Nicole Merz

P3P – Purpose, Plan, Protection, and Problems

Bachelorarbeit

Themensteller: Juniorprofessor Dr. Ali Sunyaev

Vorgelegt in der Bachelorprüfung
im Studiengang Wirtschaftsinformatik
der Wirtschafts- und Sozialwissenschaftlichen Fakultät
der Universität zu Köln

Köln, September 2014

Table of Content

List of Abbreviations

ACM	Association for Computing Machinery
AISEL	AIS Electronic Library
API	Application Programming Interface
APPEL	A P3P Preference Exchange Language
cdt	Center for Democracy and Technology
e-commerce	electronic commerce
eHealth	electronic health
FTC	Federal Trade Commission
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IE	Internet Explorer
IPWG	Internet Privacy Working Group
IT	Information Technology
OECD	Organization for Economic Co-operation and Development
OPS	Open Profiling System
P3	Platform for Privacy Preferences
P3P	Platform for Privacy Preferences Project
PET	Privacy-Enhancing Technology
PHS	Patient-Centered Health Information Technology Service
PRF	Policy References Files
W3C	World Wide Web Consortium
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language

Index of Illustrations

Index of Tables

1. Introduction

1.1 Definition of Problem

Research on information privacy and security has shown that transparency – users getting easy access to information like for what purposes their personal data are shared with and with who they are shared - plays a vital role in the users' lives[1], when using privacy-enhancing technologies (PETs) like P3P, the Platform for Privacy Preferences Project. P3P was developed to enable web browsers to read privacy policies automatically and compare them with the users' defined privacy preferences.[2] For users, a PET is software developed in order to provide an easier way of handling privacy policies[3] which are difficult to read and understand.[4] They were designed to support users in privacy related decisions leading to the decrease of the users' concerns.[5] In order to be able to get the important information to users, PETs can be helpful for them, but they are still not fully accepted.[6] The purpose of PETs is to improve protection and inform users when personal data are shared with third parties and for what purposes.[7] This should lead to an establishment of transparency of how these personal data are "being collected, stored, processed and disclosed"[8]. However, there are still major concerns of users dealing with IT services caused by a lack of transparency.[9] A characterization of Internet users' concerns include terms like collection (the exchange of personal information), control (user control over personal information) and awareness of privacy practices (information about the usage of personal data). Based on these existing threats in the World Wide Web in general, this thesis concentrates on P3P as a PET, a particular case. We analyze problems and disadvantages of the P3P focusing on the P3P development process and the users' behavior concerning this standard to increase transparency and the users' trust in IT services. Therefore, analyzing P3P

[1] Cf. Holzner, Holzner (2006), p. 3.

[2] Cf. Cranor (2003), p. 50.

[3] Cf. Cranor (2003), p. 55.

[4] Cf. Jensen and Potts (2004), p. 477.

[5] Cf. DSTI/ICCP/REG (2001), p.15.

[6] Cf. Cranor, Guduru, Arjula (2006), p. 136.

[7] Cf. Janic, Wijbenga, Veugen (2013), p. 18.

[8] Janic, Wijbenga, Veugen (2013), p. 18.

[9] Cf. Malhotra, Kim, Agarwal (2004), p. 338.

clarifies the question ‘What can we learn from the strengths and weaknesses of the privacy-enhancing technology P3P, to finally get suggested solutions of how to design PETs accepted by users?’. There is no literature review available giving an exact overview of advantages and disadvantages of P3P as well as providing different viewpoints including P3P development process and the users’ point of view. As part of the P3P process, there were several user agent prototypes developed, an important component of P3P. For that reason, an analysis of some of these user agents shows, how users interact with these tools and what sort of common problems they have dealing with P3P. It is useful to consider these strengths and weaknesses of P3P, in order to be able to get suggestions of improvement to develop and design PETs accepted by users. These PETs might reduce the users’ privacy concerns dealing with health IT services by gaining more control of their personal data. The goal of these PETs is to achieve protection of the users’ privacy, as information privacy increasingly becomes the users’ decision. As a result, this thesis presents a listing of deduced design principles regarding the development process in general and the users’ point of view in particular, to finally be able to successfully develop an easy-to-use PET. Improving the development process of a PET - which could be successfully implemented and accepted by users – is necessary, as the process should not last too long and end-users should get the chance to be involved[10] in the development process to contribute to the improvement. Also, the users’ point of view is important to bring about improvements including P3P user agents or other important P3P components like the P3P vocabulary. It might give users the opportunity to handle and understand PETs and increase the insight into the users’ sensitive personal data and how to control it.

1.2 Objectives

The main objective of this thesis is to determine design principles for the development of PETs, which are more accepted by users than P3P.

To establish a solid basis for achieving the main objective we consider information about the theoretical background of this thesis. We begin with a basic understanding and a common definition of patient-centered health information technology service (PHS) - a medical online service developed specifically for users, in order to support

[10] Cf. Hochheiser (2002), p. 290.

them - , information privacy, PETs and P3P. The background of PHS is of particular interest, as it helps understand, why these online services are important for users considering that they still have major concerns dealing with these online services. For that reason, we determine, what the current situation of information privacy in healthcare is, concentrating on major aspects to show the importance of the research field. We consider the purpose of PETs and provide an overview of basic principles of PET in order to classify P3P.

To examine P3P, we explain the purpose and guiding principles of P3P to understand, why P3P was developed to later analyze, whether or not P3P fulfilled the objectives set by developers. We also analyze the need of PETs, such as P3P, for users, as it can show, whether or not users think of P3P as a valuable tool that helps them to gain more control over their privacy. Based on P3P's development process, we determine, how long the actual process lasts and whether or not the process was completed as it would indicate problems during the process. We determine, what was developed and when, as well as who was part of the development process. In order to fully understand, how P3P works, we explore the components and specifications. This shows the complexity of the P3P's protocol and raises the question, whether users are able to understand their options regarding P3P. We give an overview of important components of P3P including P3P policy, a P3P preference exchange language (APPLE) and others. In the following chapter we refer to these terms again to be able to analyze them. When concentrating on P3P components, user agents are of special interest as users deal with them often. An overview of the P3P specifications will show how complex the P3P protocol is and how difficult users might find it to understand it. We explain the application of P3P determining, which role each party plays in the transaction and what actually happen, when users visit a web site, which is P3P-enabled. Before starting with the analysis of P3P, we verify its adoption and list the numbers of P3P-enabled web sites. We provide adoption rates to show that P3P is not a success. To point out the failure of P3P, we determine strengths and weaknesses of P3P in general and emphasize the vital role of the shortcomings.

Analyzing P3P the development process is reflected critically. We answer the question, whether there is evidence in P3P's process that led to its failure. The objective is to filter relevant information, in order to classify it in terms of strengths and weaknesses. Despite the difficulties P3P can be seen as a success. We determine, what was new about a PET like P3P and why its development process lasts so long including main

aspects leading to its delay. In addition, we state, why P3P is a PET of notice and choice as well as why this limitation of functionality could be a problem for users. Concentrating on the whole framework of P3P, we analyze several of its components. We determine a critical reflection of all P3P user agent prototypes, which were designed during ten years of development of P3P. Subsequently, we switch to the users' point of view and examine their behavior dealing with P3P to enable us to come to a conclusion, whether there is a connection between the users' difficulties dealing with P3P and the indicators for problems in the development process. To determine underlying causes for P3P not being successful we determine, what the users' concerns are in general and we analyze the situation between service providers and consumer. To achieve this, we present the users' expressions of P3P components and P3P user agent interfaces, because these are references to P3P's strengths and weaknesses and might help deduce design principles. When comparing user agents, we state, which kind of functionality users can deal well with and which not. One of the greatest problems using of P3P user agents is the reduction of precision, when translating P3P statements. We determine, why reduction is useful and what sort of problems it creates. Finally getting to the main objective, we assess design principles, which can be recommended to develop a PET like P3P that might be accepted by users, considering reduction of transparency and a decrease of trust in PETs.

1.3 Method

To analyze P3P with regards to its development process and the users' experiences with it we perform a search in different databases looking for journals. As we concentrate especially on journals, we choose databases including Association for Computing Machinery digital library (ACM), AIS electronic library (AISEL), EBSCO, IEEE Explorer (computer.org) and ProQuest. Unfortunately, EBSCO could not find any useful results to the main topic P3P. Apparently, the used search engine cannot deal with the key word 'P3P' as it does not recognize as such. Also, ACM was of limited benefit. However, all other mentioned databases brought up many results.

First, we concentrate on finding useful results on the development process of P3P. Due to that, we determine a search phrase including 'P3P', 'development process' and 'problem'. Instead of looking for development process it is also possible to find results using the word 'process'. Therefore, we logically combine 'development process' and

process with the OR operator. We also use the plural of the term ‘problem’, in order to cover all potential hits. The resulting search string is as follows: P3P AND (‘development process’ OR process) AND (problem OR problems). Where possible, we search for this string in the titles, keywords and abstracts to determine the relevance of journals.

Second, we concentrate on finding results on the users’ point of view, their concerns and expectations. Similar to the first search string, we determine keywords like ‘P3P’, ‘concern’ and ‘design’. We do not look for ‘user concern’, as the term ‘user’ is far too general in its meaning. Therefore, we choose to use the keyword ‘concern’ instead of the phrase ‘user concern’. Also, we include the plural of the keyword ‘concern’. The resulting search string is as follows: P3P AND (concern OR concerns) AND design. We use the resulting search string and limit our search by concentrating on title, keywords and the abstract of journals.

1.4 Thesis Structure

The following part of this thesis is organized in chapters. Chapter 2 presents the foundational background of the subject. This includes subchapter 2.1 concentrating on patient-centered health IT services, the research field information privacy in healthcare and an explanation of privacy-enhancing technologies. The subchapter 2.2 presents P3P including an overview of its purpose, a historical overview of the P3P development process, several components and specifications of P3P, its application, adoption rates, as well as benefits and drawbacks in general. Chapter 3 presents an analysis of P3P. Subchapter 3.1 summarizes, what results were found and identify these papers with important aspects to answer all outstanding issues. Subchapter 3.2 concentrates on a critical reflection of the development process of P3P. A short overview of the successful implementation of P3P is given in 3.2.1. In subchapter 3.2.2, P3P as a PET of notice and choice is analyzed. Sources of the development process’ delay are listed in 3.2.3. Subchapter 3.2.4 provides the strengths and weaknesses of P3P components. In 3.2.5 a critical reflection of P3P user agent prototypes is given. Subchapter 3.3 deals with the users’ point of view. In 3.3.1 we determine the users’ concerns dealing with online services. In 3.3.2, a description of the relationship between users and services providers is presented. In 3.3.3 several components of P3P are examined, in order to provide in insight-look into the users’ problems dealing with P3P. In 3.3.4 several P3P user agents

are analyzed to determine their strengths and weaknesses. These user agents are compared in subchapter 3.3.5. Problems, which are associated with the reduction of precision of P3P terms, are presented in 3.3.6. In chapter 4, we present deduced design principles. In chapter 5, we discuss the main shortcomings of P3P and validate the design principles to determine, which of them can be effectively used. In the last chapter, we present the conclusion of the thesis.

2. Theoretical Foundations

2.1 Information Privacy

2.1.1 Patient-Centered Health Information Technology Services (PHS)

2.1.1.1 Definition

Patient-centered health information technology services (PHS) are electronic health services for the users' needs.[11] Supported by PHS, users benefit from being able to make decisions regarding their own health in a compact and knowledgeable way.

2.1.1.2 Background

PHS can be assigned to eHealth, a concept including the web-based electronic exchange of health resources.[12] EHealth contains three areas including (a) the delivery of healthcare information by electronic means, (b) the improvement of health services by Information Technology (IT) and e-commerce, and (c) the improvement of the health systems management using e-commerce and e-business practices.

Services like web-based tools display the patients' health records or test results, make appointments and communicate with medical personnel.[13] Using these services, healthcare consumers rely on a confidential handling of their sensitive personal data and on the information sharing, when their personal data is gathered.[14] Unfortunately, many consumers are not aware of the lack of privacy protection. Service providers can collect and store patients' personal data.[15] However, health information technology services are needed to increase the efficiency of the healthcare system and to create access to healthcare within patients' reach. Strong efforts must be undertaken to find a way to close the "gap between the ideal and reality"[16].[17]

---

[11] Cf. for this paragraph Dehling, Sunyaev (2014), p. 89.

[12] Cf. for this paragraph WHO (2014), p. 1.

[13] Cf. Yi Hong, Patrick, Gillis (2008), p. 643.

[14] Cf. Yi Hong, Patrick, Gillis (2008), p. 646.

[15] Cf. for this and the following sentence Cliff (2012), p. 301.

[16] Yi Hong, Patrick, Gillis (2008), p. 646.

[17] Cf. Yi Hong, Patrick, Gillis (2008), p. 646.

2.1.2 Information Privacy in Healthcare

Information privacy is seen as a concept.[18] It is not only about users, who can control their personal data, but also about users being able to control the usage of their personal data. A great amount of research was done across all different kinds of disciplines like law, psychology, information systems and others. Every discipline presents its own definition of the term information privacy.[19] For instance, the law literature sees information privacy as a right. However, the information systems literature defines information privacy as the users' control over personal information.

When users visit web sites, they have to expect web sites collecting the users' personal data to use them as valuable information, for marketing purposes for example.[20] As a result, users feel uncomfortable and disrespected regarding their privacy, which leads to the users' concerns. There is a correlation between the varieties of different information privacy concerns in the research field.[21] These concerns are related to the users' contribution to the acquisition of data, the transaction activity and the government regulation.

The users' concerns about data collection can be divided in groups including security fears, identity theft, sharing of data with third parties, the lack of knowledge about data usage and user profiling.[22] Only the last three points refer to information privacy and not information security. The term sharing of data with third parties describes the users' concerns to share personal data with third parties without their explicit permission. The lack of knowledge about data usage is a problem to users, if their personal data is collected for the users' unrelated purposes. User profiling includes users being categorized. On the one hand, user profiling can be beneficial, as the users' online experiences may be facilitated. On the other hand, users are concerned, if web sites store their personal data permanently.

[18] Cf. for this and the following two sentences Pavlou (2011), p. 977.

[19] Cf. for this and the following two sentences Pavlou (2011), p. 980.

[20] Cf. for this and the following sentence Pavlou (2011), p. 977.

[21] Cf. for this and the following sentence Pavlou (2011), p. 978.

[22] Cf. for this paragraph DSTI/ICCP/REG (2001), p.16.

Privacy-enhancing technologies (PETs) give users the opportunity to get control over their personal data.[23] The wide variety of PETs makes it rather difficult for users to choose the right one.

2.1.3 Privacy-Enhancing Technology (PET)

Privacy-enhancing technology (PET) is software developed for users helping them to control and protect their privacy, when they are browsing on the Internet.[24] They were designed to support users in privacy related decisions leading to the decrease of the users' concerns.[25] However, PETs were not designed to cover all the users' privacy concerns. PETs are defined by the Center for Democracy and Technology (cdt).[26] The Organization for Economic Co-operation and Development (OECD) formulated guidelines governing the protection of privacy and transborder flows of personal data including basic principles of national application.[27] These principles contain the Collection Limitation Principle, the Data Quality Principle, the Purpose Specification Principle, the Use Limitation Principle, the Security Safeguards Principle, the Openness Principle, the Individual Participation Principle and the Accountability Principle, also shown in Table 2-1.[28]

The Collection Limitation Principle is about the limitation of personal data and "should be obtained by lawful and fair means […] with the knowledge or consent of the data subject"[29].[30] The Data Quality Principle includes the relevance of personal data. The purposes "should be accurate, complete and kept up-to-date"[31]. The Purpose Specification Principle is about "the purposes for which personal data are collected"[32]. The purposes should be stated before the data is collected. The Use Limitation Principle says that "personal data should not be disclosed, made available or otherwise used for

[23] Cf. for this paragraph DSTI/ICCP/REG (2001), p.15.

[24] Cf. Cranor, Guduru, Arjula (2006), p. 136.

[25] Cf. for this and the following sentence DSTI/ICCP/REG (2001), p.15.

[26] Cf. Beatty et al. (2007), p. 65.

[27] Cf. Cranor, Guduru, Arjula (2006), p. 139.

[28] Cf. Organization for Economic Co-operation and Development (2013), pp. 13/14.

[29] Organization for Economic Co-operation and Development (2013), p. 14.

[30] Cf. for this and the following six sentences Organization for Economic Co-operation and Development (2013), p. 14.

[31] Organization for Economic Co-operation and Development (2013), p. 14.

[32] Organization for Economic Co-operation and Development (2013), p. 14.

purposes other than those specified in accordance with"[33] the Purpose Specification Principle. However, there are two exceptions made by an agreement of the data subject or the authority of law. The Security Safeguards Principle includes the protection of personal data by security safeguards "against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data"[34].[35] The Openness Principle says that "there should be a general policy of openness about developments, practices and policies with respect to personal data"[36]. Important information about the nature of personal data and the purposes of use should be accessible for users. The Individual Participation Principle lists all individuals' rights. And the last named principle, the Accountability Principle is about the accountability of data controllers "for complying with measures which give effect to the principles stated above"[37].

Basic Principle
• Collection Limitation Principle • Data Quality Principle • Purpose Specification Principle • Use Limitation Principle • Security Safeguards Principle • Openness Principle • Individual Participation Principle • Accountability Principle

Tab. 2-1: Basic Principles of National Application

PETs can support one or more of these principles. That is why there is a wide variety of them.[38] P3P is an example for a PET. It supports two out of the eight principles: the

[33] Organization for Economic Co-operation and Development (2013), p. 14.

[34] Organization for Economic Co-operation and Development (2013), p. 15.

[35] Cf. for this and the following four sentences Organization for Economic Co-operation and Development (2013), p. 15.

[36] Organization for Economic Co-operation and Development (2013), p. 15.

[37] Organization for Economic Co-operation and Development (2013), p. 15.

[38] Cf. for this and following two sentences Cranor, Guduru, Arjula (2006), p. 140.

Purpose Specification Principle and the Openness Principle and is not directly linked to the other principles.

Another model of privacy developed by the U.S. Federal Trade Commission (FTC) provides five principles including Notice, Choice, Access, and Security as shown in Table 2-2.[39]

Privacy Principles
Notice
Choice
Access
Security

Tab. 2-2: FTC privacy principles

The principle of Notice is about users noticing web sites information practices including the purpose of collecting personal data.[40] The Choice principle states that web sites should give users options of how to handle the usage of their personal data. The Access principle says that users should have access to information, which is collected by web sites including the chance to delete this information. The Security principle implies the protection of information against certain threats. P3P supports two out of four principles including Notice and Choice.

It is difficult for users to choose the right PET regarding their concerns or even be aware of the availability of a certain PET.[41] Also, users, who already use a PET, have to be willing to use them consequently.

[39] Cf. Hochheiser (2002), pp. 281/282.

[40] Cf. for this paragraph Federal Trade Commission (2000), p. 7.

[41] Cf. for this and the following sentence DSTI/ICCP/REG (2001), p.15.

2.2 Platform for Privacy Preferences Project (P3P)

2.2.1 Purpose

The Platform for Privacy Preferences Project (P3P) is a standard machine format for privacy policies created by the World Wide Web Consortium (W3C)[42], an international community elaborating and engineering new Web standards.[43]

P3P policies are deployed by web sites to open their privacy practices – a declaration of web sites of how the users' personal data is collected and how these data are used[44] - to users. The increased transparency is achieved by providing information about what personal data is collected and how it is processed.[45] Using different mechanisms like a set of multiple-choice questions or a slider bar, users can express their privacy preferences.[46] Privacy policies can be interpreted by user agents and then compared with the users' defined privacy preferences.[47] For users, the automatic interpretation of web sites' privacy policies is an improvement, as most privacy policies are too difficult to read.[48] The reason for this is the usage of unusual terminology to unspecialized users of corporate legal departments.[49] Additionally, user agents are able to automatically inform users, whether web sites' privacy policies match the users' privacy preferences.[50] Users can determine, whether web sites may use their personal data and whether they want to stand in interaction with the web sites.[51] However, users have to act from conviction, when defining their privacy preferences, because only then P3P can be effective.[52] For that reason, users should be supported by "easy-to-use"[53] PETs like P3P.

---

[42] Cf. Cranor, Wenning (2007), p. 1.

[43] Cf. MIT et al. (2014), p. 1.

[44] Cf. Cranor et al. (2000a), p.8.

[45] Cf. Presler-Marshall (2002), p. 4/5.

[46] Cf. Beatty et al. (2007), p. 66.

[47] Cf. Cranor (2003), p. 50.

[48] Cf. Jensen and Potts (2004), p. 477.

[49] Cf. Beatty (2007), p. 66.

[50] Cf. Presler-Marshall (2002), p. 5.

[51] Cf. Cranor, Reidenberg (2002), p. 5.

[52] Cf. for this and the following sentence Reagle, Cranor (1999), p. 1.

[53] Reagle, Cranor (1999), p. 1.

1998, the P3P guiding principles were published in a W3C note.[54] These principles, including information privacy, notice and communication, choice and control, fairness and integrity, and security, are a general outline of what P3P is and what it is not.[55] The principle information privacy stands for the intention to increase privacy and trust on the World Wide Web, bringing service providers and users close.[56] P3P makes it possible for users to consider balanced decisions and for service providers to reveal their information practices. Notice and communication is about what service providers and user agents should provide.[57] Choice and control stands for using and controlling the users' personal data and sets the direction of what service providers and user agents should do to ensure the users' information privacy.[58] As the essence of P3P, it should be guaranteed that users are treated with fairness and integrity.[59] Therefore, the principle provides rules for user agents and service providers, for instance, to ensure never to mislead users. Security is the last listed principle.[60] It underlines the lack of security mechanisms in P3P as the standard can be conjunct with security tools.

2.2.2 Plan – Process of Development

P3P was officially introduced in 1997.[61] In the previous year, the Internet Privacy Working Group (IPWG), convened by the Center for Democracy and Technology (cdt), started its research on developing PETs, which support users in protecting their privacy. The IPWG, represented by IBM, AT&T, Microsoft, W3C and others, set up a subcommittee with the aim to define a privacy vocabulary. In March 1998, the P3P Harmonized Vocabulary Specification was published. The subcommittee in collaboration with W3C developed the first prototype of P3P, the Platform for Privacy Preferences (P3)[62], in 1997.[63] Overall four W3C prototypes were developed, each time with different goals.[64]

---

[54] Cf. Cranor (1998), p. 1.

[55] Cf. Cranor (1998), pp. 2 - 5.

[56] Cf. for this and the following sentence Cranor (1998), p. 2.

[57] Cf. for this and the following sentence Cranor (1998), p. 3.

[58] Cf. Cranor (1998), p. 4.

[59] Cf. for this and the following sentence Cranor (1998), pp. 4/5.

[60] Cf. for this and the following sentence Cranor (1998), p. 5.

[61] Cf. for this and the following three sentences Cranor (2002a), p. 2.

[62] Cf. World Wide Web Consortium (1997), p. 1.

P3P Specification Working Groups, convened by W3C, were responsible for developing P3P.[65] These groups were also composed of experts from academia and government. During the process of development, the base of the P3P model did not change. However, details like the data transfer of P3P were altered consistently. In 1999, the current working group was not interested in leaving the standardized data transfer mechanism a part of the P3P framework.[66] The mechanism requests the users' personal data, in order to transfer it to a server, where it is stored. Once the mechanism is removed, it is necessary for users to enter their personal data again and again. The anticipated benefit for users of time savings and privacy assurance and for online services of access to the users' data was expected. The concept of negotiation and agreement was removed from the P3P 1.0 specification completely to make the P3P implementation easier.[67] Aside from that, web sites implemented P3P to the exclusion of any other software.

Regularly the working groups received feedback on the evolved specifications presented in public working drafts. The first working draft of P3P 1.0 specifications was published in November 1998 (see Table 2-3). Based on this and other drafts, P3P user agents and editors were built by software developers. Around the same time, web sites of several organizations and companies were P3P-enabled. In 1999, a prototype of a P3P user agent, called Privacy Minder, was developed by AT&T Research.[68]

In 2001, the first user agent implementation of P3P appeared in the Microsoft Internet Explorer.[69] The IE6 uses filter cookies based on P3P policies and the user's privacy settings.[70] A year later, the AT&T Privacy Bird, a P3P user agent add-on for the IE, was released by AT&T.[71] Privacy Bird is a free online search engine displaying a bird icon

[63] Cf. Cranor, Guduru, Arjula (2006), p. 144.

[64] Cf. Cranor, Guduru, Arjula (2006), p. 143.

[65] Cf. for this and the following three sentences Cranor (2002a), p. 2.

[66] Cf. for this and the following three sentences LaLiberte (1999), p. 1.

[67] Cf. for this and the following five sentences Cranor (2002a), p. 3.

[68] Cf. Cranor, Guduru, Arjula (2006), p. 144.

[69] Cf. Cranor (2002a), p. 3.

[70] Cf. Microsoft (2014), p. 1.

[71] Cf. Cranor (2002a), p. 3.

in the browser title bar.[72] Also, IBM developed a P3P policy editor tool that is used by web sites to update their P3P policies.[73]

No.	Date	Version	
1	30-Mar-1998	P3P Harmonized Vocabulary Specification	Working Draft
2	19-May-1998	Syntax Specification	Working Draft
3	02-Jul-1998	Syntax Specification	Working Draft
4	09-Nov-1998	P3P 1.0	Working Draft
5	07-Apr-1999	P3P 1.0	Working Draft
6	26-Aug-1999	P3P 1.0	Working Draft
7	02-Nov-1999	P3P 1.0	Working Draft
8	11-Feb-2000	P3P 1.0	Working Draft
9	04-Apr-2000	P3P 1.0	Working Draft
10	24-Apr-2000	P3P 1.0	Working Draft
11	10-May-2000	P3P 1.0	Working Draft
12	15-Sep-2000	P3P 1.0	Working Draft
13	18-Oct-2000	P3P 1.0	Working Draft
14	15-Dec-2000	P3P 1.0	Candidate Recommendation
15	24-Sep-2001	P3P 1.0	Working Draft
16	28-Sep-2001	P3P 1.0	Working Draft
17	28-Jan-2002	P3P 1.0	Proposed Recommendation
18	16-Apr-2002	P3P 1.0	Recommendation
19	10-Feb-2004	P3P 1.1	Working Draft
20	27-Apr-2004	P3P 1.1	Working Draft
21	20-Jul-2004	P3P 1.1	Working Draft
22	04-Jan-2005	P3P 1.1	Working Draft
23	01-Jul-2005	P3P 1.1	Working Draft
24	10-Feb-2006	P3P 1.1	Working Draft
25	13-Nov-2006	P3P 1.1	Working Group Note

Tab. 2-3: Overview of the chronological sequence of the released P3P specifications, including Vocabulary Specification and Syntax Specification[74]

[72] Cf. PrivacyBird (no date), p. 1.

[73] Cf. for this and the following five sentences Cranor (2002a), p. 3.

After nearly six years of steady improvement, the working group released another version of the working draft of the P3P 1.0 specifications at the beginning of 2002[75] (see Table 2-3). As shown in Table 2-3, the first working draft on P3P 1.1 specifications was published two years later[76]. The final P3P 1.1 specification was published at the end of 2006[77] (see Table 2-3).

2.2.3 Components

The most important components of P3P, which we take a closer look at, include P3P policy, APPEL, user data repository and the P3P user agent.

P3P Policy

P3P policies are codified in eXtensible Markup Language (XML), a computer-readable language.[78] Human-readable privacy policies are also included.[79] There are several policy generators and editors available.[80] These include the P3PBuilder, which generates P3P policies to the W3C specifications, and the PrivacyBot.com, which supports service providers by implementing privacy practices and generates privacy policies and others. To form a P3P policy XML elements defined in the P3P specifications have to be combined, shown in chapter 2.2.4.

APPEL (A P3P Preference Exchange Language)

APPEL is a "rule-based language"[81] recommended by the W3C.[82] It was influenced by the P3P 1.0 specifications. The aim of using this language is to share rulesets - sets of

[74] Cf. Reagle (1998), p. 1; Marchiori, Jaye (1998a), p.1; Marchiori, Jaye (1998b), p.1; Marchiori, Reagle, Jaye (1998), p. 1; Marchiori, Reagle (1999a), p. 1; Marchiori, Reagle (1999b), p. 1; Cranor et al. (1999), p. 1; Cranor et al. (2000a), p. 1; Cranor et al. (2000b), p. 1; Cranor et al. (2000c), p. 1; Cranor et al. (2000d), p. 1; Cranor et al. (2000e), p. 1; Cranor et al. (2000f), p. 1; Cranor et al. (2000g), p. 1; Cranor et al. (2001a), p. 1; Cranor et al. (2001b), p. 1; Cranor et al. (2002a), p. 1; Cranor et al. (2002b), p. 1; Cranor et al. (2004a), p. 1; Cranor et al. (2004b), p. 1; Cranor et al. (2004c), p. 1; Cranor et al. (2005a), p. 1; Cranor et al. (2005b), p. 1; Cranor et al. (2006b), p. 1; Cranor et al. (2006b), p. 1.

[75] Cf. Cranor et al. (2002a), p. 1.

[76] Cf. Cranor et al. (2004a), p. 1.

[77] Cf. Cranor et al. (2006b), p. 1.

[78] Cf. Cranor, Reidenberg (2002), p. 6.

[79] Cf. Beatty et al. (2007), p. 66.

[80] Cf. for this and the following sentence Wenning (2007), pp. 3/4.

[81] Cranor (2003), p. 52.

[82] Cf. for this and the following sentence Cranor, Langheinrich, Marchiori (2002), p. 9.

preference-rules - for communication to agents, proxies and others, and enabling products to be portable.[83] Users do not create their privacy preferences with APPEL directly.[84] Rulesets are created by user agents. Preference rulesets can be imported by users. P3P user agents do not have to use APPEL, but for instance AT&T Privacy Bird does.[85]

User Data Repository

The P3P user data repository stores information about users, in order to transfer them to online services.[86] This may include contact information for payment or delivery services. Seen from the benefit point of view, users and online services profit from the users' data repositories. The users' dealing with online services is simplified, as they have to enter personal data, which is requested and used multiple times, just once in order to be stored in the users' repository.[87] This gives users more control over their personal data, as online services do not have to store the users' data in central databases. The benefit for online services is receiving the users' data every time they visit the web site. [88]

User Agent

A P3P user agent is a software tool retrieving P3P policies.[89] This software tool supports users in gathering and finding information considering privacy policies.[90] It is much easier for users to utilize P3P user agents, as it is too difficult for them to read privacy policies. For instance, when using Privacy Bird users can find information faster and precisely compared to the usage of human-readable privacy policies.[91] References to P3P policies are specified in HTTP headers or in the HTML head.[92] User

[83] Cf. Cranor, Langheinrich, Marchiori (2002), p. 7.

[84] Cf. for this and the following two sentences Hochheiser (2002), p. 279.

[85] Cf. Cranor (2003), p. 52.

[86] Cf. for this and the following two sentences Reagle, Cranor (1999), p. 52.

[87] Cf. for this and the following sentence Reagle, Cranor (1999), p. 53.

[88] Cf. Reagle, Cranor (1999), p. 52.

[89] Cf. Cranor et al. (2006), p. 10.

[90] Cf. for this and the following sentence Cranor, Guduru, Arjula (2006), p. 163.

[91] Cf. Cranor, Guduru, Arjula (2006), p. 164.

[92] Cf. Cranor et al. (2006), p. 10.

agents interpret P3P policies, in order to be compared with the users' defined privacy preferences to finally give feedback to the users about the privacy policies.[93] Data can be released, authorized by the user agent, on the condition of (a) the users' privacy preferences match the privacy policy and (b) the requested data transfer matches the privacy policy.[94] However, the user can authorize a data transfer manually, even if only one of the conditions cannot be complied.

There are different types of user agents. They can be integrated (a) into web browsers or (b) into online services and can be implemented (c) as software to add onto web browsers or (d) as stand-alone applications.[95]

Microsoft Internet Explorer 6 can be named as an example for a P3P user agent, which is part of the web browser, published in 2001.[96] It supports users by making cookie-blocking decisions in accordance with a P3P policy. Microsoft developed six cookie-blocking settings and offers users a language to create their own settings according to their needs.

Another user agent was published in 2002 by Netscape, the Netscape Navigator 7.[97] In a similar way to Microsoft, the Netscape's user agent was developed to make cooking-blocking decisions on the basis of P3P policies. There is no information available in help files on Netscape's web site.

AT&T Privacy Bird is named as an example for add-on software of the Internet Explorer.[98] A colored icon is shown on the title bar like a warning signal.[99] The bird icon changes color. As it compares the P3P policies with the users' privacy preferences, green indicates a match with the users' privacy preferences. However, red indicates no match and yellow is shown, if web sites have no P3P policies. A human-readable version of the web site's P3P policy is also available for users by clicking on the bird icon.[100]

---

[93] Cf. Cranor, Reidenberg (2002), pp. 7/8.

[94] Cf. for this and the following sentence Cranor et al. (2006), p. 10.

[95] Cf. Cranor, Reidenberg (2002), pp. 7/8.

[96] Cf. for this paragraph Cranor, Reidenberg (2002), p. 8.

[97] Cf. for this paragraph Cranor, Reidenberg (2002), p. 9.

[98] Cf. Cranor, Reidenberg (2002), p. 10.

[99] Cf. for this and the following three sentences PrivacyBird (no date), p. 1.

[100] Cf. Cranor, Reidenberg (2002), p. 10.

2.2.4 Specifications

The P3P 1.1 specifications released in a working group note on the 6th of November 2006[101] give an overview of the syntax and semantics of P3P privacy policies, as well as a mechanism of how to locate and transport privacy policies.[102] The defined P3P vocabulary is used to convey privacy practices represented by P3P policies.[103] Figure 2-1 shows an example of a P3P policy. It consists of two parts. The first part includes the web site's name and contact information and the XML element <ENTITY>, and the second part contains a statement. Based on this example we explain the meanings of these XML elements.

To form a privacy policy, XML elements defined in the P3P specifications are combined. [104] Approximately 36,000 combinations are possible to have, assuming eight major components including several subcomponents. A XML element represents a P3P component, often with multiple subcomponents. In the first line in Figure 2-1 the XML element <POLICIES> appears. Inside this element, there is only one file with one or more P3P policies for performance optimization reasons.[105] It takes only one request to get the policy, whether it is just one policy or even more. The <POLICY> element contains the location of the human-readable privacy policy.[106] The <ENTITY> element provides information about the legal entity making the representation of the privacy practices, including contact information.[107] The <DISPUTES> element illustrates, how to resolve disputes relating to privacy policies.[108] This XML element does not occur in this example. The <ACCESS> element informs users about whether they get information or can address questions to service providers.[109] This element consists of six subcomponents ranging from no data collection by the web site (nonident) to no access to data (none).

---

[101] Cf. Cranor et al. (2006), p. 1.

[102] Cf. Cranor et al. (2006), p. 7.

[103] Cf. Cranor et al. (2006), p. 9.

[104] Cf. for this and the following sentence Cranor, Guduru, Arjula (2006), p. 141.

[105] Cf. for this and the following sentence Cranor et al. (2006), p. 59.

[106] Cf. Cranor (2003), p. 51.

[107] Cf. Cranor et al. (2006), pp. 62 – 64.

[108] Cf. Cranor et al. (2006), pp. 65 – 67.

[109] Cf. for this and the following sentence Cranor et al. (2006), pp. 64/65.

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"name="policy">
        <ENTITY>
                <DATA-GROUP>
                        <DATA ref="#business.contact-
info.online.email">privacy@p3pbook.com
                        </DATA>
                        <DATA ref="#business.contact-info.online.uri">http://p3pbook.com/
                        </DATA>
                        <DATA ref="#business.name">Web Privacy With P3P</DATA>
                </DATA-GROUP>
        </ENTITY>
        <ACCESS><nonident/></ACCESS>
        <STATEMENT>
                <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
                <PURPOSE><admin/><current/><develop/></PURPOSE>
                <RECIPIENT><ours/></RECIPIENT>
                <RETENTION><indefinitely/></RETENTION>
                <DATA-GROUP>
                        <DATA ref="#dynamic.clickstream"/>
                        <DATA ref="#dynamic.http"/>
                </DATA-GROUP>
        </STATEMENT>
</POLICY>
</POLICIES>
```

Fig. 2-1: Example of a P3P policy[110]

The <STATEMENT> element is a container.[111] It includes a <PURPOSE> element, a <RECIPIENT> element, a <RETENTION> element, a <DATA-GROUP> element and optionally a <CONSEQUENCE> element. Beginning with the last named element, <CONSEQUENCE> contains an explanation of handling data in a human-readable text.[112] The <PURPOSE> element includes eleven types of purposes and provides information about the usage of personal data.[113] Each <STATEMENT> element contains also a <RECIPIENT> element.[114] This element includes six types of recipients and gives information about the legal entity distributing personal data. The <RETENTION> element provides information about the type of retention policy.[115] This includes five different types like no-retention and others.

[110] Cf. Cranor (2003), p. 51.

[111] Cf. for this and the following sentence Cranor et al. (2006), p. 68.

[112] Cf. Cranor et al. (2006), p. 71.

[113] Cf. Cranor (2003), p. 52.

[114] Cf. for this and the following sentence Cranor et al. (2006), p. 78.

[115] Cf. for this and the following sentence Cranor et al. (2006), p. 81.

2.2.5 Application of P3P

Basically, a P3P transaction occurs between a web site (web server) visited by a user and a user agent (web browser), as we can see in Figure 2-2. Before the privacy policy of a web site can be interpreted, the P3P policy has to be received first.[116] Therefore, XML-encoded files called P3P policy reference files (P3P PRF) have to be located. There are four mechanisms stating the location of PRFs.[117] The most used mechanism is placing the PRF in a "well-known" location. The files can also be indicated through an HTML linktag, an XHTML linktag or through an HTTP header.

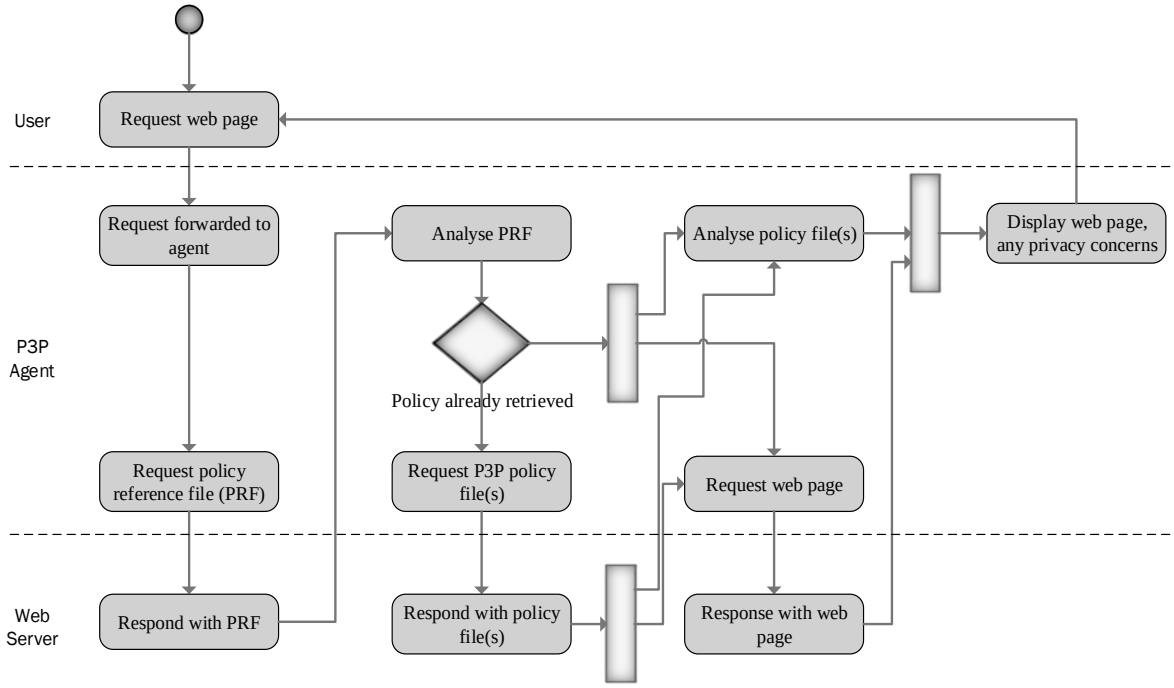

Fig. 2-2: Activity diagram for interaction between user agent and web server[118]

If users visit a web site, the request is forwarded to the user agent, as shown in Figure 2-2. The user agent sends a request to the web server, in order to get the PRF.[119] In reply to this, the web site sends the PRF. For each HTTP resource, the user agent has to determine which P3P policies have to be requested. After determining, whether or not

[116] Cf. for this and the following sentence Cranor et al. (2006), p. 17.

[117] Cf. for this and the following two sentences Cranor et al. (2006), p. 18.

[118] Cf. Reay, Dick, Miller (2009), p. 1105.

[119] Cf. for this and the following five sentences Reay, Dick, Miller (2009), p. 1104.

the policies are already retrieved, the agent sends a request to the web server for those policies, which have not been retrieved yet. Once the server responded, the user agent analyses, whether there are any matches with the user's privacy preferences. The actual web site is also requested and when the web server responses with that site, the user agent displays the requested web site including further information, which are important for the user about the privacy policy.

2.2.6 Adoption Rate

From the beginning of the development, P3P's success was depending on the users' opinions and expectations dealing with this technology.[120] P3P's success is also connected with the will of service providers to deploy P3P policies. In this context, some researchers believe that P3P suffers of a chicken-and-egg problem.[121] The users' demand of P3P will not increase until a widespread introduction of P3P by service providers and service providers are not willing to adopt P3P until there is a greater user demand.

Search API	Total Hits	P3P-enabled Hits
Google	378,183	39,574 (10.46%)
Yahoo!	372,819	39,055 (10.47%)
AOL	371,641	35,251 (9.48%)

Tab. 2-4: Search API results[122]

It seems reasonable to get an overview of the P3P adoption in recent years. But concrete facts and figures are sensitive to the used methodology.[123] An examination of search API (Application Programming Interface) results showed that an average of around ten percent of hits were P3P-enabled hits.[124] Google, Yahoo! and AOL were used to search

[120] Cf. for this and the following sentence Reagle, Cranor (1999), p. 55.

[121] Cf. for this and the following sentence Reagle, Cranor (1999), p. 54.

[122] Cf. Cranor et al. (2008), p. 287.

[123] Cf. Cranor (2008), p. 294.

[124] Cf. for this and the following three sentences Cranor (2008), p. 287.

for “typical” search terms. As shown in Table 2-4, Yahoo! lists more P3P-enabled hits than Google. Although, the difference between the obtained results of those two search APIs is slight.

It is interesting to note that there are differences between search results using search APIs including Google, Yahoo! and AOL concentrating on categories like shopping, health, news and business.[125] Here again, the search APIs vary in P3P-enabled hits. However, much more interesting is the difference between the numbers of categories. The data makes it possible to divide all listed categories into three classes. The first class includes all categories, like business and research, providing P3P-enabled hits with less than ten percent. The second class shows a measured value between ten and twelve percent. Examples for this class are news and entertainment. Categories providing P3P-enabled hits with more than 12 percent include shopping and sports. One thing we can see from these results is that there is a link between occurrence of P3P-enabled web sites and the popularity of a category.

	E-Commerce Top 300	**Forbes**	**Ranking.com**	**Total**	**AT&T 2003 Survey**
Sites	299	495	4885	5553	5728
Sites with P3P	63	17	408	463	538
Percentage of sites with P3P	21.1%	3.4%	8.4%	8.34%	9.4%

Tab. 2-5: P3P adoption rates[126]

From a global point of view, P3P-enabled web sites are found in 49 countries including the United Kingdom, Japan, Australia, Canada and Germany.[127]

[125] Cf. for this paragraph Cranor et al. (2008), p. 290.

[126] Cf. Beatty et al. (2007), p. 67.

[127] Cf. Cranor et al. (2008), p. 292.

When comparing different studies on the subject, figures vary.[128] But it can be seen that the number of P3P-enabled web sites has increased between 2003 and 2006 from approximately 10.25% to 13.59%.

Another study which compared P3P adoption rates, shown in Table 2-5, reveals slightly different values. All values are significantly below the ten percent mark and show a low adoption of P3P.[129]

2.2.7 Benefits and Drawbacks

The introduction of P3P increases the users' sensitivity for privacy issues.[130] For example, in Figure 2-3 we see the influence of P3P on the users' relationship to privacy policies. There were six categories examined. They ranged from users, who never read privacy policies - when visiting web sites - to users, who read most privacy policies. Looking at the figure, you notice that users are more aware of privacy policies after installing Privacy Bird. Before installing the user agent, either users never used to read privacy policies or just occasionally did.

P3P also gives users a sense of security having privacy icons that inform them, when privacy policies differ from their privacy preferences.[131]

Another positive aspect is the improvement of privacy policies.[132] Because of the multiple-choice options of P3P policies, service providers have to be more specific and explicit about their privacy practices.

Compared to other PETs with P3P, users are able to make better decisions based on the P3P policies' depth of detail.[133]

Another decisive argument for using P3P is the automatic deployment of privacy policies to users. Deviations from users' privacy preferences can be automatically detected and displayed.

There are not only benefits of P3P. A major problem is that P3P is too complex.[134] As we have seen before, there are many specifications and an increased number of

[128] Cf. for this and the following sentence Cranor et al. (2008), p. 294.

[129] Cf. Beatty et al. (2007), p. 67.

[130] Cf. for this and the following sentence Cranor, Arjula, Guduru (2002), p. 9.

[131] Cf. Cranor (2006), p 172.

[132] Cf. for this and the following sentence Cranor (2003), p 55.

[133] Cf. for this and the following two sentences Beatty et al. (2007), p. 69.

combinations. P3P's difficult handling can prevent users from using it.[135] It was suggested that eight categories would be enough to be more manageable for programmers.[136]

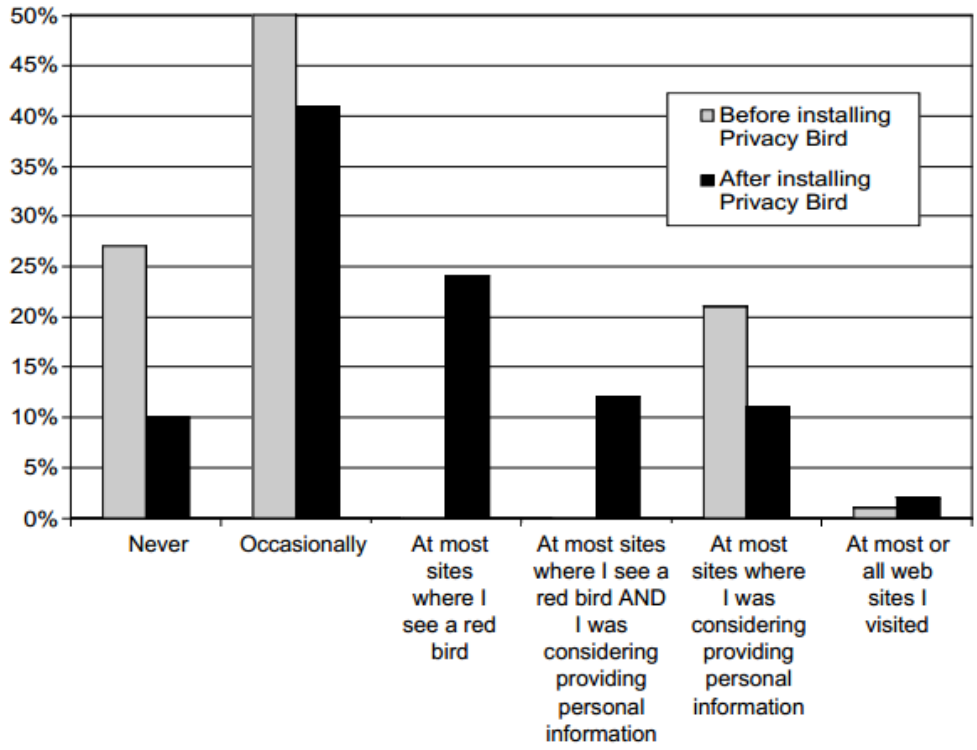

Fig. 2-3: Users responds on AT&T Privacy Bird[137]

Another problem is that users often have no experience with PETs in general.[138] There is no need for them to adopt P3P, although this PET can decrease users' concerns.
If users might be able to trial P3P in a limited time, the PET could be more adopted.[139] Instead, users have to invest plenty of time and effort to install a P3P user agent and learn how to use it.

[134] Cf. for this and the following sentence Schwarz (2009), p. 8.

[135] Cf. Beatty et al. (2007), p. 69.

[136] Cf. Schwarz (2009), p. 8.

[137] Cf. Cranor, Arjula, Guduru (2002), p. 9.

[138] Cf. for this and the following sentence Beatty et al. (2007), p. 69.

[139] C. for this and the following three sentences Beatty et al. (2007), p. 70.

P3P observability – users seeing the benefits of this technology – is too low. If users do not understand the advantages of using a certain technology, they will invest neither time nor effort to use P3P.

Online service providers are concerned that using P3P leads to more additional liability.[140] Privacy advocates note that P3P will not improve the protection of users' personal data.

As we have seen before, there is a slight increase of the P3P adoption rate.[141] However, considering the fact that P3P's development started in the mid-nineties of the last century the adoption rate is still too low.[142]

Considering the stated benefits and drawbacks, there are not only advantages using P3P. There are lots of weaknesses, which we have to analyze to learn from the work that was done.

[140] Cf. for this and the following sentence Cranor (2003), p 54.

[141] Cf. Beatty et al. (2007), p. 67.

[142] Cf. Cranor et al (2008), p. 321.

3. Analyzing P3P

3.1 Literature Search Providing Responses

Through the search process we got many promising search results. Therefore, we had to eliminate some of the listed papers. Since we are focusing on the P3P development process and the users' point of view in our analysis of P3P, we concentrated on abstracts and then in addition on headlines of the papers to get an impression, what aspects these papers include. Thus, we focused on important aspects of the analysis and determined overlaps in different papers.

3.2 P3P Development Process – A Critical Reflection

3.2.1 Successful Implementation of A "Social Protocol"[143]

As a "social protocol"[144] P3P improves the users' privacy when browsing the Internet.[145] P3P is a successful first step to enable users to be informed about how their personal data is used, which data is collected and what consequences this leads to. Users need to create an understanding of these consequences. P3P enables users to increase control over their personal data and warn them, when web sites' privacy practices could damage the users' privacy. Users gain an insight for what reasons they share their personal data with third parties and who this third party is.

Developing P3P was challenging, as a major goal was to merge different legal and social settings.[146] There were developers from America, Europe and Asia involved in the design process of P3P. Under a global influence, P3P changed from being e-commerce oriented to broadly oriented.

3.2.2 PET of Notice and Choice

As we have seen before, P3P is a narrowed concept of information privacy protection.[147] It is a PET of notice and choice – meaning that users' personal data is

[143] Hochheiser (2002), p. 276.

[144] Hochheiser (2002), p. 276.

[145] Cf. for this paragraph Ackerman (2004), p. 435.

[146] Cf. for this and following two sentences Reagle, Wenning (2000), p. 7.

[147] Cf. for this and following sentence Hochheiser (2002), p. 287.

collected and used anyhow. Notice stands for providing P3P policies.[148] Choice describes the users' ability to choose their privacy preferences. Consequently, P3P is not a PET to hinder service provider from collection and usage of personal data.[149] Users are only informed by P3P, whether or not a web site does collect and use their personal data to provide transparency. It is not a tool assessing web site privacy policies whether they are acceptable for users or not.[150]

As we have seen in 2.1.3, P3P does not support all of the FTC privacy principles, only two out of eight.[151] The remaining principles are only limitedly supported. For instance, the Individual Participation Principal is represented by the <ACCESS> element.

3.2.3 Delay of P3P

P3P suffers from an unusually long development process.[152] As we have seen in chapter 2.2.2, it took around ten years. Constantly, several parties did a critical reflection of the P3P development process to help W3C and the Specification working groups to improve P3P.[153] This stage was rather time-consuming and exertive. Furthermore, the P3P specifications were affected by various changes.[154] For instance, XML Schemas and other specifications were developed during the design process of P3P. Both development processes had to be coordinated and harmonized. Also, a patent dispute regarding P3P has had a negative impact on the implementation including all participants. All these aspects - including the removal of OPS and the protocol for policy negotiation and data-transfer - led to a delay of P3P.

Open Profiling System (OPS)

There was criticism that the Open Profiling System (OPS) was part of P3P.[155] OPS refers to the exchange of profile information – often requested information by a web site

[148] Cf. for this and following sentence Hochheiser (2002), p. 283.

[149] Cf. for this and following sentence Hochheiser (2002), p. 287.

[150] Cf. Hochheiser (2002), p. 283.

[151] Cf. for this and following two sentences Hochheiser (2002), p. 283.

[152] Cf. Cranor (2002b), p. 4.

[153] Cf. for this and following sentence Cranor (2002b), p. 4.

[154] Cf. for this and following three sentences Cranor (2002b), p. 5.

[155] Cf. Schwarz (2009), p. 4.

- between two parties under the users' permissions.[156] It is about a way of communication, including storing and releasing the users' personal data, which can be trusted by (a) individuals and services, (b) services mediated by individuals and (c) individuals. Even before the P3P specification group could start with its work, concerns rose regarding OPS.[157] These concerns revolved around the fear that OPS would not contribute to privacy protection. Accordingly, companies wanted to use OPS to get more control over the users' choices. This indicates the difference between the terms 'privacy' and 'privacy practices', which users do not conceive. As a result of that, it is difficult to understand how it is possible that P3P enables web sites to give users an impression of privacy, and at the same time these web sites can collect the users' personal data. Finally, OPS was removed from P3P.

Policy Negotiation and Data-Transfer

The protocol for policy negotiation and data-transfer was removed from P3P 1.0 specification as a result of a working group decision.[158] It was stated that the protocol was too complex and therefore it was considered to be a threat to the implementation process and the first rapid prototype of P3P. Also, representatives from industry had no interest in the data-transfer mechanism. In contrast to Europe, the US was not convinced of the protocol for negotiation and data-transfer. Since the policy negotiation was removed, it is impossible for service providers to come up with different privacy policies.[159]

3.2.4 Analyzing P3P Components

As the P3P development process includes the development of P3P components as well, we concentrate on P3P policy, APPEL and P3P vocabulary focusing on problematic issues. Before focusing on the users' point of view in chapter 3.3, we determine the disadvantages of these components, as it reveals problems of developers and implementers.

---

[156] Cf. for this and following sentence Hensley et al. (1997), p. 2.

[157] Cf. for this and following five sentences Schwarz (2009), p. 4.

[158] Cf. for this and following three sentences Reagle, Wenning (2000), p. 5.

[159] Cf. Tatli (2007), p. 246.

P3P Policy

A P3P policy is static.[160] Dynamic behaviors are not part of the P3P specifications. For instance, when using a location provider, users are concerned to give too much personal information away. There are just two options, either users share their location directly or not. It may be possible to "blur"[161] users' locations and using zip codes instead. Unfortunately, this cannot be expressed in P3P.

Complexity of the P3P Vocabulary and APPEL

Both the structure of the privacy policy vocabulary and APPEL are complex.[162] First, the privacy policy vocabulary needs complexity to assist service providers in building their privacy policies correctly. Second, APPEL also needs complexity to assist users in building their privacy preferences specifically. That implies a conflict between the intention of P3P and users' possibilities to handle the amount of choices properly.

Not all privacy issues can be addressed by the P3P vocabulary.[163] It just provides information about used privacy policies.[164] For instance, users like to see more information about the consequences, when they release information to a web site or information about companies that collect their personal data. Unfortunately, these aspects cannot be implemented in a user agent.

P3P's vocabulary could not be tested by end-users to determine differences between the users' expectations and P3P's definitions.[165]

3.2.5 Critical Reflection on P3P User Agent Prototypes

As mentioned before, four P3P prototypes have been developed.[166] Each prototype pursues a different goal oriented by the latest P3P specifications.

The first prototype of a user agent was developed by W3C in 1997.[167] It was demonstrated at the US Federal Trade Commission meeting.[168] Feedback was given that

---

[160] Cf. for this paragraph Tatli (2007), p. 246.

[161] Tatli (2007), p. 246.

[162] Cf. for this paragraph Hochheiser (2002), p. 288.

[163] Cf. Cranor, Guduru, Arjula (2006), p. 168.

[164] Cf. for this and following two sentences Cranor, Guduru, Arjula (2006), p. 167.

[165] Cf. Hochheiser (2002), p. 290.

[166] Cf. for this and following sentence Cranor, Guduru, Arjula (2006), p. 143.

users were overwhelmed by the number of choices for privacy preferences.[169] Standard settings for privacy preferences were recommended.[170] It would facilitate the users' decisions, if they only had to choose between privacy settings instead of selecting privacy preferences individually. This prototype informed users via pop-up window with an option to ignore the warning, if their privacy preferences did not match with a webs site's privacy policy[171]. It quickly became evident that users would be stressed out by these pop-up windows. A solution for this was sought.

Therefore, another user agent prototype – called the Privacy Minder - was developed by AT&T Research in 1999.[172] Recommended settings were implemented in the form of APPEL rules. It succeeded in making it easier for users to select their privacy preferences. It was a step forward, but another problem came up. Choosing the right setting was difficult for users, as they did not know, which of those fitted in best with their privacy preferences. An integrated floating toolbar including menus to select a privacy setting replaced a pop-up window. Instead, users were now informed by symbols about whether or not a web site's privacy policy matched with the users' privacy preferences.

Later the AT&T/Microsoft P3P browser helper object was implemented for the Internet Explorer 5.[173] It was tested on P3P policies of real web sites. This prototype focused on conditions – encoded into APPEL rule sets - of providing warnings to users. A list of conflicts between the users' privacy preferences and the web sites' privacy practices is shown to users. The implementation concentrated on an interface, where users are able to select their privacy preferences on just one screen. Efforts were made to ensure that the main aspects of privacy policies were shown, as it was impossible to represent all combinations of privacy practices. These aspects include the collection of users' personal data, the purpose of the collection of personal data and sharing personal data with third parties represented by XML elements data, purpose and recipient. It was focused on 12 data practices, which users could form a strong opinion on. Then, it

[167] Cf. Cranor, Guduru, Arjula (2006), p. 144.

[168] Cf. World Wide Web Consortium (1997), p. 1.

[169] Cf. Cranor, Guduru, Arjula (2006), p. 144.

[170] Cf. for this and following sentence Cranor, Reagle (1998), p. 9.

[171] Cf. for this and following sentence Cranor, Guduru, Arjula (2006), p. 144.

[172] Cf. for this paragraph Cranor, Guduru, Arjula (2006), p. 144.

[173] Cf. for this paragraph Cranor, Guduru, Arjula (2006), p. 145.

would be easier for them to select their privacy preferences. However, users had problems to choose acceptable data practices.[174] After a discussion with the focus group, it was identified that users were able to select unacceptable rather than acceptable data practices.

The AT&T browser helper object prototype was developed to test the usability of the interface in 2001.[175] For setting their privacy preferences, users had to make 13 choices on a settings window. High, medium and low settings were developed, in order to simplify the selection of privacy preference settings for users. However, the usability test showed that to users the meaning of high, medium and low was not clear. In addition, to reduce the use of technical terminology new wordings were defined. A colored "hand symbol"[176] in the toolbar informed users, whether their privacy preferences matched the web sites' privacy practices. The aim was to raise the users' awareness for the software providing important information. However, the colors were noted more often rather than the shape of the symbol. The test conducted that users were still confused when making privacy decisions, as they had problems understanding certain terms. Also, users expect the privacy settings to be in one place and were confused that they were not.

3.3 Users Point of View

3.3.1 User Concerns

Asking users - who have knowledge about PETs - about their concerns regarding information privacy, when browsing the Web, approximately one half of users is very concerned about their information privacy and one tenth is not concerned.[177] The others are concerned, but not so much. Numbers shift, when users were asked about their concerns regarding specific web site data practices. 98% of them are concerned about web sites sharing their personal data with third parties. 96% of the users are concerned, when web sites collect their personal data to create information about their browsing

[174] Cf. for this and following sentence Cranor, Guduru, Arjula (2006), p. 146.

[175] Cf. for this paragraph Cranor, Guduru, Arjula (2006), p. 147.

[176] Cranor, Guduru, Arjula (2006), p. 147.

[177] Cf. for this and following five sentences Cranor, Arjula, Guduru (2002), p.7.

activities, habits, and others. 65% of users are concerned when web sites store their personal data for profiling purposes without any connection to their name and the like.
Asking users about their attitude regarding cookies, almost 80% of them are concerned about cookies and the others are either not concerned or do not know, what cookies are.[178] It hardly surprises that users - occupying themselves with PETs – fear the use of cookies. Also, more than half of them do not know, what third-party cookies are, whether they have heard of them or not. Fortunately, the others have great knowledge about it.
As we have seen before, a major problem is that P3P suffers from not being adopted.[179] If users rely on P3P user agents, when browsing the Internet, they have great expectations. Many users – when using P3P user agents - think that P3P would be more adopted by them, if web sites provided more P3P privacy policies.[180] User agents lose their value, if they mostly determine that web sites are not yet P3P-enabled.[181]

3.3.2 Win/Win Situation

P3P was considered as a threat by many companies, as it also enables users to get some awareness of how these companies collect and store the users' personal data.[182] Some companies pointed out that they see a conflict between cross-selling and privacy protection.[183] They feared that users acquire knowledge about how they can stipulate conditions, under which users can share their personal information with third parties. A win/win situation for users and companies could not exist anymore. Studies showed that users are not interested in sharing their personal data for the purpose of analyzing their browsing behavior, but are willing to share their personal data to fulfil transactions.

3.3.3 P3P Components from User Perspectives

During the development process of P3P, developers and implementers had to consider the complexity of P3P components. As users operate with the P3P protocol, it is

[178] Cf. for this and following three sentences Cranor, Arjula, Guduru (2002), p.7.

[179] Cf. Beatty et al. (2007), p. 68.

[180] Cf. Cranor, Arjula, Guduru (2002), p.8.

[181] Cf. Cranor, Arjula, Guduru (2002), p.7.

[182] Cf. Schwarz (2009), p. 6.

[183] Cf. for this and following three sentences Lee, Speyer (1998), p. 6.

necessary to know, what kind of problems they have, when dealing with certain components of the P3P standard. That is why we concentrate on privacy policies, then on privacy preferences and settings, including the 'Yes' and 'No' options and APPEL. Also, we emphasize that there is no mechanism integrated in P3P for a warning, in case web sites do act contradictory to their privacy policies[184].

Privacy Policies

As we have seen before, P3P specifications provide the syntax to build P3P policies.[185] Although there are around 36,000[186] combinations of components, it is still limited. Possibly, these combinations are not enough to express all privacy policy information. From the users' point of views, designers have to find a solution for a trade-off between a PET representing complex privacy policy information and an easy display of these information for users. On the one hand, it is on behalf of users that all privacy policies information can be represented, so that they have access to all information they need to make responsible decisions. On the other hand, it is likely that users are to be overexerting, when using a tool to select their privacy preferences and they have to fully understand, what privacy policy information stand for.

Privacy Preferences

Sometimes users make trade-offs regarding their conception of privacy.[187] For instance, usually, when users visit a web site, they do not want the site to collect their personal data for profiling purposes. It depends on what kind of web sites users visit. On the one hand, users are willing to share their personal data for monitoring and profiling, if web sites make personalized recommendations regarding their purchasing behavior including books. On the other hand, users feel different about the same matter when visiting a medical web site, as they do not want to be monitored and profiled. It seems that their personal data is now much more valuable for them than before.

---

[184] Cf. Hochheiser (2002), p. 288.

[185] Cf. for this paragraph Cranor, Guduru, Arjula (2006), p. 142.

[186] Cf. Cranor, Guduru, Arjula (2006), p. 141.

[187] Cf. for this paragraph Cranor, Guduru, Arjula (2006), p. 142.

Privacy Settings

When using a Privacy Bird, privacy settings have to be configured.[188] Asking users, whether they ever changed their settings, around three quarters of them reply that they did change the setting once or several times and add that they were easy to change. The others never changed their settings. Comparing P3P experts – users who have a great amount of experience with P3P – with non-experts, the former change their privacy settings more often to test the user agent pursuing the best possible outcome.

For some users the privacy setting options were too difficult. It was suggested to support users by providing a dialog to supply information to users.[189]

As Privacy Bird offers an optional sound effect, users have different opinions about it.[190] Around half of the users turn the sound off. Two thirds of the remaining users tune the settings in such a way that every different color bird plays a different sound. The others tune the settings to provide sound at all web sites.

Yes and No option

While the P3P working group was not willing to let the idea of transparency go, a few companies decided that this was not the way they want their relationship with consumers to be.[191] For instance, companies want P3P to define three instead of only two options regarding data collection, 'Yes' (data is collected), 'No' (data is not collected) and 'Maybe' (data might be collected). To realize the concept of transparency, P3P just plan to have two options as the 'Maybe' is understood as a 'Yes' by users. Consequently, there would be no need to have a 'Maybe' option.

APPEL

What seems to be an easy-to-use language, can lead to problems for users.[192] The main problem is that it is almost impossible to build simple privacy preferences the right way. Even if it seems to be correct, it may stand for a different goal. A P3P policy includes more than one statement. If only one of the statements of the P3P privacy policy

[188] Cf. for this paragraph Cranor, Arjula, Guduru (2002), p.8.

[189] Cf. Cranor, Arjula, Guduru (2002), p.8.

[190] Cf. Cranor, Arjula, Guduru (2002), p.8.

[191] Cf. for this paragraph Schwarz (2009), p. 6.

[192] Cf. for this and following three sentences Agrawal et al. (2003), p. 631.

matches the defined APPEL rule, the rule fires – meaning either the P3P policy matches users' privacy preferences or it does not[193]. The rule draws a wrong conclusion. Users can only specify, "what is unacceptable"[194] instead of "what is acceptable"[195].[196]

No Technical Mechanism for Warning

There is no technical mechanism provide by P3P that warns users, when web sites do act contradictory to their privacy policies.[197] The problem is that users are not aware of this lack of such a mechanism. They run the risk to make decisions based on wrong assumptions.

3.3.4 P3P User Agents – Analyzing Interfaces

As mentioned before, using P3P is too complicated for users, regarding for example building their own privacy preferences or even creating privacy policies.[198] As a result of these emerging concerns, P3P tools like P3P user agents and P3P policy generators were developed to support users and reduce their concerns. Of special interest are user agents.

To achieve the best possible impact of P3P, the end-user tool has to be easy-to-use and understand able.[199] Therefore, designers of P3P user agents have to look for a trade-off between an easy-to-use tool with clearly understandable requirements and a tool that provides all necessary information about a web sites privacy practices. To counteract this problem, it is possible to simplify the P3P vocabulary and APPEL. One the one hand, this would lead to a reduction of complexity for a potential end-user tool. On the other hand, this oversimplification could lead to the users' distraction. Under those circumstances users are not able to make the right decision anymore.

---

[193] Cf. for this and following sentence Agrawal et al. (2003), p. 630.

[194] Agrawal et al. (2003), p. 637.

[195] Agrawal et al. (2003), p. 637.

[196] Cf. Agrawal et al. (2003), p. 637.

[197] Cf. for this paragraph Hochheiser (2002), p. 288.

[198] Cf. for this and following sentence Cranor (2002b), p. 14.

[199] Cf. for this paragraph Hochheiser (2002), p. 290.

Web browsers have design problems regarding the interface.[200] For instance, having such problems in the Microsoft Internet Explorer (IE) and Netscape Navigator leads to confused users, who are not able to get easy access to relevant information they do comprehend. It is difficult for users to get to the control panel of the IE6's P3P interface.[201]

In contrast to IE6, the AT&T Privacy Bird is a browser plug-in and is able to handle more detailed policies to describe privacy practices.[202] The major problem of the Privacy Bird is that users first have to download and then install the AT&T tool. This could have a deterrent effect on users.

To analyze interfaces of user agents more precisely, we concentrate on Privacy Bird and Microsoft Internet Explorer 6.

Privacy Bird

The four prototypes developed during the development phase formed the basis for another user agent called Privacy Bird.[203] Privacy Bird is an add-on for different versions of Internet Explorer and was intended to be a support for users.[204] When a red bird appears, users should read the privacy policies to gather more information. As a result, it is no longer necessary for users to read privacy policies at each web site.

Asking users, they confirm the Privacy Bird as an easy-to-use tool.[205] Aside from that, developers indicate that there is still much room for improvement. Users can select their privacy preferences by means of a specification interface.[206] On the one hand, either high, medium or low privacy settings can be chosen. On the other hand, users can customize their own privacy settings.

Also, there tends to be a misunderstanding regarding the colored bird icon.[207] Users did not realize the correct meaning of the yellow icon. They assumed that a yellow icon

---

[200] Cf. for this and following sentence Hochheiser (2002), pp. 290/291.

[201] Cf. Hochheiser (2002), p. 291.

[202] Cf. for this paragraph Hochheiser (2002), p. 291.

[203] Cf. Cranor, Guduru, Arjula (2006), p. 147.

[204] Cf. for this and following two sentences Cranor, Arjula, Guduru (2002), p.8.

[205] Cf. for this and following sentence Cranor, Arjula, Guduru (2002), p.8.

[206] Cf. for this and following two sentences Cranor, Guduru, Arjula (2006), p. 148.

[207] Cf. for this paragraph Cranor, Guduru, Arjula (2006), p. 168.

appears, when a web site's privacy policy is not good enough to show a green icon but also not bad enough to show a red one.

Microsoft Internet Explorer 6 (IE6)

In contrast to Privacy Bird, IE6 provides only four privacy options for users.[208] Also, the wording used in the interface includes more jargon that is confusing for users and experts as well. The privacy report provided by IE6 is similar to the Privacy Bird policy summary and is much more difficult to read as it includes paragraphs instead of bulleted items for P3P elements.[209]

3.3.5 Comparing P3P User Agent

Asking users, the wording used in Netscape 7 is clearer compared to Internet Explorer 6.[210] However, finding the P3P –related menus was more complicated in Netscape than in IE6.

The main objective of user agents is to provide information to users.[211] Users believe that it is easier to work with Privacy Bird than reading human-readable privacy policies, the reason for that being that privacy policies are hard to understand for users, as the used wording is too difficult for non-experts. It is interesting to know, how users would feel about user agents, when privacy policies were formulated more briefly and simply. When using IE6, users get information slower and not as accurate compared to reading a privacy policy.[212] However, they pointed out that it is much easier using a user agent than to actually read a web sites' privacy policy. When evaluating the accuracy of user agents fining information, IE6 is approximately in the same position in the score. Generally, users need more time working with user agents like Privacy Bird, when they do not have much experience in doing so, compared to users, who are familiar.[213] Comparing Privacy Bird with IE6, users reported that Privacy Bird is more useful, easier in regards to understanding policy summaries and finding information than

[208] Cf. for this and following sentence Cranor, Guduru, Arjula (2006), p. 157.

[209] Cf. Cranor, Guduru, Arjula (2006), p. 158.

[210] Cf. for this and following sentence Cranor, Guduru, Arjula (2006), p. 162.

[211] Cf. for this and following two sentences Cranor, Guduru, Arjula (2006), p. 163.

[212] Cf. for this and following two sentences Cranor, Guduru, Arjula (2006), p. 164.

[213] Cf. Cranor, Guduru, Arjula (2006), p. 165.

IE6.[214] Also, they believe that Privacy Bird is more likely to be used in the future and therefore would recommend it to a friend. For instance, the Privacy Bird policy summary is easier to read and understand and well-structured. In contrast, the IE6 policy summary was seen as too difficult to get exact information fast.

Additionally, there are differences between user agents in presenting information.[215] In contrast to Privacy Bird, IE6 presents information on web site data retention policies. Privacy Bird provides information about opt-in and opt-out choices. Also, a human-readable consequence field, where information about each P3P statement displayed is provided by web sites. While IE6 provides information about data that is collected by web sites pooled in categories, Privacy Bird makes information about all data elements available.[216]

3.3.6 Reducing Precision of P3P Terms

Implementers of user agents have to consider their product to be useable for non-experts.[217] As a result, they have to simplify the wording. They bundle P3P elements in order to define a single term for a few P3P elements. For instance, when combining P3P elements of the same type, recipients' choices are narrowed down from six to two.[218] Despite the improvement of reducing complexity there is still a limit. The users' privacy preferences cannot be represented by a single package of P3P elements. As a result, a certain complexity of the P3P vocabulary is needed.

When users visit web sites collecting health and medical information about them – which users often find reasonable – complexity might be reduced, if warnings were limited, including profiling, marketing and others.[219] It would help users, if they only get warnings, when health and medical web sites collect their personal data for an unreasonable purpose.

---

[214] Cf. for this and following three sentences Cranor, Guduru, Arjula (2006), p. 166.

[215] Cf. for this and following three sentences Cranor, Guduru, Arjula (2006), p. 166.

[216] Cf. Cranor, Guduru, Arjula (2006), p. 166.

[217] Cf. for this and following two sentences Cranor, Reidenberg (2002), p. 11.

[218] Cf. for this and following three sentences Cranor, Guduru, Arjula (2006), p. 153.

[219] Cf. for this and following sentence Cranor, Guduru, Arjula (2006), p. 153.

P3P Policy Statements and User Agent Simplifications

The simplification of P3P terms leads to the users' confusion and "consumer deception"[220].[221] If user agents misrepresent privacy statements due to inaccuracy, users might be at risk.[222] When companies set their privacy practices and user agents 'translate' these information for users, there is no guarantee that companies do not provide users with false and inaccurate information or even respect their own privacy statements.[223] In result, user agents are not capable – when simplified P3P terms are used – of providing accurate privacy information to users.[224] Even if web sites act according to their privacy practices, there is still a chance that user agents get the P3P statement translation wrong and cause the users' false conclusions. It is the responsibility of developers and implementers to make sure that users are not harmed, when relying on misrepresented P3P statement translations. The wrong development of user agents not only results in the users' harm, but in the defamation of web sites. Web site developers fear that the inaccurate translation of the P3P statements might lead to their liability and the defamation of a business. A web site's reputation might be compromised, if user agents provide users with false information.[225] For instance, if user agents trivialize the used data collection policy of a web site, users might think of it as a fraud.

[220] Cranor, Reidenberg (2002), p. 15.

[221] Cf. Cranor, Reidenberg (2002), p. 15.

[222] Cf. Cranor, Reidenberg (2002), p. 16.

[223] Cf. Cranor, Reidenberg (2002), p. 15.

[224] Cf. for this and following four sentences Cranor, Reidenberg (2002), p. 16.

[225] Cf. for this and following sentence Cranor, Reidenberg (2002), p. 17.

4. Design Principles

4.1 Definition

Design principles are generalized suggestions for improvement, which first are deduced from occurred problems of P3P, then assessed and finally tested.[226] Note that in this thesis we do not have the opportunity to test the deduced design principles.

4.2 Appropriate Design Principles

4.2.1 Process Model

The P3P development process, as we have seen in chapter 3.2.3, lasted too long. There are indications of a sequential development, as the P3P development process was divided into sequential phases like requirements analysis, software design, implementation, and others.

One way to shorten the development process might be to develop a PET like P3P in an agile development process. There are some positive aspects about an agile development process in contrast to the traditional system development.

Not all requirements have to be determined in the beginning of the development process.[227] When involving end-users in this process, their feedback can be of great benefit to designers and implementers. As a result, existing requirements can be extended or may be added at any time to improve the software product. That is one great advantage of the agile development. Furthermore, the weighting of requirements - depending on cost and time factors, as well as the users' feedback - is often difficult during a traditional system development. The involvement of the end-user greatly is a vantage prioritized in the first principle of the agile manifesto.[228] The P3P development process would have benefited from such a vantage. Designers could have acted earlier, in order to achieve a better deployment of P3P.

[226] Cf. Widjaja, Gregory (2012), p. 6.

[227] Cf. for this paragraph Laudon, Laudon, Schoder (2010), p. 942.

[228] Cf. Cunningham (2001), p. 1.

4.2.2 Involvement of End-Users

It is necessary to include end-users in the development process to ensure that all implemented features are accurate. The example of P3P's vocabulary - which was never tested by end-users – shows that it would have helped, if developers had been able to detect the differences between the P3P definitions and users' perceptions.[229] Testing P3P with a group of representatives of Internet users is not possible.[230] P3P specifications were developed without any end-user influence.[231]

4.2.3 PET Supporting All Privacy Principles

As users rarely differentiate between different privacy principles, as presented in chapter 2.1.3, it could be a step forward to think about the development of a PET that supports all listed principles.[232] As we have determined in chapter 3.2.2, P3P intended to be 'only' a PET of notice and choice, but many users are not aware of this constraint.

4.2.4 Keep A PET Like P3P Simple

As we have seen before, the P3P standard - including too many categories for data-type and for data-use – is too complex.[233] The number of different categories leads too many combinations. As a result, users and service providers feel overwhelmed. A P3P standard, which is much simpler, might receive more acceptances by users.

4.2.5 Rehabilitation of P3P User Agent's Trustworthiness

As we have seen in chapter 3.3.6, user agents' trustworthiness is compromised as modifications of P3P terms are done, in order to simplify them.[234] These modifications lead to less accurate P3P statements and the users' confusion as well as to a possible

[229] Cf. Hochheiser (2002), p. 290.

[230] Cf. Hochheiser (2002), p. 290.

[231] Cf. Cranor, Reidenberg (2002), p. 19.

[232] Cf. Hochheiser (2002), p. 283.

[233] Cf. for this paragraph Schwarz (2009), p. 8.

[234] Cf. Cranor, Reidenberg (2002), p. 18.

defamation of web sites.[235] Suggested solutions might be the user agents' documentation and a certification, which we will deal with in the following.

Documentation

To increase transparency of how user agents translate the web sites' P3P statements it might be useful to provide documentation.[236] As a result, users are given the possibility to realize the user agents' simplifications. Also, service providers and consumers are enabled to understand the user agents' reactions. Apart from this, it may be helpful to manage a platform for the users' feedback. The users' opinion may be conducive to developers and implementers to warn them about misrepresented translation of P3P statements. However, increasing transparency will not solve the problem. It is an option to support users and web sites to get aware of the constraints of trustworthiness.

Certification

The accuracy of user agents can be ensured with a certificate - a kind of assurance for all parties including users, web sites and implementers.[237] Users and web sites benefit from a certificate, as each party interacts based on the understanding of terms used by user agents. Web sites can be certain that their privacy policies are correctly represented by user agents. Implementers benefit of the use of a certificate, as it assures no defamation of web sites. Nevertheless, it is difficult to develop criteria, which ensure the user agents' accuracy.

[235] Cf. Cranor, Reidenberg (2002), pp. 16/17.

[236] Cf. for this paragraph Cranor, Reidenberg (2002), p. 18.

[237] Cf. for this paragraph Cranor, Reidenberg (2002), p. 18.

5. Discussion

All points of the P3P analysis, which are listed in chapter 3, belong to different aspects of P3P. The key aspects of the P3P development process analysis include the delay of P3P and the critical reflection of P3P user agent prototypes. As the analysis in chapter 3 clearly shows, the shortcomings predominate the advantages of P3P. Despite the fact that the major idea of designing a PET supporting users to better understand web site privacy practices is good[238], it is also too complex[239]. All of the points mentioned above in chapter 3.2 are relevant, but there are some points, which are of key importance to the failure of P3P. First of all, to name the delay of P3P including the P3P specifications, which were affected by various changes[240] as well as the removal of OPS[241] and the protocol for policy negotiation and data-transfer[242]. Second, the P3P user agent prototypes, which were developed during the P3P development process, are of high importance to the progress of P3P, as all four prototypes pursued different goals. It was possible to improve the next prototype with the weaknesses of the predecessor kept in mind. The key aspects of the analysis of the users' point of view include the analysis of user agent interfaces, and the simplification of P3P terms. The P3P user agent Privacy Bird performed best among many user agents according to the users' option.[243] Other important shortcomings of P3P are that user agents are not capable – when simplified P3P terms are used – of providing accurate privacy information to users.[244]

Each of the listed design principles in chapter 4 has their benefits and drawbacks. Starting with the development process, the agile development process, as suggested in chapter 4.2.1, has quite a lot advantages and might lead to an improvement, according to the length of a development process as well as of the resulting quality of the software product. However, it is only one possibility that can be chosen. There are a lot of other different software development processes to consider depending on the PET that is developed.

---

[238] Cf. Ackerman (2004), p. 435.

[239] Cf. Hochheiser (2002), p. 288.

[240] Cf. for this and following three sentences Cranor (2002b), p. 5.

[241] Cf. Schwarz (2009), p. 4.

[242] Cf. Reagle, Wenning (2000), p. 5.

[243] Cf. Cranor, Guduru, Arjula (2006), p. 166.

[244] Cf. for this and following four sentences Cranor, Reidenberg (2002), p. 16.

Involving end-users in the development process, as presented in chapter 4.2.2, might have its benefits, as the end-users' feedback can help to enhance the development process and make it more effective and efficient. The question remains, when to involve these end-users and how. The favored feedback has to be of high-quality to be helpful to developers. As a result, end-users have to be representative and should not consist only of experts or non-experts.

The suggestion of developing a PET that supports all privacy principles is an ideal state. For that reason, it is unrealistic to design a PET supporting all privacy principles instead of focusing on major ones, as it was done with P3P. However, the question remains, how many privacy principles should be supported by one PET.

The problem of keeping a PET simple, stated in chapter 4.2.4, might help users to better handle a PET, but carries problems and threats. Designing a PET that is too simplified and cannot fulfill its desired functions would be useless.

The recommendation of the user agents' documentation and a certification, presented in chapter 4.2.5, might be useful and helpful to users as well as service providers. It is difficult to users and service providers to agree on certain terms, which both sides benefit from.

6. Conclusion

Based on the results, it can be concluded that there are too many different reasons, why P3P never could be successful. However, there are some design principles given in this thesis that help to prevent a few mistakes from being made again.

At an early stage of this thesis, we realize that P3P failed not only, because it was not adopted as it was supposed to, as we have seen in chapter 2.2.6, but as it missed the users' assumptions of a PET improving their information privacy and decreasing their concerns about their personal data. As we have seen in chapter 2.1.3, P3P does not support all privacy principles of a PET, but to be successful, it should have. Further research on the subject might focus on a PET that supports all privacy principles. The research field information privacy and the resulting users' concerns are too complex to be simplified in a way that they can be categorized specifically to finally develop a PET that can be exactly tailored to cover all the users' problems.

The aspects of the analysis of P3P listed in chapter 3 are just the most important ones. Literature does in fact provide more aspects, which we did not cover, as it would have exceeded the extent of this thesis. Furthermore, the analysis shows that, classifying the aspects in terms of strengths and weaknesses, it is not expressive enough. For that reason, we decided to structure the analysis in different parts of P3P and analyze, what about which part of it is an advantage or a disadvantage.

Afterwards, it turned out to be the correct choice to split the chapter of the P3P analysis in two parts, first concentrating on the P3P development process and then focusing on the users' point of view. The ideas and suggestions of developers and implementers led to results that users often did not understand or rendered them unable to handle P3P correctly. Without an appropriate end-user support during the P3P development process, it is difficult to design a PET for users, which they can accept or they are even willing to.

Users dealing with PHS are aware of the risks and dangers that are associated with sharing their personal data with third parties more than other users, when browsing the Internet. For those users, a PET developed in the future should concentrate more on the users' concerns.

During the research for this thesis we got more and more aware of the great importance of P3P user agents for the P3P framework. As a result, we devote more attention to user agents than we had expected. As we have seen in the course of the thesis, although only

partially, an analysis of P3P user agents is very extensive, but at the same time instructive for both developers and users. It would have been interesting to determine, what user agents would look like and how they would be constructed considering the fact that it should be an easy-to-use tool for users imposing special requirements on information privacy in connection with PHS.

In a future work it may also be interesting to determine, what W3C did exactly to achieve market acceptance not only of end-users but also of service providers.

Bibliography

Ackerman (2004):

Mark S. Ackerman: Privacy in pervasive environments: next generation labeling protocols. In: Personal and Ubiquitous Computing, Volume 8, Issue 6, pp. 430 – 439

Agrawal et al. (2003):

Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu (2003): An XPath-based preference language for P3P. In: Proceeding of the 12th international conference on World Wide Web (WWW 2003), May 20 – May 22, Budapest, Hungary 2003, pp. 629-639

Beatty et al. (2007):

Patricia Beatty, Ian Peay, Scott Dick, James Miller: P3P Adoption on E-Commerce Web Sites. A Survey and Analysis. In: Internet Computing, Volume 11, Issue 2, 2007, pp. 65 - 71

Cliff (2012):

Barbara Cliff: Using Technology to Enhance Patient-Centered Care. In: Journal of Healthcare Management, Volume 57, Issue 5, 2012, pp. 301 – 303

Cranor (1998):

Lorrie F. Cranor (Editor): P3P Guiding Principles. W3C NOTE 21-July-1998. http://www.w3.org/TR/NOTE-P3P10-principles, Last Accessed 31.08.2014

Cranor (2002a):

Lorrie F. Cranor: The Role of Privacy Advocates and Data Protection Authorities in the Design and Deployment of the Platform for Privacy Preferences. In: Proceeding of the Twelfth Conference on Computers, Freedom and Privacy (CFP 2002), April 16 - 19, San Francisco, USA 2002, pp. 1 – 8

Cranor (2002b):

Lorrie F. Cranor: P3P and Privacy on the Web FAQ. http://www.w3.org/P3P/p3pfaq#OPS, Last Accessed 08.09.2014

Cranor (2003):

Lorrie F. Cranor: P3P. Making Privacy Policies More Useful. In: IEEE Security and Privacy, Volume 1, Issue 6, 11/2003, pp. 50 – 55

Cranor et al. (1999):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 2 November 1999. http://www.w3.org/TR/1999/WD-P3P-19991102, Last Accessed 28.08.2014

Cranor et al. (2000a):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 11 February 2000. http://www.w3.org/TR/2000/WD-P3P-20000211, Last Accessed 28.08.2014

Cranor et al. (2000b):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 04 April 2000. http://www.w3.org/TR/2000/WD-P3P-20000404, Last Accessed 28.08.2014

Cranor et al. (2000c):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 24 April 2000. http://www.w3.org/TR/2000/WD-P3P-20000424 , Last Accessed 28.08.2014

Cranor et al. (2000d):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 10 May 2000. http://www.w3.org/TR/2000/WD-P3P-20000510, Last Accessed 28.08.2014

Cranor et al. (2000e):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 15 September 2000. http://www.w3.org/TR/2000/WD-P3P-20000915/, Last Accessed 28.08.2014

Cranor et al. (2000f):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 18 October 2000. http://www.w3.org/TR/2000/WD-P3P-20001018, Last Accessed 28.08.2014

Cranor et al. (2000g):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Candidate Recommendation 15 December 2000. http://www.w3.org/TR/2000/CR-P3P-20001215, Last Accessed 28.08.2014

Cranor et al. (2001a):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 24 September 2001. http://www.w3.org/TR/2001/WD-P3P-20010924, Last Accessed 28.08.2014

Cranor et al. (2001b):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0)

Specification. W3C Working Draft 28 September 2001. http://www.w3.org/TR/2001/WD-P3P-20010928, Last Accessed 28.08.2014

Cranor et al. (2002a):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Proposed Recommendation 28 January 2002. http://www.w3.org/TR/2002/PR-P3P-20020128/, Last Accessed 29.08.2014

Cranor et al. (2002b):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Recommendation 16 April 2002. http://www.w3.org/TR/2002/REC-P3P-20020416/, Last Accessed 28.08.2014

Cranor et al. (2004a):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle, Matthias Schunter: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 10 February 2004. http://www.w3.org/TR/2004/WD-P3P11-20040210/, Last Accessed 28.08.2014

Cranor et al. (2004b):

Lorrie F. Cranor, Brooks Dobbs, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler- Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, Rigo Wenning: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 27 April 2004. http://www.w3.org/TR/2004/WD-P3P11-20040427, Last Accessed 28.08.2014

Cranor et al. (2004c):

Lorrie F. Cranor, Brooks Dobbs, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler- Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, Rigo Wenning: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 20 July 2004. http://www.w3.org/TR/2004/WD-P3P11-20040720, Last Accessed 28.08.2014

Cranor et al. (2005a):

Lorrie F. Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler- Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, Rigo Wenning: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 4 January 2005. http://www.w3.org/TR/2005/WD-P3P11-20050104/, Last Accessed 28.08.2014

Cranor et al. (2005b):

Lorrie F. Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler- Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, Rigo Wenning: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 1 July 2005. http://www.w3.org/TR/2005/WD-P3P11-20050701/, Last Accessed 28.08.2014

Cranor et al. (2006a):

Lorrie F. Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler- Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, Rigo Wenning: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 10 February 2006. http://www.w3.org/TR/2006/WD-P3P11-20060210/, Last Accessed 28.08.2014

Cranor et al. (2006b):

Lorrie F. Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler- Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, Rigo Wenning: The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Group Note 13 November 2006. http://www.w3.org/TR/2006/NOTE-P3P11-20061113/, Last Accessed 28.08.2014

Cranor et al. (2008):

Lorrie F. Cranor, Serge Egelman, Steve Sheng, Aleecia M. McDonald, Abdur Chowdhury: P3P Deployment on Websites. In: Electronic Commerce Research and Applications, Volume 7, Issue 3, 2008, pp. 274-326

Cranor, Arjula, Guduru (2002):

Lorrie F. Cranor, Manjula Arjula, Praveen Guduru: Use of a P3P User Agent by Early Adopters. In: Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES 2002), November 21, 2002, pp. 1 – 10

Cranor, Guduru, Arjula (2006):

Lorrie, F. Cranor, Praveen Guduru, Manjula Arjula: User Interfaces for Privacy Agents. In: ACM Transactions on Computer-Human Interactions, Volume 13, Issue 2, 6/2006, pp. 135 – 178

Cranor, Langheinrich, Marchiori (2002):

Lorrie F. Cranor, Marc Langheinrich, Massimo Marchiori: A P3P Preference Exchange Language 1.0 (APPEL1.0). W3C Working Draft 15 April 2002. http://www.w3.org/TR/P3P-preferences/, Last Accessed 02.09.2014

Cranor, Reagle (1998):

Lorrie F. Cranor, Joseph Reagle: Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project. http://www.w3.org/People/Reagle/papers/tprc97/tprc-f2m3.html, Last Accessed 12.09.2014

Cranor, Wenning (2007):

Lorrie F. Cranor, Rigo Wenning: W3C - Platform for Privacy (P3P) Project. Enabling smarter Privacy Tools for the Web. http://www.w3.org/P3P/, Last Accessed 13.08.2014

Cunningham (2001):

Ward Cunningham: Principles behind the Agile Manifesto. http://agilemanifesto.org/principles.html, Last Accessed 22.09.2014

Dehling, Sunyaev (2012):

Tobias Dehling, Ali Sunyaev: Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure. In: Proceedings of the 3rd USENIX conference on Health Security and Privacy (HealthSec 2012), August 6 – August 7, Bellevue, WA 2012, pp. 1 - 10

Dehling, Sunyaev (2014):

Tobias Dehling, Ali Sunyaev: Secure Provision of Patient-Centered Health Information Technology Services in Public Networks. Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. In: Electronic Markets, Volume 24, Issue 2, 2/2014, pp. 89 – 99

DSTI/ICCP/REG (2001):

Directorate for Science, Technology and Industry Commitee for Information, Computer and Communications Policy: Inventory of Privacy-enhancing Technologies (PETs), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final, Last Accessed 04.09.2014

Earp, Payton (2006):

Julia B. Earp, Fay C. Payton: Information Privacy in the Service Sector. An Exploratory Study of Health Care and Banking Professionals. In: Journal of Organizational Computing and Electronic Commerce. Volume 16, Issue 2, 2006, pp. 105 - 122

Federal Trade Commission (2000):

Federal Trade Commission: Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress. http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf, Last Accessed 17.09.2014

Florini (2007):

Ann Florini: Transparency for an Open World. Columbia University Press 2007

Gritzalis (2004):

Stefanos Gritzalis: Enahncing Web Privacy and Anonymity in the Digital Era. In: Information Management and Computer Security, Volume 12, Issue 3, pp. 255 - 288

Hensley et al. (1997):

Pat Hensley, Max Metral, Upendra Shardanand, Donna Converse, Mike Myers: Proposal for an Open Profiling Standard. http://www.w3.org/TR/NOTE-OPS-FrameWork, Last Accessed 08.09.2014

Hochheiser (2002):

Harry Hochheiser: The Platform for Privacy Preferences as a Social Protocol: An Examnination Within the U.S. Policy Context. In: ACM Transactions on Internet Technology, Volume 2, Issue 4, Novemer 2002, pp. 276 - 306

Holzner, Holzner (2006):

Burkart Holzner, Leslie Holzer: Transparency in Globar Change. The Vanguard of the Open Society. University of Pittsburgh Press 2006

Janic, Wijbenga, Veugen (2013):

Milena Janic, Jan P. Wijbenga, Thijs Veugen: Transparency enhancing tools (TETs): An Overview. In: Proceedings of the Third InternationalWorkshop on Socio-Technical Aspects in Security and Trust. (STAST 2013), Juni 29, Tulane University, New Orleans, LA, USA 2013, pp. 18 - 25

Jensen, Potts (2004):

Carlos Jensen, Colin Potts: Privacy Policies as Decision-Making Tools. An Evaluation of Online Privacy Notices. In: ACM: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2004), April 24–29, 2004, Vienna, Austria. New York, NY, USA 2004, pp. 471 – 478

Kolari et al. (2005):

Pranam Kolari, Li Ding, Shashidhara G, Anupam Joshi, Tim Finin: Enhancing web privacy protection through declarative policies. In: Proceedings of the sixth IEEE International Workshop on Policies for Distribution Systems and Networks (POLICY 2005), June 6 – June 8, Stockholm, Sweden 2005, pp. 1 – 10

LaLiberte (1999):

Daniel LaLiberte: Removing Data Transfer from P3P. http://www.w3.org/P3P/data-transfer.html, Last Accessed 29.08.2014

Laudon, Laudon, Schoder (2010):

Kenneth Laudon, Jane Laudon, Detlef Schoder: Wirtschaftsinformatik. Eine Einführung. 2. Edition, München, Germany 2010

Lee, Speyer (1998):

Kenneth Lee, Gabriel Speyer: White Paper: Platform for Privacy Preferences Project (P3P) & Citibank. http://www.w3.org/P3P/Lee_Speyer.html, Last Accessed 09.09.2014

Marchiori, Jaye (1998a):

Massimo Marchiori, Dan Jaye (Editors): Platform for Privacy Preferences (P3P) Syntax Specification. W3C Working Draft 19-May-1998. http://www.w3.org/TR/1998/WD-P3P10-syntax-19980519.html, Last Accessed 28.08.2014

Marchiori, Jaye (1998b):

Massimo Marchiori, Dan Jaye (Editors): Platform for Privacy Preferences (P3P) Syntax Specification. W3C Working Draft 2-July-1998. http://www.w3.org/TR/1998/WD-P3P10-syntax-19980702, Last Accessed 28.08.2014

Marchiori, Reagle, Jaye (1998):

Massimo Marchiori, Joseph Reagle, Dan Jaye (Editors): Platform for Privacy Preferences (P3P1.0) Specification. W3C Working Draft 9-November-1998. http://www.w3.org/TR/1998/WD-P3P-19981109/, Last Accessed 28.08.2014

Marchiori, Reagle (1999a):

Massimo Marchiori, Joseph Reagle (Editors): Platform for Privacy Preferences (P3P) Specification. W3C Working Draft 7 April 1999. http://www.w3.org/TR/1999/WD-P3P-19990407/, Last Accessed 28.08.2014

Marchiori, Reagle (1999b):

Massimo Marchiori, Joseph Reagle (Editors): Platform for Privacy Preferences (P3P) Specification. W3C Working Draft 26 August 1999. http://www.w3.org/TR/1999/WD-P3P-19990826, Last Accessed 28.08.2014

McDonald, Cranor (2008):

Aleecia McDonald, Lorri F. Cranor: The Cost of Reading Privacy Policies. In: A Journal of Law and Policy for the Information Society, Volume 4, Issue 3, 2008, pp. 543 – 564

Microsoft (2014):

Microsoft: Privacy in Internet Explorer. http://msdn.microsoft.com/en-us/library/ie/ms537343%28v=vs.85%29.aspx, Last Accessed 29.08.2014

MIT et al. (2014):

MIT, ERCIM, Keio, Beihang: About W3C. http://www.w3.org/Consortium/, Last Accessed 21.08.2014

Organization for Economic Co-operation and Development (2013):

Organization for Economic Co-operation and Development: The OECD Privacy Framework. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, Last Accessed 04.09.2014

Pavlou (2011):

Paul A. Pavlou: State of the Information Privacy Literature: Where Are We Now And Where Should We Go? In: MIS Qaurterly, Volume 35, Issue 4, 2011, pp. 977 – 988

PrivacyBird (no date):

PrivacyBird: Find web sites that respect your privacy. http://www.privacybird.org/, Last Accessed 29.08.2014

Presler-Marshall (2002):

Martin Presler-Marshall: The Platform for Privacy Preferences 1.0 Deployment Guide. W3C Note 11 February 2002. http://www.w3.org/TR/2002/NOTE-p3pdeployment-2002021, Last Accessed 30.08.2014

Reagle (1998):

Joseph Reagle (Editor): P3P Harmonized Vocabulary Specification. W3C Working Draft 30-March-1998. http://www.w3.org/TR/1998/WD-P3P10-harmonization-19980330, Last Accessed 28.08.2014

Reagle, Cranor (1999):

Joseph Reagle, Lorrie F. Cranor: The Platform for Privacy Preferences. In: Communications of the ACM, Volume 42, Issue 2, 2/1999, pp. 48–55

Reay, Dick, Miller (2009):

Ian Reay, Scott Dick, James Miller: An Ananlysis of Privacy Signals on the World Wide Web: Past, Present and Future. In: Information Sciences, Volume 179, Issue 8, 2009, pp. 1102 – 1115

Reagle, Wenning (2000):

Joseph Reagle, Rigo Wenning: P3P and Privacy on the Web FAQ. http://www.w3.org/P3P/P3FAQ.html, Last Accessed 08.09.2014

Schnorf, Ortlieb, Sharma (2014):

Sebastian Schnorf, Martin Ortlieb, Nikhil Sharma: Turst, Transparency & Control in Inferred User Interest Models. In: ACM: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2014), April 26 – May 1, 2014, Toronto, Ontario. Canada, C 2014, pp. 2449 - 2454

Schwartz (2009):

Ari Schwartz: Looking back at P3P: Lessons for the Future. In: Center for Democracy and Technology, 11/2009, pp. 1 – 9

Stelzer (2009):

Dirk Stelzer: Enterprise Architecture Principles: Literature Review and Research Directions. In: Proceedings of the Seventh International Conference on Service-Oriented Computing (ICSOC 2009), November 23rd, 2009, Stockholm, Sweden 2009, pp. 12 - 21

Tatli (2007):

Emin I. Tatli: Extending P3P/Appel for Friend Finder. In: Proceeding oft he Internation Conference on the Moblie Data Management, (MDM 2007), May 01, Mannheim 2007, pp. 243 - 247

Wenning (2007):

Rigo Wenning: Platform for Privacy Preferences (P3P) Project

P3P 1.0 Implementations. http://www.w3.org/P3P/implementations.html, Last Accessed 01.09.2014

Widjaja, Gregory (2012):

Thomas Widjaja, Robert Wayne Gregory: Design Principles for Heterogeneity Decisions in Enterprise Architecture Management. In: Proceeding of the thirty third International Conference on Information Systems (ICIS 2012), December 16 – 19, Orlando, Florida, USA 2012, pp. 1 - 11

Winter, Aier (2011):

Robert Winter, Stephan Aier: How are Enterprise Architecture Design Principles Used? In: Proceeding of the Fifteenth IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW 2011), August 29 - September 02, 2011, Helsinki, Finland, pp. 314 – 321

WHO (2014):

World Health Organization: E-Health. http://www.who.int/trade/glossary/story021/en/, Last Accessed 06.09.2014

World Wide Web Consortium (1997):

World Wide Web Consortium: FTC Comment: Script of W3C P3 Prototype. http://www.w3.org/Talks/970612-ftc/ftc-sub.html, Last Accessed 29.08.2014

Xu, Teo, Tan (2006):

Heng Xu, Hock-Hai Teo, Bernard Tan: Information Privacy in the Digital Era. An Exploratory Research Framework. In: Proceedings of the Twelfth Americas Conference on Information Systems (AMCIS 2006), August 04 – August 06, 2006, Acapulco, Mexico, pp. 899 - 906

Yi Hong, Patrick, Gillis (2008):

Yi Hong, Timothy B. Patrick, Rick Gillis: Protection of Patient's Privacy and Data Security in E-Health Services. In: Proceeding in the International Conference on BioMedical Engeneering and Informatics (BMEI 2008), May 27 – May 30, 2008, Sanya, pp. 643 - 647