.com`. The participant also showed some confusion with the tasks he was given, so they had to be reformulated and clarified. The introduction to the test and the system were also improved, since the participant showed some confusion when approaching the system as well.

### 6.2.2 Usability Test Results

The different things noted during the tests are summarized in paragraphs by the tasks that were performed while the event was noted. The tasks can as already mentioned be found in Appendix A, but are also included here for the sake of simplicity. The findings listed are then further discussed and used for improvement of the design in the next chapter.

**1. Open Privacy Advisor and read about how the system works.** Many of the participants went directly into the information option first and read the text presented there, as was the intended action. In addition, some of the participants went to the settings and history, and some even changed the settings to their preferences.

**2. Browse to twitter.com. Check Privacy Advisor's advice on how the page should be handled, and provide your feedback in Privacy Advisor.** Twitter was a page recommended accepted by Privacy Advisor and all users accepted the page regardless of whether they had a relation to the page or not. Some of the first tests performed had some technical problems, and Privacy Advisor would not react. The participant was then asked to continue on to the next task. Some of the participants also had difficulties recognizing Privacy Advisor when the icon had changed to the green symbol. A few on the other hand had difficulties understanding the meaning of accept and reject, and what happened when they pushed the buttons.



**3. Browse to linkedin.com. Evaluate the page in the same way as before.**

LinkedIn was also safely recommended by Privacy Advisor and most of the participants agreed, even though many of them did not use it or was familiar with it. One of the participants said that he accepted LinkedIn because it appeared to be a professional network. A user that did not already have a user account on LinkedIn said that he would have wanted to see the pages privacy policy in Privacy Advisor.

**4. Browse to paypal.com and evaluate the page.**

PayPal was recommended rejected by Privacy Advisor. 11 people overruled the advice, while eight people followed Privacy Advisor's advice. Some of the participants reacted to this, and became skeptical since they used PayPal. Most people who accepted the page used it regularly, while the ones who rejected it did not have any relation to it. Some also stated that the meaning of accept and reject button was unclear when the system advised them to reject the page. They were uncertain if accept in this context meant to accept the system's advice to reject the page or accept the page as in the previous cases.

**5. Browse to facebook.com and evaluate the page.**

Facebook was also recommended rejected by Privacy Advisor. All participants had a user account on Facebook, but only four people agreed to the advice, while 15 overran the advice. All participants were aware that Facebook is a page where a lot of information is shared among users, but many stated that they are very restricted regarding what information they share. At the same time some of the participants wanted to see more details on why Facebook should be rejected, than were presented in the advice (and in the details for those who looked at it).

**6. Go to Privacy Advisor's history and change the decision on gmail.com if you think this is the right thing to do.**

Going to the systems history appeared to be a very straight forward step. 17 participants let Gmail be accepted, because they already had a user account and trusted Gmail. Only two participants saw the details provided for Gmail, saying that Gmail should be rejected. They then took this advice into consideration and rejected Gmail.

**7. Browse to youtube.com. Check the details to Privacy Advisor's advice on the page before evaluating it.**

Many of the participants rushed through the task and accepted the advice when Privacy Advisor recommended YouTube, without looking for additional details. Some of the participants found the details button, but many had already pushed the details button in the previous task. One of the participants stated that the details button was not intuitive, but he understood the

meaning of it since there were no other choices.

**8. Go to Privacy Advisor and explain what you think the different settings mean.** Most users understood the meaning of "number of policies for comparison" and the weighting. The high and low level of privacy on the other hand were more difficult to understand. Several of the participants thought the levels indicated in percentage how many webpages the program had, or would recommend accepted or rejected.

In addition some of the participants also said that the program was very easy to navigate in, and that they liked the availability of it. They appreciated that they could interact with Privacy Advisor in the browser without interrupting the work in progress in the actual browser.

## 6.3 Results from the Questionnaire

The results from the questionnaire are presented in the following subsections. The results are presented in the same order as the questions were asked in the questionnaire.

### 6.3.1 User Statistics

The gender of the participants where quite evenly distributed, with 11 women and eight men out of 19 participants. The age distribution showed that 17 out of 19 were between 20-34 years old, while the two last participants were between 35-50 years old. This can be seen in Figures 6.1 and Figure 6.2.

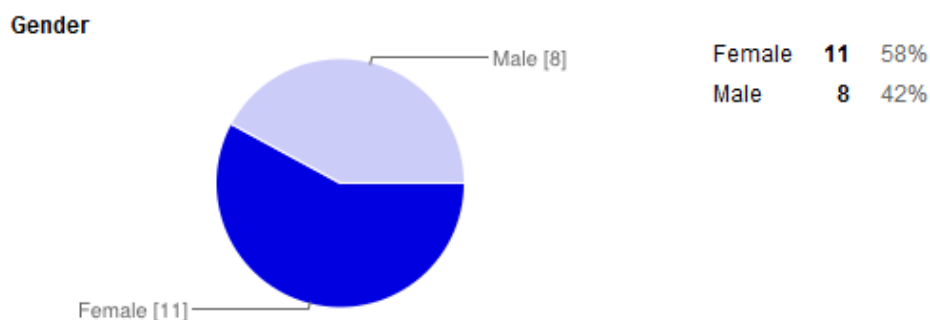


Figure 6.1: Gender of participants

When answering how often they used the Internet, all 19 answered every day. While describing what they used the Internet for, email, social networks, news and

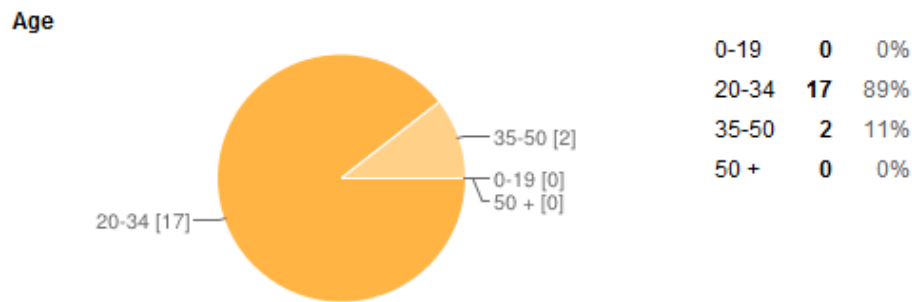


Figure 6.2: The age of participants

work or school related work was often repeated. Some also stated that they used the Internet for gaming, video or TV, banking services, shopping, music and chatting. All 19 participants said that they participate in social networks online, while 15 out of 19 use the Internet for shopping and 16 out of 19 use Google services that require a user account, as shown in Figure 6.3 and Figure 6.4



Figure 6.3: Results on Internet shopping

### 6.3.2 System Related Feedback

On system related questions, the participants were first asked what they thought about navigating in the program. 14 stated that they thought it was easy, while five thought it was ok, but sometimes it was unclear which buttons to push. The result is graphically represented in Figure 6.5.

As can be seen in Figure 6.6, 13 liked the design, two found it ok, but it did not appeal to them while four did not have any opinion about it. No one stated that they did not like the design.

The thoughts on the system's visibility were more scattered. Ten participants thought the visibility was suitable, six thought it sometimes was difficult to notice the program, one said he did not notice the program, while two clearly stated that the



Figure 6.4: Results on using Google’s services

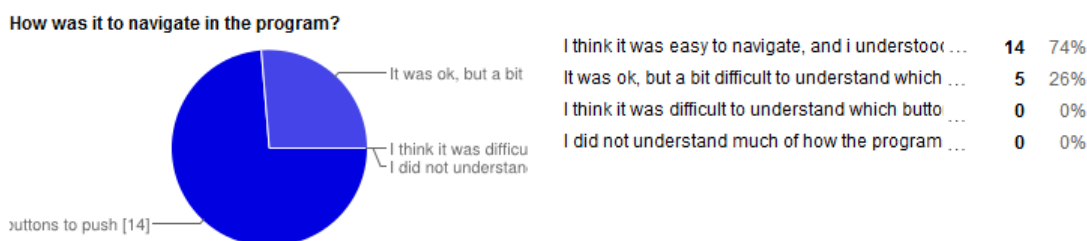


Figure 6.5: Results on navigation

system should be even more visible. No one thought the visibility were disturbing. The results are graphically represented in Figure 6.7. When asked if they noticed the icons change, all 19 said yes.

Further, when asked if they felt they could trust the program, the answers were widespread. Seven participants said yes, six said only in some cases, four did not know if they trusted the program and two said no. The results are presented in Figure 6.8.

Further, when the participants were asked if Privacy Advisor helped them make decisions many of the participants said that it was mostly helpful on webpages they did not already know of, but that the program made them more critical and aware of which information they shared online. Many of the users said that they based their decisions on their own experiences and opinions, in addition to what Privacy

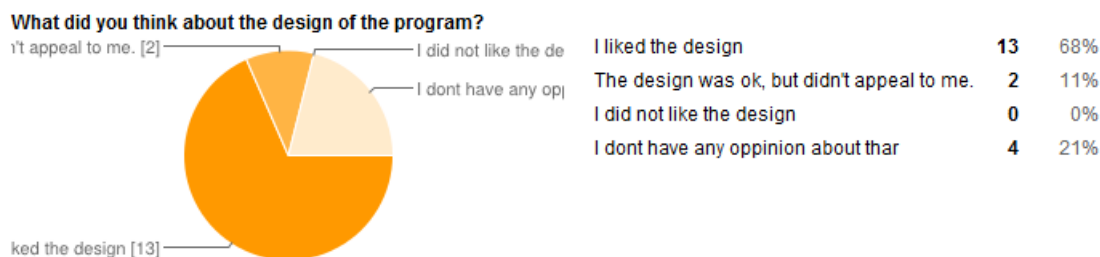


Figure 6.6: Opinions on the interface design



Figure 6.7: Results on visibility.

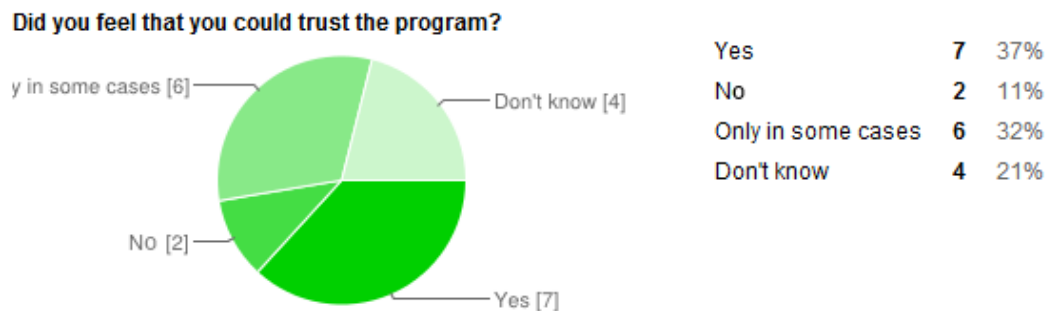


Figure 6.8: Results on trusting the program

Advisor had to say. One said that it was easier to accept a website if Privacy Advisor agreed, but when Privacy Advisor disagreed the user became more skeptical. It was also stated that the additional information provided on each webpage evaluated was helpful. One stated that he did not trust the program because he did not know how it handled his information.

The final question in this part concerned the advice given on Facebook, whether it was accepted or rejected and why. The ones that accepted Facebook said it was because they already had a user account and wanted to use the service Facebook provided independently of the privacy provided. Some said that they were aware of what information they shared and did not have any negative experiences and therefore trusted Facebook, but liked the additional information given in the program. One stated that Facebook should be accepted because so many users use it and therefore it must be reliable.

The ones that rejected Facebook said it was because they did not trust what Facebook might do with their information or because they would not want to accept other pages with similar privacy policies as Facebook.

### 6.3.3 Privacy Related Feedback

The last part of the questionnaire concerned privacy related topics. Here the participants were asked what they associated with the word "privacy". All of them answered protection of data and control over who has access to their private data. Further they were asked two questions on sharing information online. When asked if they worried about the information they provide online, 17 out of 19 said yes, while two said no or that they had never thought about it. On the question concerning how much they think about what kind of information they share online 12 answered often and seven said sometimes. The results are represented in figure 6.9 and Figure 6.10.

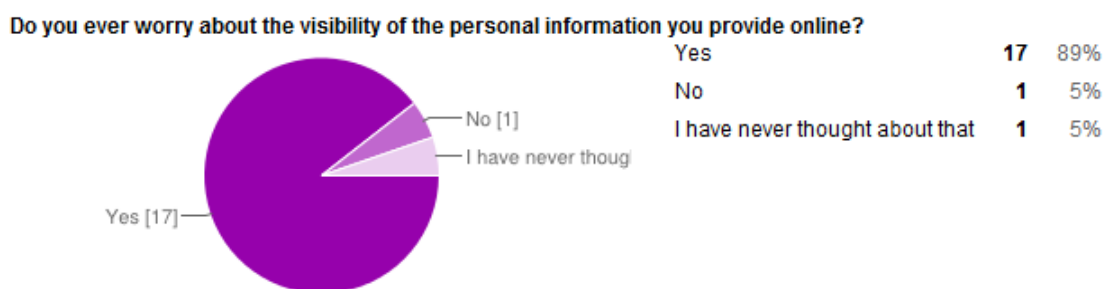


Figure 6.9: Thoughts on information sharing

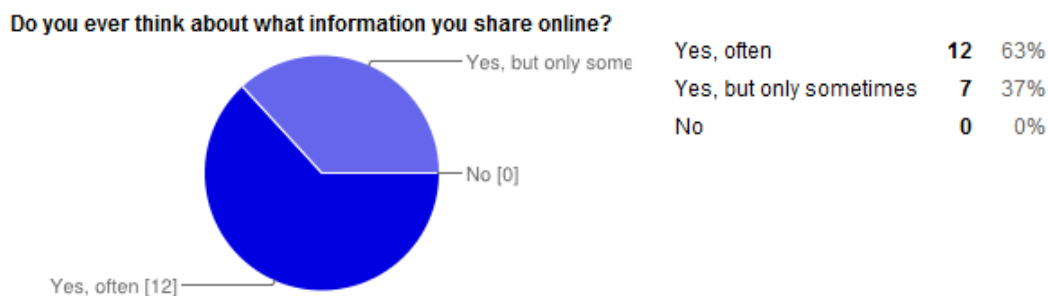


Figure 6.10: Thoughts on shared information

When asked to describe things the participants thought could go wrong when sharing too much information many expressed concerns about pictures they share online, typically on Facebook. Some also expressed concerns about identity thefts and bank account information that can be stolen and misused. A few also said that targeted marketing and phone sellers was a concern they had by sharing too much information online. One in particular expressed the following concern when asked this question:

*"I have actually no idea, and feel sometimes I can do nothing against providing the information. I find it very annoying, for example when applications that you*

*download for your smart phone always require some kind of information, and you can not install them unless you accept all of them. Also I believe the information can be hacked and stolen, as has happened several times before”.*

This statement actually illustrates the concern many of the participants had to privacy on the Internet.

When asked if they read privacy policies when creating user accounts online, whereas 14 said no and five said sometimes, see Figure 6.11. They were also asked if they would use a program like Privacy Advisor (a modified version of the one they tried), ten said yes, seven said maybe and only two said no, as seen in Figure 6.12.

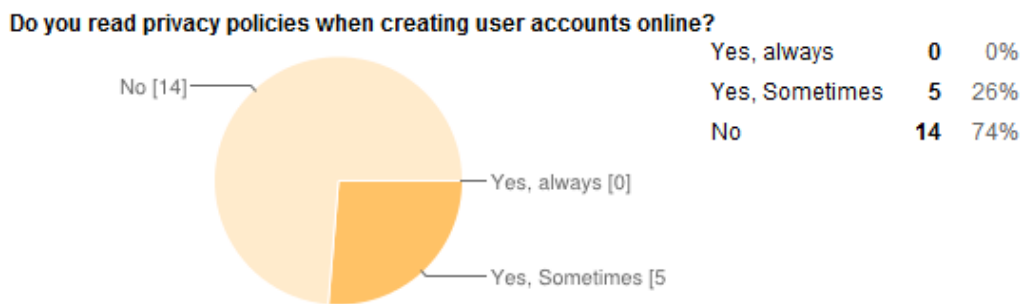


Figure 6.11: Results on reading privacy policies

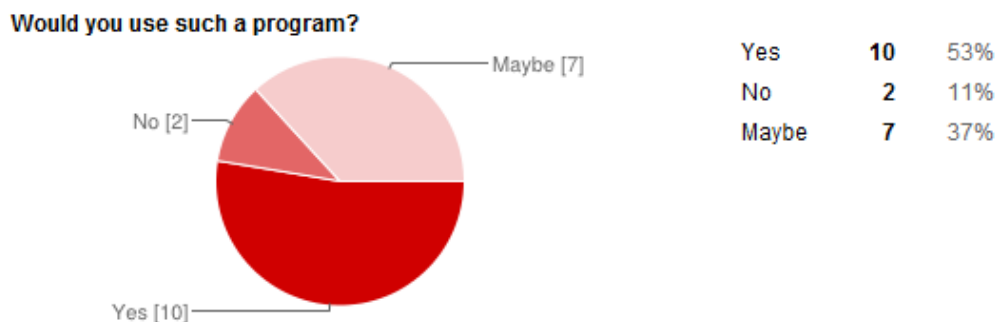


Figure 6.12: Thoughts on using Privacy Advisor

In the end the participants were given the opportunity to provide some additional thoughts and comments. Here participants commented that they thought it is important with such a program, since most people don't read privacy policies on the Internet. They also said that the program should be more visible when a page is recommended rejected, because in this setting they were focused on the icons, but that they might not notice them in another setting. One also wanted to know more of how the program actually worked in the background, because he did not understand much of it.





# Chapter 7

## Evaluation and Discussion

In this chapter I will discuss the suggested design based on the results from the tests and on how the system's learning process works. Improvements to the design will also be made and presented here.

### 7.1 Test Results

The purpose of the tests was to check the effectiveness, efficiency and to some extent also the satisfaction of the suggested design. In other words, the tests were conducted to check if the design worked. The results showed things that worked well, but also things that needed to be changed or improved.

#### 7.1.1 Functioning Design Elements

The navigation in the program got good feedback, and the majority of the participants said it was easy and straight forward. No remarkable problems in navigation were noted, apart from the details button which was not intuitive or not noticed. This is both discussed and fixed later in this chapter. It also seemed like the menu had very obvious choices where the participants went directly to the selection intended. The participants also expressed optimism to be more observant to privacy and security, and felt like the system could have importance.

They also liked that the advices and the information given from Privacy Advisor did not disturb the work they had going on in the browser. Positive feedback was also given on the icons in the browser. The participants felt that they were nice looking with a simple design and not too ostentatious in the browser.

These are all things that are considered as important factors of the design and have therefore remained unchanged or only gone through minor changes.

### 7.1.2 Further GUI Improvements

One thing that appeared to be a challenge was the "accept" and "reject" buttons in the advices. There were sometimes confusions on what accept and reject meant when the advice said that the webpage was unsecure, whether it was to accept the web page or accept the advice given by Privacy Advisor. This appeared to be a "breach" of the usability heuristic on match with the system and the real world presented in Chapter 2.5.3, because the user did not recognize the meaning of the buttons.

This have now been clarified by replacing the accept and reject buttons with the question of whether the user trusts the web page. By asking the user if he or she trusts the webpage, the misconceptions from the tests should be avoided, since the meaning of the question should be implicit and applicable in all situations. The new solution can be seen in Figure 7.1.



Figure 7.1: The new advice window

Another thing the users pointed out was the visibility of the system. Nine of the participants indicated that the system's visibility had to be improved. The rest of them said the visibility was suitable, but this might be because they were paying special attention to the program during the tests, and would probably not notice it otherwise. Since the focus during the test was on Privacy Advisor, one has to consider the fact that it is unlikely that the same applies outside the testing environment.

It is therefore suggested to increase the system's visibility to some extent by making the advice window open automatically when entering a new webpage for

the first time, and thus make it fit better with the heuristic on visibility of system status from Chapter 2.5.3. Once feedback is given on a webpage the advice should not appear again. It could also be an idea to have a reminder when entering a webpage that one already expressed one did not trust. This would however be an issue if you reject Facebook because you don't want to trust similar pages, even though you continue to use Facebook, as was the case with one of the participants in the tests.

Some of the users also had some problems understanding the meaning of the details button, as it was a plus sign in an orange circle. In other words was the affordance of the button not good enough. It was therefore decided to change the button to a normal colored link, using the word "details+" to indicate its purpose. The link should provide better affordance as the use of descriptive links is normal. The new solution for the detail button can also be seen in Figure 7.1.

The history window also went through some small changes, these including changing the details buttons to the same link and also changing the choice from "accepted" and "rejected" to "Trusted" and "Not Trusted". This was done to keep the windows similar and consistent with the changes in other windows as encouraged in the usability heuristics. Besides this, the rest of the window remains the same. The changes in the history window can be seen in Figure 7.2.

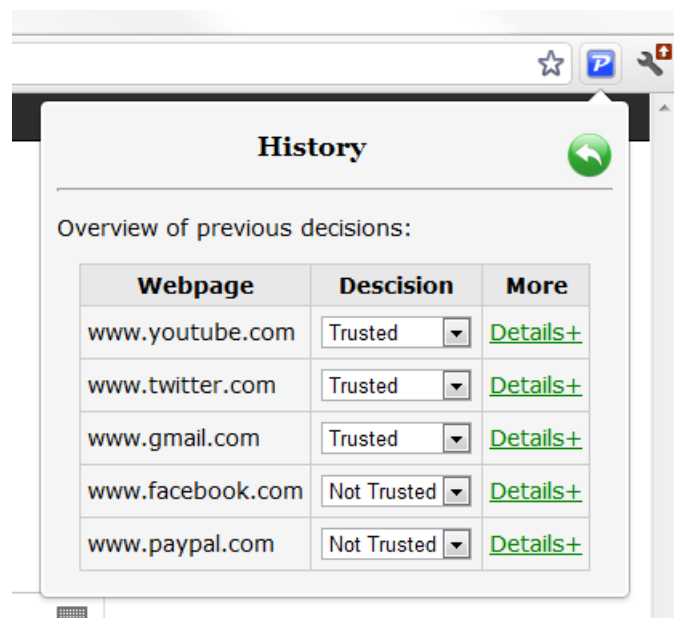


Figure 7.2: New history window

The participants were not asked to use the comment field, but some minor changes were made on it as well to make it look a more aesthetically pleasing. This can also be seen in the new advice figure (Figure 7.1).

### 7.1.3 Information to Users

Some users said that they would prefer to gain more information on why the webpages should be trusted or not. The only information already provided in an advice was the encouragement to either accept or reject a webpage, the level of privacy and what other pages was treated information in a similar manner.

In response to this, and by request from SINTEF ICT and some of the participants, a new functionality was added to the program. The ability of reading the current webpage's privacy policies in Privacy Advisor is now added. On the details-page advices you can click on a link that will open and show the entire privacy policy in the window. A scrollbar is also added to the window to avoid the window of expanding over the whole screen, as privacy policies often are long texts. An example of this can be seen in Figure 7.3.

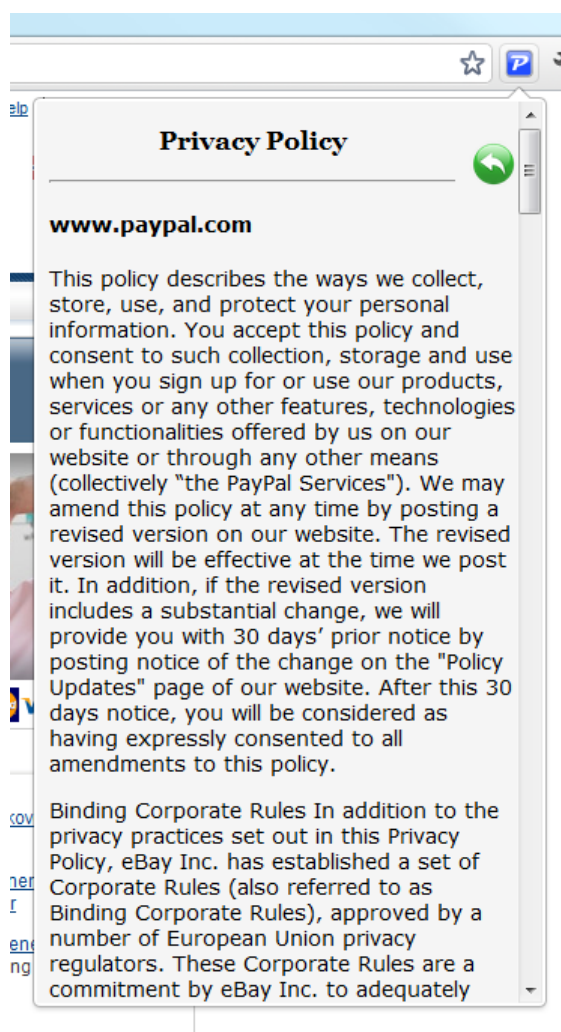


Figure 7.3: Privacy policy in Privacy Advisor

In addition, the text in the information window was simplified and a short description on how the advices and the user feedback work was added. This was done

to increase the users understanding of the program and trying to avoid confusing situations where the user don't recognize the program when the icons have changed, as was the case in some of the tests.

The participants managed to interact with the system in a good way without any special problems and showed an understanding for the programs intention. One thing that was of interest for some of the users were the understanding on how the advice engine works, but this might be because the participants were particularly technically interested students and this might not be as interesting for most people.

#### **7.1.4 The System's Learning Process**

As described earlier the system learns from previous cases by looking at the cases that are similar to the current one and based on the majority of these decides what the advice should be. The majority of cases are the  $n$  out of  $k$  cases that is most similar and gave the same advice. The percentage  $n$  makes of the  $k$  cases, is recognized as the level of confidence, and is used for expressing how certain Privacy Advisor is in the given advice.

In the design used for testing this percentage was called "level of privacy", and is now changed to "level of confidence" because this is more correct in accordance to the system's learning process. Also the meaning of "level of confidence" should be clearer for the user, as it is a more familiar choice of words and better match with the real world, just like the details button. This can also be seen in Figure 7.1.

Also the settings window went through some changes. Since the design used for testing provided the ability to adjust the percentage that would decide if an advice would be to trust a webpage or not. The reason for this was some confusion from my side on how the system worked and this option is now removed, since it in reality is something that can't be adjusted by the user. The new settings window can be seen in Figure 7.4.

Due to the changes in both the accept and reject button and the settings, the text in the "undetermined privacy" page were updated. The text is now changed to be more correct to the changes mentioned in this subsection. The new feedback buttons are added and also the opportunity to add comments on the feedback. The comments were added in order to make the page more consistent with the rest of the program. The window can be seen in Figure 7.5.

## **7.2 The System's Usability**

In Chapter 3 on methodology it was stated that I was going to check the usability of the system and that the system's effectiveness, efficiency and satisfaction were to

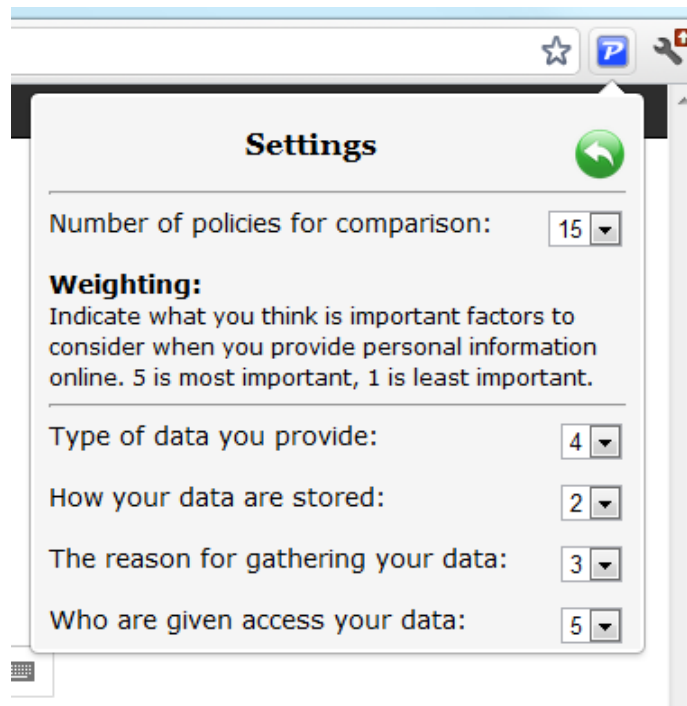


Figure 7.4: The new settings window.

be measured. I want to emphasize again that the tests were only conducted on 19 participants, which means that there are not really any good quantitative measures on the three parameters listed below. The results will still be used to say something about tendencies and to try to determine the usability based on the amount of data collected.

Based on the results and notes from the tests, the three could be measured and evaluated.

### 7.2.1 Effectiveness

The effectiveness of the system or to what extent the participants were able to complete the tasks given proved to be satisfying. All users were able to conduct all the tasks given and no one interrupted the tests due to frustration or incompetence to complete a task. Some users had to be given a little hint in the second task, but I believe that this is because few of the participants had experiences with Google Chrome Extensions or even privacy programs such as Privacy Advisor. Once an experience is made with an advice, the most advance function of the system is learned. In other words, the effectiveness of the program is thought of as good. Especially when minor changes or improvements were added to the design.

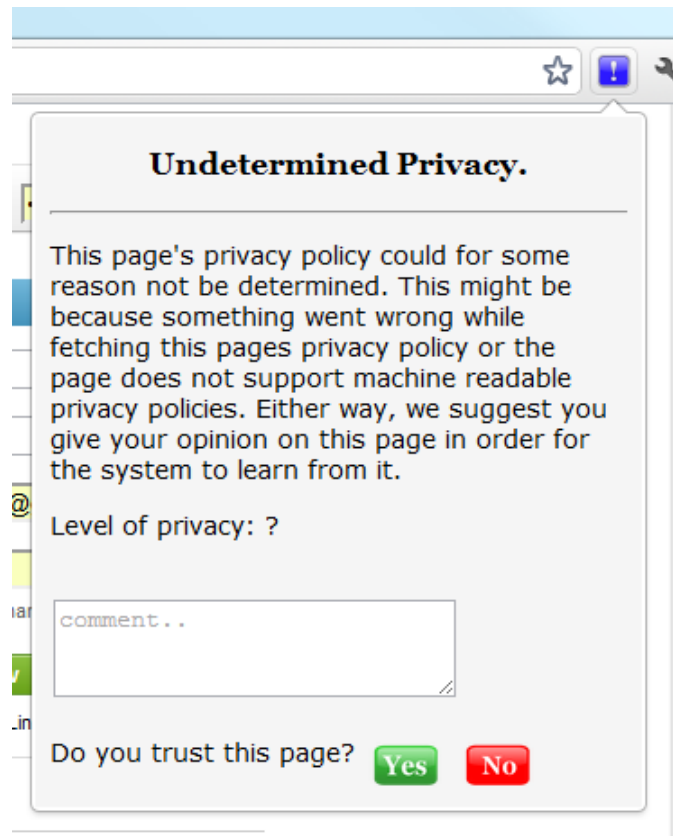


Figure 7.5: The undetermined privacy window.

### 7.2.2 Efficiency

The efficiency of the program and execution of the tasks were measured by looking at how fast the tasks were completed and registering if some tasks appeared to be very time-consuming. No special cases were noted, and most tasks were conducted within a reasonable amount of time. The only thing registered that made some of the participants stop and think twice were some of the design issues discussed and improved above, like the details button. When these are fixed, the efficiency of the program should also be considered as satisfying.

### 7.2.3 Satisfaction

At last there was the satisfaction with the system. Even though 2 of the participants said they would not use such a program and 7 said maybe, the rest said yes. The tests made the participants very aware and interested in privacy and security related issues. Many of the participants expressed that they thought the program was very useful and made them focus on their privacy, which they thought was very positive. Due to the positive feedback on the system, the effectiveness and efficiency of it and the results from the tests, the system's satisfaction is also considered as adequate.

## 7.3 Validity of the Tests

Even though tests have been conducted in order to improve the design, determine the usability of the program and look for tendencies on privacy related topics, it is not given that the results are 100% reliable or correct. It is therefore important to consider the results with a critical eye.

### 7.3.1 Selection of Participants

The participants mainly consisted of friends and acquaintances that agreed to test the program. The distribution in age could have been better, since most of them were students and a bigger variety of age could have given a more realistic outcome that better represents the tendencies among most people.

The same applies for the background of the participants as most of them were students, whereupon most of them were studying within the fields of science or technology.

When it comes to the number of participants used in the tests, 19 should be more than enough when looking purely on usability testing. Most breakdowns were discovered after approximately 6-7 participants, while the same breakdowns were repeated for the rest of the participants. When looking at the statistics for the questionnaire on the other hand, even more users would be desirable in order to make the results more statistically correct as described in Oates [27].

The process of finding and recruiting participants for the tests could preferably been better planned in order to get a bigger variety and amount of people, with respect to both age and background, which in turn better represents society.

### 7.3.2 Validity of the Results

The actual results produced should be taken with a portion of reasonable judgment. For example, the participant can be inhibited from acting as they would under normal circumstances because they are asked to perform predefined tasks under observation. The possibility of the participants' acting as they think I want them to, rather than how they normally would are definitely present, as described in Chapter 3.4.2 as the Hawthorn-effect.

The same applies when answering the questionnaire, even though the received results were anonymous. The fear of doing something wrong or being perceived as stupid could also affect the participants during the tests.

This will however always be the case when conducting usability tests on other people and is therefore difficult to avoid. It is therefore not considered as a big problem in this case, but the results are still being evaluated with reasonable judgment.



### 7.3.3 Tasks and Questions

When planning tasks and questions for use in research, it can be easy to be wiser after the event, concerning the tasks given and the outcomes or results from the research. This meaning that after the results are gained and interpreted, one often think that one could have reformulated the questions or the alternative answers to better fit the direction of the research to gain better statistical results. This could even happen, despite good planning.

This was also the case in this work. Some more time could have been used while planning the tasks and questions, in order for get better quality of the results. This was the case for some questions in these tests as well. For example when asking the age of the participants, the alternatives were quite broadly divided leading to difficulties in saying something useful on age differences. This could in this case also be due to the selection of participants, but could still have been improved.

The same applies to how often the participants used the Internet. If I knew that everyone would answer "every day", I should have provided more specific alternatives for answers. Even though some questions or answers could have been improved, I still find the results satisfying in terms of usability and developing the design which was the main focus of the tests.

When it comes to the practical tasks that were given on the system it might be an idea to include some less familiar webpages to the tests, to see if the users really use Privacy Advisor for help or if they only base their decisions on their own experiences. Even if familiar webpages were added to see what is really important for the users, service or privacy, some of the tasks could have been revised or some extra tasks could have been added. Still, I think most of the breakdowns were found and Privacy Advisor's potential was shown.



# Chapter 8

## Future Work

In this chapter I will present some ideas for future work based on the work done and presented in this thesis. These are ideas I had during the work on this thesis and should only be considered as inspiration rather than a definite future plan.

### 8.1 System Improvements

There are some ideas for improvements of the system; one includes functionality and one on the design.

#### 8.1.1 Additional Features

As of today, there is no embedded functionality to withdraw specific policy data from the system's advice engine, but it would be an idea to implement this because it would give the user the opportunity to get concrete statements in the advices on why a webpage not should be trusted. These statements could also be affected by the weighting of what elements the user thinks is important. For example, a user that thinks data collected for the purpose of telemarketing is unacceptable would weight purpose as an important factor to consider when comparing policies. The user would then probably appreciate to receive a warning if the webpage is looming to sell the users information to telemarketing firms. The potential statement could be something like this;

"This page does not take care of your privacy in a good way and should not be trusted because: - This webpage collect your information for telemarketing purposes and might sell your contact information to telemarketing firms."

### 8.1.2 GUI Improvements

The interface design suggested is a fully functional design, but might need even more improvements in order to be adapted to the final product. Due to the lack of my designer abilities and experience, the graphical elements and the overall look of the program could be further improved in order to be more aesthetically nice.

The design should also be adjusted to include additional functionalities that might be chosen to be implemented. As discussed in Chapter 5.4.6 the main menu of the suggested design is flexible and can easily be extended to include more elements and thus more features or functionalities.

Since the program is not a finished product yet, this thesis only provide a suggestion for the interface design and it should therefore have a final improvement or walkthrough before it is used for the final product.

## 8.2 A Fully Functional Extension

At the time of writing the logic for Privacy Advisor is developed as a offline tool in Java, while the suggested design is implemented as an extension for Google Chrome using HTML, CSS and JavaScript. A suggestion for further work is therefore to connect the two and make them work together as a fully functional program.

There might be several ways in which this can be done. One solution could be to employ the existing logic as a web service running on a separate server and let the extension communicate with it. This would require the extension to stand for the interaction with the user and collect input from both the browser and the user, and then send it to the web service for further processing. The results would then be sent back to the extension to be displayed for the user. For example could the extension be responsible for retrieving the privacy policy and the web service for processing and creating the advice. The advantage of this solution is that the existing code in Java would not have to be "translated" into JavaScript or vice versa.

It is also possible to rewrite the entire code to one language, or even make Privacy Advisor work a program that runs locally on the computer and communicated with the browser.

## 8.3 Support for Other Standards

Today Privacy Advisor only support the P3P standard for evaluating webpages. The standard is not mandatory in any way for websites or service providers to use, and this might affect the overall usability of Privacy Advisor if it won't work on important webpages because the service provider decided to use another standard.

As mentioned in Section 2.2.2 there exists several additional privacy policy standards that could be implemented in addition to P3P, to cover a wider range of webpages that can be evaluated by the program. This is therefore suggested as a potential expansion of Privacy Advisor in order to make it better and more functional.

## **8.4 Additional Security Functionality**

As of today Privacy Advisor's functionality is mainly concentrated on giving the user advice on different websites privacy policies. In order to make the program even more attractive on the market among all the other tools on the market, one possibility could be to add even more privacy and security functionality to it. The reason for this suggestion is that users would probably not use a program for each functionality, and would therefore choose the tool that best suits his or her needs or covers most of the wanted functionality.

Since Privacy Advisor now is suggested to run in the browser, it would be most appropriate if the new functionality would be possible to implement and run from the browser as well. Suggestions for additional functionalities could be one or more of the following.

### **8.4.1 Delete Cookies**

In Section 2.1.2 it was barely mentioned that cookies can be a privacy concern because they store information about a user that can be used on a webpage to identify or recognize a user. The information stored in cookies can be age, gender, buying preferences or maybe even email addresses [10]. The information can differ, but will not contain information that the user have not voluntarily provided at some point. Still, the users' preferences for information shared with others could change, and it can be to keep track of the information already provided online. The cookies are usually stored in the browser and exchanged with websites when visiting them.

A possible function can therefore be to delete cookies that are stored in the browser in order to maintain the user's privacy in one more way.

### **8.4.2 Erase History and Temporary Files**

One can also say much about people by looking at their activities, because they sometimes reflect on a person's interests and daily routines. A lot of information is stored in the browser from such activities, for example all the webpages and links visited or downloaded files.

A second possibility would therefore be to delete all history and temporary files in a browser, in order to clean all traces of a user's Internet activity and maintain the user's privacy.

### **8.4.3 Malware Scanning**

The last suggestion is however somewhat different from the other two, as it is more focused on security in general and not necessarily privacy. This includes the ability to scan elements on the Internet for malware in order to prevent the user from getting affected by them. This could work by scanning links in search results like Privacy Finder did or scan the visited webpage for infected elements and warn the user about the findings. Some of this functionality is already implemented in some anti-virus programs today and is working quite nicely.

This idea would however cause some extra work in order to implement new logic and functionality for the program, but would result in valuable functionality for the user.

# Chapter 9

## Conclusion

In this thesis I have provided a design suggestion for Privacy Advisor. The design have been reached through prototyping and usability testing, where feedback from SINTEF ICT and potential users have been important factors in improving the design. Two prototypes were developed, where feedback from the first were used to improve the design into an extension, which were used for usability testing. The test results were then used for the final improvements and evaluation of the design.

The test results and feedback showed that there were some breakdowns in the system which needed to be improved or fixed. These were mainly representation of text or buttons that were not intuitive enough and therefore created some confusions and misconceptions. Still, the tasks given during the tests were completed within reasonable time and nearly as intended. In addition the usability was decided as good based on the data collected.

Further, the degree of user involvement also appeared to be reasonable as the suggested design allows the user to interact more efficiently with the program than the original UIs did. This conclusion is also based on the fact that the participants did not show any signs of annoyance while interacting with the program during the tests. The user is given the opportunity to provide some of his preferences to the system when it comes to weighting, but the user is not required to and it's not a laborious task. The interaction is also adapted to suit the learning process of the system, at it is also described for the user in the program.

The potential of Privacy Advisor as a working program is definitely present based on the results, but how it will do on the marked is somewhat more difficult to decide. Here Privacy Advisor would have to compete with many similar programs providing different functionalities. However, Privacy Advisor is obviously useful as reading and interpreting privacy policies is a lacking activity among people using the Internet.

Based on the results and the final improvements on the prototype I believe I have provided an adequate response to this thesis.





# References

- [1] Martin Gilje Jaatun, Inger Anne Tøndel, Karin Bernsmed, and Åsmund Ahlmann Nyre. Privacy Enhancing Technologies for Information Control. In *Privacy Protection Measures and Technologies in Business Organizations*, pages 1–31. IGI Global, 2012.
- [2] Karin Bernsmed, Inger Anne Tøndel, and Åsmund Ahlmann Nyre. Design and Implementation of a CBR-based Privacy Agent. In *To appear in Proceedings of the Seventh International Workshop on Frontiers in Availability, Reliability and Security*, FARES 2012, August 2012.
- [3] SINTEF. Homepage of SINTEF. [www.sintef.no/home](http://www.sintef.no/home). Web-page retrieved 12th of April, 2012.
- [4] Privacy Bird. The Webpage of Privacy Bird. <http://www.privacybird.org>. Web-page retrieved 9th of February, 2012.
- [5] IBM Open Collaborative Research Initiative. Open Innovation in Privacy and Security Policy Management. <http://projects.cerias.purdue.edu/ocrproj/enduser.html>. Web-page retrieved 30th of April, 2012.
- [6] Google Inc. Google Chrome’s Online Market for Extensions. <https://chrome.google.com/webstore/detail/mlomiejdfkolichcflejclcbmpeaniij>. Web-page retrieved 30th of April, 2012.
- [7] The Tor Project Inc. Tor - Anonymity Online. <https://www.torproject.org/>. Web-page retrieved 30th of April, 2012.
- [8] Datatilsynet. Hva er Personvern? <http://www.datatilsynet.no/personvern/Hva-er-personvern/>. Web-page retrieved 2th of May, 2012.
- [9] European Court of Human Rights. European Convention on Human Rights. <http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf>. Web-page retrieved 2th of May, 2012.

- [10] Winnie Chung and John Paytner. Privacy Issues on the Internet. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, page 9, 2002.
- [11] Facebook. Data Use Policy. [http://www.facebook.com/full\\_data\\_use\\_policy](http://www.facebook.com/full_data_use_policy). Web-page retrieved 8th of May, 2012.
- [12] VG Nett. Personvern-policy / integritetspolicy. <http://static.vg.no/policy/integritetspolicy.html>. Web-page retrieved 8th of May, 2012.
- [13] Erika Morphy. Privacy Policies: The Good, The Bad and the Witty. <http://www.ecommercetimes.com/rsstory/65618.html>. Web-page retrieved 10th of May, 2012.
- [14] Platform for Privacy Preferences (P3P) Project. P3P. [www.w3.org/P3P/](http://www.w3.org/P3P/). Web-page first time retrieved 16th of February, 2012.
- [15] Slim Trabelsi. Second Release of the Policy Engine. Technical report, Privacy and Identity Management in Europe for Life, 2010. Funded by the European Community's Seventh Framework Programme, for the PrimeLife Project.
- [16] Anne H. Anderson. A Comparison of two Privacy Policy Languages: EPAL and XACML. In *Proceedings of the 3rd ACM Workshop on Secure Web Services, SWS '06*, pages 53–60. ACM, 2006.
- [17] Stuart Russell and Peter Norvig. *Artificial Intelligence - A Modern Approach*. Prentice Hall, 2003.
- [18] Tom M. Mitchell. *Machine Learning*. McGraw-Hill, 1997.
- [19] Inger Anne Tøndel and Åsmund Ahlmann Nyre. Towards a Similarity Metric for Comparing Machine-Readable Privacy Policies. In *Open Problems in Network Security*, Lecture Notes in Computer Science, pages 89–103. Springer Berlin / Heidelberg, 2012.
- [20] Wikipedia. Hamming distance. [http://en.wikipedia.org/wiki/Hamming\\_distance](http://en.wikipedia.org/wiki/Hamming_distance). Web-page retrieved 24th of May, 2012.
- [21] Ben Shneiderman and Catherine Plaisant. *Designing the User Interface - Strategies for Effective Human-Computer Interaction*. Addison Wesley, 4th edition, 2005.
- [22] Dag Svanæs. Brukbarhetstesting. <http://www.idi.ntnu.no/emner/it3402/F6Brukbarhetstest.pdf>, 2001. Lecture notes from the subject TPD4134 - User Interface Design, lectured in the fall of 2011 at NTNU.

- 
- [23] Kristiina Karvonen. The Beauty of Simplicity. In *Proceedings on the 2000 Conference on Universal Usability*, CUU '00, pages 85–90. ACM, 2000.
- [24] Don Norman. Don Norman's Website. <http://www.jnd.org>. Web-page retrieved 28th of February, 2012.
- [25] Jakob Nielsen. Ten Usability Heuristics. [http://www.useit.com/papers/heuristic/heuristic\\_list.html](http://www.useit.com/papers/heuristic/heuristic_list.html). Web-page retrieved 28th of February, 2012.
- [26] Wikipedia. KISS-prinsippet. <http://no.wikipedia.org/wiki/KISS-prinsippet>, 2012. Web-page retrieved 13th of February, 2012.
- [27] Briony J. Oates. *Researching Information Systems and Computing*. SAGE Publications Ltd, 2006.
- [28] Michael D. Myers. Qualitative Research in Information Systems. *MISQ Discovery*, pages 241–242, 1997. Society for Information Management and The Management Information Systems Research Center.
- [29] Dag Svanæs. Prototyping og brukbarhetstesting. [http://dag.idi.ntnu.no/IT3402\\_2009/prototyping\\_brukbarhetstesting.pdf](http://dag.idi.ntnu.no/IT3402_2009/prototyping_brukbarhetstesting.pdf), 2009. Lecture notes from the subject IT3402, lectured in 2009 at NTNU.
- [30] Gry Seland. Vedlegg: Brukbarhetstesting v.h.a. Papiprototyper. [http://dag.idi.ntnu.no/IT3402\\_2009/Vedlegg%"20papirprototyper.pdf](http://dag.idi.ntnu.no/IT3402_2009/Vedlegg%). Document that was part of the curriculum in the subject TDT4180 Human Computer Interaction in the spring of 2011 at NTNU.
- [31] Norsk Nettlesikon. Hawthorne-effekt. <http://snl.no/Hawthorne-effekt>, 2009. Web-page retrieved 14th of March, 2012.
- [32] Inger Anne Tøndel, Åsmund Ahlmann Nyre, and Karin Bernsmed. Learning privacy preferences. In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pages 621–626, August 2011.
- [33] W3Schools. W3Schools Browser Statistics. [http://www.w3schools.com/browsers/browsers\\_stats.asp](http://www.w3schools.com/browsers/browsers_stats.asp). Web-page retrieved 17th of February, 2012.
- [34] Paint.NET. Paint.net a trademark from dotPDN LLC. [www.getpaint.net](http://www.getpaint.net). Web-page retrieved 16th of February, 2012.
- [35] Carol Barnum, Nigel Bevan, Gilbert Cockton, Jakob Nielsen, Jared Spool, and Dennis Wixon. The Magic Number 5: is it Enough for Web Testing? In *CHI '03 extended abstracts on Human factors in computing systems*, pages 698–699. ACM, 2003.

- [36] Google Inc. Google Chrome Extensions. <http://code.google.com/chrome/extensions/overview.html>. Web-page retrieved 30th of January, 2012. The webpage contains information on how to build Google Chrome extensions.

# Appendix A

## Testing Documents

This appendix will present in detail the documents used for the testing phase. It will show the exact tasks the participants were asked to perform and the questionnaire they were asked to fill in after the practical part of the test.

### A.1 Tasks for Usability Testing

The practical tasks for the usability tests were performed in the Google Chrome browser. The browser was already opened when the test started, and the participant was informed where the program was located and that everything during the test should be conducted in the browser, and only the browser. The participants were provided with a paper with a short introduction and some simple, but detailed tasks to perform. The papers content is cited below.

#### Tasks

If some of the webpages are unfamiliar to you, just ask and I can explain them for you.

1. Open Privacy Advisor and read about how the system works.
2. Browse to [twitter.com](https://twitter.com). Check Privacy Advisor's advice on how the page should be handled, and provide your feedback in Privacy Advisor.
3. Browse to [linkedin.com](https://www.linkedin.com). Evaluate the page in the same way as before.
4. Browse to [paypal.com](https://www.paypal.com) and evaluate the page.
5. Browse to [facebook.com](https://www.facebook.com) and evaluate the page.
6. Go to Privacy Advisor's history and change the decision on [gmail.com](https://www.gmail.com) if you think this is the right thing to do.

7. Browse to youtube.com. Check the details to Privacy Advisor's advice on the page before evaluating it.
8. Go to Privacy Advisor and explain what you think the different settings mean.

## A.2 Questionnaire

After the completion of the practical test with Privacy Advisor the participants were asked to fill out a digital questionnaire containing the questions listed below. The questions were a combination of multiple choices with alternative answers listed or questions that required text based answers. The form existed in both English and Norwegian, but only the English one is listed here since the Norwegian form contains the exact same questions, only in Norwegian.

### Participant related

1. Gender?
  - (a) Male
  - (b) Female
2. Age?
  - (a) 0-19
  - (b) 20-34
  - (c) 35-50
  - (d) 50+
3. How often do you use the Internet?
  - (a) Every Day
  - (b) 3-5 times a week
  - (c) 1-2 times a week
  - (d) A Few times a month
  - (e) Never
4. What do you usually use the Internet for?
5. Do you participate in social networks on the Internet?
  - (a) Yes

- (b) No
- 6. Do you use the Internet for shopping?
  - (a) Yes
  - (b) No
- 7. Do you use any of Google's services online? (Services that require a user account)
  - (a) Yes
  - (b) No

**Program Related**

- 8. How was it to navigate in the program?
  - (a) I think it was easy to navigate, and I understood which buttons to push
  - (b) It was ok, but a bit difficult to understand which buttons to push
  - (c) I think it was difficult to understand which buttons to push
  - (d) I did not understand much of how the program worked
- 9. What did you think about the design of the program?
  - (a) I liked the design
  - (b) The design was ok, but did not appeal to me
  - (c) I did not like the design
  - (d) I don't have any opinion about that
- 10. What did you think about the visibility of the program?
  - (a) I think the visibility was suitable
  - (b) At times it was hard to notice the program
  - (c) I did not notice the program
  - (d) I found the programs visibility disturbing
  - (e) The program should be more visible
- 11. Did you notice the icons change?
  - (a) Yes
  - (b) No

12. Did you feel that you could trust the program?
  - (a) Yes
  - (b) No
  - (c) Only in some cases
  - (d) Don't know
13. Did you feel that the program helped you make decisions? Why/Why not?
14. What do you think is the purpose of this program?
15. Did you choose to accept or reject Facebook? And why did you take that choice?
16. When you were asked to change decision on gmail.com in the programs history, did you? And why did you make that choice?

### **Privacy Related**

17. What do you associate with the word privacy?
18. Do you ever worry about the visibility of the personal information you provide online?
  - (a) Yes
  - (b) No
  - (c) I have never thought about it
19. Do you ever think about what information you provide online?
  - (a) Yes, often
  - (b) Yes, but only sometimes
  - (c) No
20. What do you think can go wrong when you share a lot of information online?
21. Do you read privacy policies when creating user accounts online?
  - (a) Yes, always
  - (b) Yes, sometimes
  - (c) No
22. Would you use such a program?



- (a) Yes
- (b) No
- (c) Maybe

23. Other thoughts and comments?



# Appendix B

## Detailed Design

This appendix contains the detailed code for the Google Chrome extension developed through the work in this thesis. This is the final edition of the design as presented in the evaluation in Chapter 7. All information on how a Google Chrome extension is built and works is taken from Google Chrome's own webpages on extensions [36], unless otherwise specified.

### B.1 The Google Chrome Extension

Google Chrome extensions are really just a folder with files, written in HTML, CSS and JavaScript, which constitutes a working application that is uploaded and run in your browser and provides some kind of extra functionality. Google Chrome provides the opportunity for extensions to communicate with web-pages, servers or even features in the actual browser such as bookmarks and tabs.

What functions are implemented are specific for each extension, but common for all of them is that they need to consist of a manifest file and one or more HTML files. JavaScript files or other file types are optional.

### B.2 Manifest

The manifest file is a JavaScript Object Notation (JSON) formatted file, named `manifest.json` that provides the browser with information about the extension that is needed to run it. This information includes what properties, capabilities and important files the extension makes use of. The Manifest file for Privacy Advisor is given below.

```
2 {  
    "name": "Privacy Advisor",  
    "version": "1.0",
```

```
4     "description": "The Privacy Advisor extension.",
5     "background_page": "background.html",
6
7     "browser_action": {
8         "default_icon": "privacyadvisor.png",
9         "popup": "popup.html"
10    },
11
12    "content_scripts": [{
13        "matches": ["http://www.google.com/*"],
14        "css": ["style.css"],
15        "js": ["javascript.js"]
16    }],
17
18    "permissions": [
19        "tabs",
20        "http://**/*",
21        "https://**/*",
22        "background"
23    ]
24 }
```

Listing B.1: The Manifest File: manifest.json

The manifest file tells Google Chrome that this extensions name is Privacy Advisor, that the file `background.html` will be running in the background of the browser, that `popup.html` is the main page of the extension and also that `style.css` is the CSS applicable for the extension. The manifest also stated that `javascript.js` is the file containing JavaScript code, but in this case it's an empty file (and therefore not included in this appendix), it's just included in the manifest because Google Chrome requires it.

## B.3 Background Pages

Privacy Advisor has a background page, `background.html` which runs a JavaScript called `bg.js` that always runs in the background checking for new events in the browser. This script is responsible for checking what webpages are visited and changing the icons and content of the extension window in accordance. The script `bg.js` only simulates the intended functionality of the system, but for the user it appears as the functionality is in place. The background files can be seen in the two listings below.

```
<!doctype html>
```

2

```

<html>
4   <head>
      <title>Background</title>
6     <script src="bg.js"></script>
  </head>
8   <body>
  </body>
10 </html>

```

Listing B.2: The Background Page: background.html

```

chrome.tabs.onUpdated.addListener(function(tabId, changeInfo, tab){
2   var url = tab.url;

4   if(url=="http://twitter.com/" || url=="http://www.youtube.
      com/"){
      chrome.browserAction.setIcon({path:"ok.png"});
6     chrome.browserAction.setPopup({popup:"ok.html"});

8   }else if(url=="http://www.facebook.com/" || url=="https://www
      .paypal.com/no"){
      chrome.browserAction.setIcon({path:"notok.png"});
10    chrome.browserAction.setPopup({popup:"notok.html"});

12   }else if(url=="http://www.linkedin.com/"){
      chrome.browserAction.setIcon({path:"alert.png"});
14    chrome.browserAction.setPopup({popup:"alert.html"});

16   }else{
      chrome.browserAction.setIcon({path:"privacyadvisor.png
18     "});
      chrome.browserAction.setPopup({popup:"popup.html"});
20   }
});

```

Listing B.3: The Background Script: bg.js

## B.4 HTML Pages

The HTML pages controls the navigation and content of the actual extension that the user interacts with. The code is quite simple as the focus is on design rather than functionality. All HTML files used are given below.

```

<!doctype html>
2 <html>

```

```

4  <head>
      <title>Hovedmeny</title>
6  <link rel="stylesheet" type="text/css" href="style.css" />
</head>
8
10 <body>
      <h3> Privacy Advisor </h3>
      <hr />
12
      <a href="info.html"></a>
14 <a href="settings.html"></a>
      <a href="history.html"></a>
16 </br>
18 </body>
</html>

```

Listing B.4: The Main Menu: popup.html

```

<!doctype html>
2 <html>
4 <head>
      <title>Information</title>
6 <link rel="stylesheet" type="text/css" href="style.css" />
</head>
8
10 <body>
      <a href="popup.html"></
          a>
      <h3> Information </h3>
12 <hr />
14 <small>
      Privacy Advisor helps you to think about privacy and how you
          share personal information when browsing the internet.
16 The program gives you advice on whether webpages can be trusted
          , according to your preferences.
      </br></br>
18 The advices are based on what you have done on previous
          webpages that treat your information in a similar way.
      </br></br>

```

```

20     The system gives you advice with using the following symbols in
        your browser.

22     </br>
        </br>

24     This symbol indicates that the
        webpage handles your information in a good way and can
        safely be accepted.

        </br>
        </br>

26     This symbol indicates that
        the webpage should not be trusted with your personal
        information and should be rejected.

        </br>
        </br>

28     This symbol indicates that
        the privacy of the webpage could not be determined for the
        current webpage.

        </br>
        </br>

30     This symbol indicates that
        the privacy of the webpage could not be determined for the
        current webpage.

        </br>
        </br>

32     </br>
        </br>

34     When the icons change you can see the advice given and the
        details that form the basis of it. You are then asked to
        indicate whether you trust the webpage or not. The system
        will then use your feedback for adapt future advices to
        your privacy preferences.

        </small>
        </br>

36     </br>

38     </body>
        </html>

```

Listing B.5: The Information Page: info.html

```

<!doctype html>
2 <html>

4     <head>
        <title>Settings</title>
        <link rel="stylesheet" type="text/css" href="style.css" />
    </head>

8     <body>
10     <a href="popup.html"></a>
        >
        <h3> Settings </h3>
12     <hr />

```

```
14      Number of policies for comparison:
16      <select id="choice" name="choice">
18          <option>5</option>
18          <option>10</option>
20          <option selected="selected">15</option>
20          <option>20</option>
22          <option>25</option>
22          <option>30</option>
24      </select>
24
26      <br><br>
26
28      <b>Weighting:</b>
28      </br>
30      <small>Indicate what you think is important factors to
30          consider when you provide personal information online. 5 is
30          most important, 1 is least important.</small>
30      <hr />
32
32      Type of data you provide:
34      <select id="choice" name="choice">
34          <option>1</option>
36          <option>2</option>
36          <option>3</option>
38          <option selected="selected">4</option>
38          <option>5</option>
40      </select>
40      <br><br>
42      How your data are stored:
42      <select id="choice" name="choice">
44          <option>1</option>
44          <option selected="selected">2</option>
46          <option>3</option>
46          <option>4</option>
48          <option>5</option>
48      </select>
50      <br><br>
50      The reason for gathering your data:
52      <select id="choice" name="choice">
52          <option>1</option>
54          <option>2</option>
54          <option selected="selected">3</option>
56          <option>4</option>
56          <option>5</option>
56      </select>
```



```

58     <br><br>
    Who are given access your data:
60     <select id="choice" name="choice">
        <option>1</option>
62         <option>2</option>
        <option>3</option>
64         <option>4</option>
        <option selected="selected">5</option>
66     </select>

68 </body>
</html>

```

Listing B.6: The Settings Page: settings.html

```

<!doctype html>
2 <html>

4     <head>
        <title>History</title>
6         <link rel="stylesheet" type="text/css" href="style.
            css" />
    </head>

8     <body>
10        <a href="popup.html"></a>
        <h3> History </h3>
12        <hr />
        <p> Overview of previous decisions: </p>

14        <table id="history">
16            <thead>
                <th>Webpage</th>
18                <th>Descision</th>
                <th>More</a></th>

20            </thead>
            <tbody>
22                <tr>
                    <td>www.youtube.com</td>
24                    <td><select name="choice">
                        <option selected="selected">Trusted<
                            /option>
26                    <option>Not Trusted</option>
                    <option>None</option>
                    </select></td>
28                </tr>
            </tbody>
        </table>
    </body>
</html>

```

```

    <td><a href="details.html" >Details+</a></td>
    >
30 </tr>
    <tr>
32 <td>www.twitter.com</td>
    <td><select name="choice">
34 <option selected="selected">Trusted<
        /option>
        <option>Not Trusted</option>
36 <option>None</option>
        </select></td>
38 <td><a href="details.html">Details+</a></td>
    </tr>
40 <tr>
    <td>www.gmail.com</td>
42 <td><select name="choice">
        <option selected="selected">Trusted<
        /option>
44 <option>Not Trusted</option>
        <option>None</option>
46 </select></td>
    <td><a href="details2.html">Details+</a></td>
    >
48 </tr>
    <tr>
50 <td>www.facebook.com</td>
        <td><select name="choice">
        <option>Trusted</option>
        <option selected="selected">Not
            Trusted</option>
54 <option>None</option>
        </select></td>
56 <td><a href="details2.html">Details+</a></td>
    >
    </tr>
58 <tr>
    <td>www.paypal.com</td>
60 <td><select name="choice">
        <option>Trusted</option>
62 <option selected="selected">Not
            Trusted</option>
        <option>None</option>
64 </select></td>
    <td><a href="details2.html">Details+</a></td>
    >
66 </tr>
</tbody>
```

```

68         </table>
70     </body>
</html>

```

Listing B.7: The History Page: history.html

```

<!doctype html>
2 <html>
4     <head>
        <title>Ok</title>
6         <link rel="stylesheet" type="text/css" href="style.css" />
8         <script type="text/javascript">
            function changeDisplay() {
10                 chrome.browserAction.setIcon({path: "
                    privacyadvisor.png"});
                chrome.browserAction.setPopup({popup: "popup.
                    html"});
12            }
        </script>
14    </head>
16    <body>
        <h3>Safe Page</h3>
18        <hr />
        This page protects your privacy in a good way and can safely be
            trusted.
20        </br>
        </br>
        Level of confidence: 85%
22        <a href="details.html" id="link">Details+</a>
24        </br>
        </br>
26        <form><textarea id="comment" rows="3" cols="25" placeholder
            ="comment.."></textarea></form>
        </br>
28        Do you trust this page?
        <a href="popup.html" onClick="changeDisplay()"></a>
30        <a href="popup.html" onClick="changeDisplay()"></a>
32    </body>
</html>

```

Listing B.8: Advice for Good Pages: ok.html

```
1 <!doctype html>
2 <html>
3
4 <head>
5   <title>Not ok</title>
6   <link rel="stylesheet" type="text/css" href="style.css" />
7
8   <script type="text/javascript">
9     function changeDisplay(){
10       chrome.browserAction.setIcon({path:"
11         privacyadvisor.png"});
12       chrome.browserAction.setPopup({popup:"popup.
13         html"});
14     }
15   </script>
16 </head>
17
18 <body>
19   <h3>Unreliable page</h3>
20   <hr />
21   This page does not take care of your privacy in a good way and
22   should not be trusted.
23
24   <br>
25   <br>
26   Level of confidence: 79%
27
28   <a href="details2.html" id="link">Details</a>
29   <br>
30   <br>
31   <form><textarea id="comment" rows="3" cols="25" placeholder
32     ="comment.."></textarea></form>
33   <br>
34   Do you trust this page?
35   <a href="popup.html" onClick="changeDisplay()"></a>
37   <a href="popup.html" onClick="changeDisplay()"></a>
39
40 </body>
41 </html>
```

Listing B.9: Advice for Bad Pages: notok.html

```

2 <!doctype html>
  <html>
    <head>
4      <title>Settings</title>
      <link rel="stylesheet" type="text/css" href="style.css" />
6      <script type="text/javascript">
          function goBack(){
8              window.history.back()
          }
10     </script>
  </head>
12
  <body>
14     

16     <p> Details: Safe Page </p>
     <hr />
18     <p>This page's privacy policy can safely be accepted. This
        decision is based on decisions you made in similar cases.
        This page handles your information in a similar manner as the
        following webpages. </p>

20     www.gmail.com</br>
22     www.twitter.com

24     <a href="policy.html" id="link" >See Policy</a>

26 </body>
</html>

```

Listing B.10: Details for Good Pages: details.html

```

2 <!doctype html>
  <html>

4   <head>
      <title>Details</title>
6      <link rel="stylesheet" type="text/css" href="style.css" />

8      <script type="text/javascript">
          function newTab(){
10             chrome.tabs.create({'url': chrome.extension.getURL('
                policy.html')});
          }
12

```

```

14     function goBack(){
15         window.history.back()
16     }
17     </script>
18 </head>
19
20 <body>
21     
23
24     <p> Details: Unreliable Page </p>
25     <hr />
26     <p>This page's privacy policy should be rejected because it
27         handles your information in a poor way.
28     The advice is based on decisions you made in previous cases on
29     pages that handle your information in a similar way as this
30     one. </p>
31
32     www.ebay.com </br>
33     www.paypal.com
34     </br>
35     </br>
36     <a href="policy.html" id="link" >See Policy</a>
37
38 </body>
39 </html>

```

Listing B.11: Details for Bad Pages: details2.html

```

1 <!doctype html>
2 <html>
3
4 <head>
5     <title>alert</title>
6     <link rel="stylesheet" type="text/css" href="style.css" />
7
8     <script type="text/javascript">
9         function changeDisplay(){
10             chrome.browserAction.setIcon({path:"
11                 privacyadvisor.png"});
12             chrome.browserAction.setPopup({popup:"popup.
13                 html"});
14         }
15     </script>
16 </head>
17
18 <body>

```

```

18 <h3>Undetermined Privacy.</h3>
    <hr />
    <p>This page's privacy policy could for some reason not be
        determined. This might be because something went wrong
        while fetching this pages privacy policy or the page does
        not support machine readable privacy policies.
20    Either way, we suggest you give your opinion on this page in
        order for the system to learn from it.    </p>
    <p>Level of privacy: ? </p>
22    </br>
    <form><textarea id="comment" rows="3" cols="25" placeholder
        ="comment.."></textarea></form>
24    </br>

26    Do you trust this page?
    <a href="popup.html" onClick="changeDisplay()"></a>
28    <a href="popup.html" onClick="changeDisplay()"></a>

30    </body>
</html>

```

Listing B.12: Undetermined Privacy Page: alert.html

```

<!doctype html>
2 <html>

4   <head>
    <title>Privacy Policy</title>
6    <link rel="stylesheet" type="text/css" href="style.css" />

8    <script type="text/javascript">
        function goBack(){
10            window.history.back()
        }
12    </script>
</head>

14 <body id="policy">
16    
    <h3>Privacy Policy </h3>
18    <hr />
    </small>
20    <h4>www.paypal.com</h4>
    <p>
22    Policy text here...

```

```
24     </p>
        </small>
26 </body>
</html>
```

Listing B.13: Privacy Policy Page: policy.html

## B.5 The CSS

This CSS is controlling the styling of all the html pages presented above.

```
body { font-family: 'Verdana';
2         background-color: whitesmoke;
         min-width: 320px;
4         overflow-x: hidden;
         font-size: 90% }
6
a#link { float: right; }
8
a:link { /*Unvisited*/ color: green; }
10
a:visited { /*Visited*/ color: green; }
12
a:hover { /*Mouse over*/ color: blue; }
14
a:active { /*Selected*/ color: blue; }
16
table#history {         margin: 1em;
18                     border-collapse: collapse; }
20
td, th {         padding: .3em;
                border: 1px #ccc solid; }
22
thead { background: #E8E8E8; }
24
h3 { text-align: center;
26     font-family: 'Georgia'; }
28
img#choice { margin: 3px;
              float: center;
30              width: 40px;
              height: 25px; }
32
img#details { height: 25px;
34              width: 28px; }
```



```
36 img#return{ width:30px;
                                     height:30px;
38                                     float:right; }

40 img#menu{      margin:5px;
                                     float:center;
42                                     width:90px;
                                     height:100px; }

44 img#info{      float:left;
46                                     margin:5px;
                                     border:0px solid black;
48                                     vertical-align:middle;
                                     width:30px;
50                                     height:30px; }

52 img#detailsreturn{ width:30px;
                                     height:30px;
54                                     float:right;
                                     margin:10px; }

56 p{ width:310px; }

58 select{ float:right; }
```

Listing B.14: The CSS File: style.css



# Appendix C

## Running the Extension

This appendix explains how the Privacy Advisor Extension can be installed and run in the browser.

### C.1 Installation and Execution

Running and installing the Google Chrome extension requires that you have the browser installed on your computer, regardless of the version. If the browser is installed, follow the steps listed below to install and run the extension.

1. Go to the following url: `chrome://settings/extensions`.
2. Put a checkmark on the box for developer mode.
3. Press the "Load unpacked extension" and upload the entire folder containing all the files of Privacy Advisor.
4. Make sure the extension is activated.
5. The extension should then be ready for testing and a blue icon should have appeared in your browser window.
6. Use the tasks from Appendix A to see how the design works.

The extension also requires that you are not logged into any of the webpages when going through the tasks described in Appendix A. Sometimes the extension have problems noticing changes in the browser on the first attempt (seems to be dependent on the computer or browser running), so it might help to press F5 to reload the webpage to get the advices activated.

