

Towards Assured Informed Consent in Privacy Notice Design

An Eye Movement Detection Approach

Makame Makame
2016

Master (120 credits)
Master of Science in Information Security

Luleå University of Technology
Department of Computer science, Electrical and Space engineering

DEDICATION

*This thesis is dedicated to my beloved wife **Muzdalifa Mkubwa Ali** and dearest son **Mahmud Makame Hamza**. I owe you two years of hugs, kisses and my totally undivided attention.*

ABSTRACT

To be able to provide data collecting services to customers, service providers are required by law to design privacy policies and present their content to users as privacy notices that inform the user on privacy consequences and demonstrate that an explicit informed consent of the user has been collected before processing of the data. However, despite the increase in data collection by services and hence increase of privacy impact, yet privacy notices do not implement proper mechanisms that can assure that data subjects are well informed and their consent are provided with comprehension. The root of this problem is the fact that typically only theoretical description of what consent is and what it involves is offered by existing literature but no “practical” design guides are available for decision makers and practitioners on how to effectively integrate a targeted consent level in privacy notices. This thesis work addresses the need for explicit integration of consent in privacy notice designs by presenting the Extended Privacy Notice Design Space (XPNDS) construct that guides on explicitly incorporating different levels of consent in privacy notices. This thesis uses theories of eye movement in reading and technical references from computer vision for comprehension and attention determination to prove the feasibility of integrating higher level of consent in the design space that may guide to assured informed consent. The construct can be used by managers to communicate, practitioners to design, and regulators to analyze informed consent incorporation in privacy notice designs. Unlike most works available in the literature on consent which only provide theoretical opinion of what informed consent is, this work casts the conceptual consent guidelines into a practical privacy notice design space to provide an XPNDS that guides to the practicality of achieving assured informed consent in privacy notices. It is the hope of the author that the XPNDS will be useful to both practitioners and academicians in incorporating informed consent in privacy notice designs to an assured level.

Key Words: Privacy Notice, Informed Consent, Privacy Notice Design Space, Design Science Research.

ACKNOWLEDGEMENT

First and foremost, all praises are to my creator and sustainer who gave me good health, energy, happiness, and all the necessities required to complete the thesis.

I would also like to express my deepest gratitude and appreciation my supervisor Dr. Ali Ismail Awad for his commitment and efforts in conveying his professional research skills throughout the research supervision period.

Likewise, I would also like to thank all the staffs/instructors in the Information Security program for the best knowledge that they were willing to share with us. Special thanks to Professor Tero Päivärinta for broadening my research capabilities specially on Design Science Research methodology.

Moreover, I am very grateful my brotherly friend Ebenezer Okoh for all the free, best, wise, and helpful advices and guidance from the day we met. I have learnt a lot from you.

Similarly, I would like to thank my classmate Fortune Munodawafa for his honest support, valuable discussion, and having my back during the whole study period.

I would also like to acknowledge the experts that gave their review on the output of this research work.

Furthermore, I would like to acknowledge the Swedish Government for funding my entire master program study at Luleå University of Technology through Swedish Institute Scholarship. I am very grateful.

Lastly and most importantly, I would like to thank my dear parents for raising me well to reach this point, my family members for their support and belief in me, and my beloved wife and son for their patient and support during the whole period of my study. I love you all.

TABLE OF CONTENTS

ABSTRACT.....	ii
ACKNOWLEDGEMENT	iii
LIST OF FIGURES	vii
LIST OF TABLES	viii
ABBREVIATIONS	ix
CHAPTER ONE.....	1
INTRODUCTION	1
1.1 Overview	1
1.2 Problem Statement.....	2
1.3 Motivation	2
1.4 Research Objectives	3
1.5 Methodology and Contribution	3
1.6 Delimitation	4
1.7 Thesis Organization.....	4
CHAPTER TWO	5
LITERATURE REVIEW	5
2.1 Literature Review Methodology.....	5
2.2 A Design Space for Privacy Notice Design.....	5
2.3 Consent in Prior Privacy Notice Artifacts	7
2.4 Identified Research Gap	10
2.5 Problem Relevance	11
CHAPTER THREE	12
METHODLOGY	12

3.1	Design Science Research Methodology	12
3.2	DSR Methodological Procedures	13
CHAPTER FOUR	18
DESIGN REQUIREMENTS VALIDATION	18
4.1	Overview	18
4.2	Eye Movement in Reading and Cognition	18
4.3	Requirements Feasibility Proof Using Eye Movements Analysis.....	20
4.4	Practical Suitability of Eye Movements Detection Approach.....	25
CHAPTER FIVE	26
THE EXTENDED PRIVACY NOTICE DESIGN SPACE	26
5.1	Design Process.....	26
5.2	Development Process Consideration	27
5.3	The Extended Privacy Notice Design Space Construct.....	29
CHAPTER SIX	35
EVALUATION	35
6.1	Overview	35
6.2	Case Study Evaluation (ericsson.com).....	35
6.3	Use Cases Evaluation	38
6.4	Experts Evaluation.....	41
6.5	Evaluation of Research.....	42
CHAPTER SEVEN	45
DISCUSSION	45
7.1	Overview	45
7.2	Design Output Interpretation.....	45

7.3	Objective Fulfillment.....	45
7.4	Contribution to Practice.....	46
7.5	Implication to Knowledge	46
7.6	Limitation of the Research	46
7.7	Lesson Learned.....	47
7.8	Future Works	47
CHAPTER EIGHT		49
CONCLUSION.....		49
REFERENCES		50

LIST OF FIGURES

Figure 1. Privacy Policy Notice Design Space [12].	6
Figure 2. Design Science Research methodological procedures [34].....	12
Figure 3. Pseudocode representation of CURD algorithm.	14
Figure 4. Design search's knowledge bases iterations for privacy notice design space development.	15
Figure 5. Evaluation activities within a DSR process [35].....	16
Figure 6. A sample illustration of acceptable gazing patterns for a notice with 0.5 Appreciation factor.	22
Figure 7. Eye movement during reading [46].....	24
Figure 8 Contributions of different research steps/actions/iterations to the design and development of the XPNDS.	28
Figure 9. The Extended Privacy Notice Design Space.	29
Figure 10. First Layer cookies privacy notice for ericsson.com.....	36
Figure 11. Layer I notice design interpretation on XPNDS.....	36
Figure 12. Layer II notice design interpretation on XPNDS.	37
Figure 13. Cookies content setting in Google Chrome.....	37
Figure 14. Layer III notice design interpretation on XPNDS.	38
Figure 15. LinkedIn profile privacy notice.	39
Figure 16. XPNDS analysis of LinkedIn profile privacy notice.....	39
Figure 17. XPNDS analysis of Windows 10 mobile location access notice.	39
Figure 18. Windows 10 mobile location access interactive notice.	40
Figure 19. Just in time location access notification in Windows 10 mobile.....	40
Figure 20. XPNDS analysis of Windows 10 mobile just-in-time location access notice.....	41

LIST OF TABLES

Table 1. Categorization of the existing privacy notice artifacts using the Privacy Notice Design Space.....	8
Table 2. Comparison of existing proposed consent improvement models by their relevance and shortcomings in integrating consent in privacy notices.....	10
Table 3. The range of mean fixation durations and the mean saccade length in silent reading, oral reading, scene perception, and visual search [38].....	19
Table 4. The effects of targeted cognition level on the experiment behavior.....	20

ABBREVIATIONS

API	Application Program Interface
APPEL	A P3P Preference Exchange Language
CCTV	Closed-circuit Television
CURD	Cite-Up-Reference-Down
DSR	Design Science Research
EC	European Council
FD	Fixation Duration
IEEE	Institute of Electrical and Electronics Engineers
IPV	Integrated Privacy View
JITCTA	Just-In-Time Click Through Agreement
MRA	Most Relevant Article
P3P	Platform for Privacy Preferences Project
PET	Privacy Enhanced Technologies
SL	Saccade Length
W3C	World Wide Web Consortium
XPNDS	Extended Privacy Notice Design Space

CHAPTER ONE

INTRODUCTION

1.1 Overview

Privacy notice presents a portion of privacy policy to the data subject to notify on the occurrence and/or consequence of a data collection activity. Privacy policies are established principle in legal domains to codify data collection and usage practices [18]. They are used to describe organizations data practices on data collection, use, and disclosure [57]. They are much popular among online service vendors for communicating privacy attitude among their users. Privacy policies are considered to build a notion of fair warning and informed consent [58].

Application of privacy notice is visible in different domains such as public areas, health services, financial services, and most of services that have privacy policies (written or otherwise). With the growth of the internet, the adaptation of online services has also increased [59] and different technological ideas have been transformed into services such as online: education, commerce, communication, health, and other utility based services. For a long time, privacy notices have been used to communicate the privacy policies to the subject, in major parts of the world the presence of such notices is required by law [1].

Government and international organizations requires the privacy notice to provide the data subject with certain level of consent, and for critical environments, informed consent is required [2]. Moreover, for environment where there is a close tie between the notice provider and the subject, assured informed consent may be required.

Therefore, privacy notices are required for privacy policy presentation and subject's consent determination. Notices from different services may require different levels of consent and some environments may require assured levels of consents beyond what is suggested by regulatory bodies.

Privacy notices plays an important role in conveying privacy policies and ensuring that the consent of the subject is collected, the subject are well informed of the policy, and the subject comprehends

the notice contents. However, the significance of the privacy notice depends heavily on its design and design principles followed [12]. Although the rules exist, without explicit design guides, most of the notice designed for use do not meet the requirements established by the law and others are struggling in need for higher level of informed consent determination assurance to be able to provide their privacy intensive services.

1.2 Problem Statement

To be able to provide data collecting services to customers, service providers are also required by law [1] to design privacy policies and to present their content to users as privacy notices which should inform a user on the privacy consequences and demonstrate that an explicit informed consent of the user has been collected before processing of the data. Enormous efforts are imposed by regulatory bodies such as the European Council (EC) requiring that data subjects' consent to processing of their personal data must be freely given, specific, informed, and unambiguously revealed through either statement or a clear agreeing action to signify agreement, and a consent must be explicit for sensitive data [2]. However, despite the increase in data collection by services and hence increase of privacy impact, yet privacy notices do not implement proper mechanisms that can assure that data subjects are well informed and their consent are provided with comprehension [3]. The root of this problem is the fact that typically only theoretical description [4] of what consent is and what it involves is offered by existing literature but no "practical" design space guides are available for decision makers and practitioners on how to effectively integrate a desired consent level in privacy notices.

1.3 Motivation

The motivation for this research comes from the need to find solutions for the problem of inappropriate claim of integration of informed consent in notice designs by service vendors and the use of old consent determination techniques while new technologies are available that can redefine informed consent determination in notices. It is the researcher's belief that achievement of proper ways to determine data subject's assured informed consent will help providing enough trust and stimulate the rise of provision of sensitive services remotely through the internet.

For example, patient's informed consent is critical in e-therapy where physician provides treatment over the internet [7]. Accomplishing assurance of informed consent determination will unlock more e-health services that can be provided remotely through the internet via special consumer devices. In essence, even mobile phone devices are now able to be used for symptom assessment, remote treatment monitoring, and treatment progress tracking [8],[9] and hence much can be provided to satisfy remote diagnostics.

1.4 Research Objectives

Informed consent involves disclosing to data subject on potential privacy sensitive action of a service in a way that it can be comprehended and an agreement or declination decision can be made [5]. Friedman et al. [6] proposed a conceptual model of online informed consent that demands fulfillment of agreement, comprehension, disclosure, competence, and voluntariness. However, still there are claims [3],[60] on the current notion of consent and its effectiveness on managing with the changing information technologies. This research work has the following goals: (1) It aims at addressing the need for privacy notice design space construct that explicitly guides on consent integration in privacy notice design to an assured informed level. (2) It aims at developing design construct that provide practical design guide on achieving different level of consent in privacy notices.

1.5 Methodology and Contribution

To achieve the aforementioned goals of the research, a design science research (DSR) methodology was used to design a new construct for guiding privacy notice design referred as Extended Privacy Notice Design Space (XPNDS). The term "extended" exists because the design space was built on top of an existing construct which was refactored and extended to explicitly integrate consent. This fulfill the DSR requirement for improvement and extension of contents of the knowledge base for further research and practice [10]. To integrate higher level of consent in the design space that may guide to assured informed consent, theories of Eye movement in reading and computer vision technicalities were used to prove the possibility of determining comprehension requirement for informed consent. Besides methodological contribution, the benefit of XPNDS also includes (1) practitioners are provided with explicit practical design guide for integrating consent in privacy notices, (2) managers are able to use the construct guide in

determining the level of consent to be used in the design based on policy or privacy impact, and (3) it provide standard design communication platform between managers and practitioners.

1.6 Delimitation

Although privacy notice covers different application domains, the scope of this design work is based on privacy notice designs for software services (online or offline). However, the resultant artifacts proved to accommodate design application beyond the targeted domain.

1.7 Thesis Organization

The organization of the thesis follows the publication scheme for design science research study as in [11] and therefore, the rest of the chapters are organized in the following themes. Chapter Two analyses literatures on prior design knowledge and artifacts deducing limitations that helps in designing requirements. Chapter Three describes the methodologies used with reference to their respective authorities. Then, XPNDS description covers Chapter Four and Chapter Five in which the former test the validity of requirements and their applicability in real world through design search, and the later provide description of the final construct design. Chapter Six provide evaluation of the XPNDS followed by discussion in Chapter Seven and lastly Chapter Eight concludes the thesis.

CHAPTER TWO

LITERATURE REVIEW

2.1 Literature Review Methodology

Having the problem and objectives clearly identified in Chapter One, in this chapter, the requirements for fulfilling the objectives of the proposed solution are defined. The requirement formulation process begins by conducting an extensive literature review on state of the art privacy policy presentation design artifacts on their implementation of informed consent and reflect these artifacts to the only current privacy notice design theory which has been chosen because of its recentness and dynamism of its authors that includes both researchers and practitioners from leading industry (Google, RAND). The primary and only utilized search engine for the purpose of this research is Google Scholar (chosen for its ability to perform search from within many journals sources and other academic search portals such as Science Direct and IEEE). To maximize the cover of related works, a Cite-Up-Reference-Down (CURD) literature search technique was used in addition to key word search. The technique is explained in details in the methodology section (Chapter Three). The artifacts are classified and their shortcoming are analyzed, and reflected to the privacy notice design space to reveal the general weakness in informed consent implementation and propose the requirements that the new solution should consider.

Prior approaches to improve the problem of consent in privacy policies design for better user reading and comprehension (i.e. providing informed consent) were first categorized based on the efforts used to improve consent. To ground the classification to existing academic (Descriptive knowledge [11]) and practical (Prescriptive Knowledge [11]) knowledge base, the articles are dialyzed using the privacy notice design space proposed by Schaub et al. [12] in 2015.

2.2 A Design Space for Privacy Notice Design

In their design construct, Schaub, Balebako, Durity, and Cranor proposed and evaluated a privacy notice design space that provides a taxonomy and vocabularies that helps system designers and privacy engineers in considering different dimensions of privacy notice. The construct provides four privacy notice design dimensions which are notice's Timing (when it is presented), Channel

(how it is presented), Modality (communication model used), and Control (how are the choices provided) [12] as illustrated by Figure 1 below.

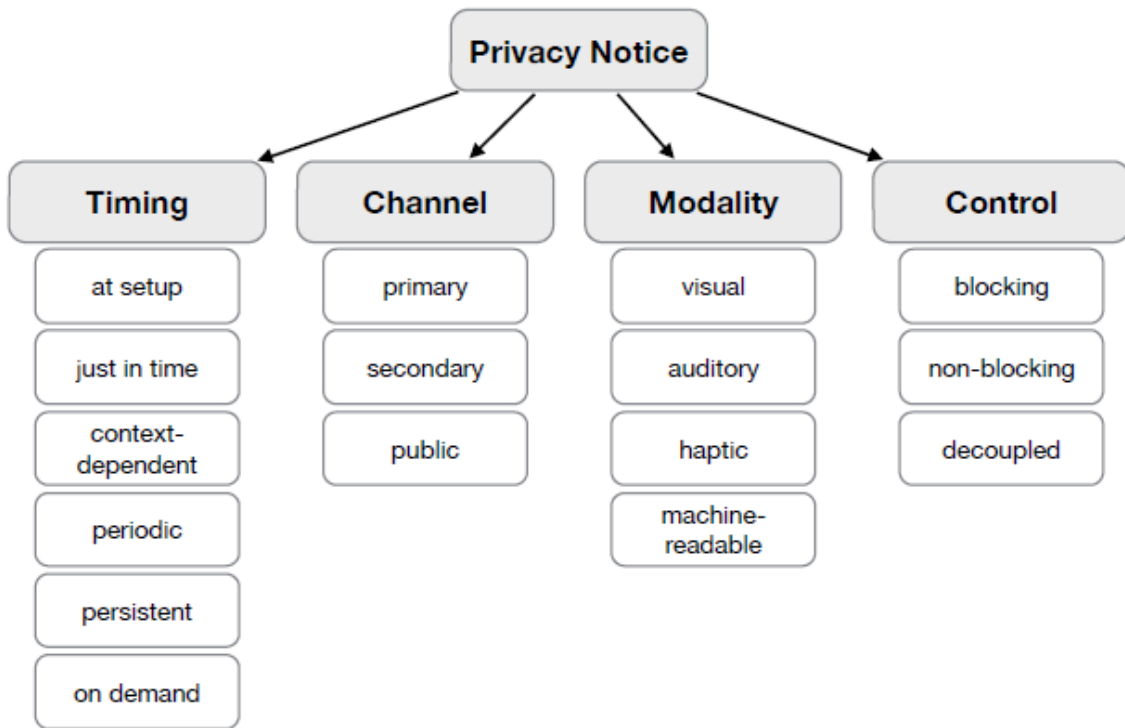


Figure 1. Privacy Policy Notice Design Space [12].

Timing of the privacy notice has been found to have a significant influence in the way the notice is perceived by the user [13, 14, 15]. A privacy notice can be presented once during software setup, or just in time of privacy sensitive event, or on change of context like location or network. Also the notice can be a periodic reminder for the user, persistently displayed throughout out the use of the service, or can be accessed separately on demand.

Channel states how the privacy notice is presented to the user. A primary channel is the one in which the privacy notice is presented on the same platform as the one the service itself is provided with. For example, if a service is provided through a web interface, then the policy notice will be integrated as part of the web interface. A secondary channel use other platform different from the main like email and public channel utilize publicly available platforms like billboards and posters.

Modality specify the way in which the privacy notice is communicated to the user. These include visual, auditory, haptic(vibration), and machine-readable. For online services, the most common

are visual presentation of the policies as texts and graphics [16] and the machine-readable format using privacy policies presentation languages like P3P [17], APPEL [18], and PrimeLife Policy Language [19] which are commonly used in implementations of Privacy Enhanced Technologies (PET).

Control provides the user with decisions on possible control of their data. Options to opt-in and opt-out of data activity may be available to the user. The user may need to pause and make choices and therefore provide consent. Controls may wait for user action (blocking) or not (no-blocking), or can be placed separate from the main notice (decoupled). Here some level of consent consideration can be deduced but not explicitly addressed.

There are however, other conceptual design proposals such as that by Friedman et al. [6] which also proposed design principles for informed consent online and also the one by Bonnici [61] who improved the Friedman et al.'s initial online informed consent definition. However, these designs do not provide practical guide on how to achieve the quality of their proposals.

2.3 Consent in Prior Privacy Notice Artifacts

From the above privacy notice design space, it can be observed that informed consent is not given enough attention on the design, it can be achieved with in the output of the design process but no explicit guides have been set forth to govern. With the findings form the design constructs, the study shifted to the how the privacy notice artifacts design does to achieve informed consent. The efforts to make users read and understand online services privacy policies had been categorized in five categories. The categorization is based on prioritized order of design dimensions. The order of prioritization starts with Timing (high priority), Modality, Control, and Channel having the least priority. It should be noted that the focus for this case was on online software services privacy notice artifacts, and changing of the order of priorities may result to different categories. Nevertheless, this research found the aforementioned prioritization scheme as the best fit for classifying software services privacy policy presentation for improving of user's consent and understanding.

Table 1 bellow summarizes the five categories of existing of privacy notice designs in the context of software services. It has been observed that while the common privacy notice Channel used in

software services remains to be primary (integrated with in the service itself), Timing and Control dimensions of the notice design have been the tuning-knob in searching for effective privacy policy presentation that are meant to be easy for customer to read and understand. Moreover, the visual (Modality) is the basic way of presenting the policies in online services as even machine-readable (Modality) is usually encapsulated with visual representation for the user to comprehend and interact where necessary.

Table 1. Categorization of the existing privacy notice artifacts using the Privacy Notice Design Space.

Category	Timing	Modality	Channel	Control	Source
I	at setup	visual	primary	non-blocking	[21,23,25]
II	on demand	visual	primary	decoupled	[26,27]
III	periodic	visual	primary	blocking	[29]
IV	just in time	visual	primary	blocking	[30]
V	persistent	machine-read	primary	non-blocking	[31]

Category I comprises of privacy policy presentation artifact models that are presented during the setup/installation/registration of a service. As the normal policy documents are argued by several researches to be very long and difficult to understand [20], these models focused on refining the visual design of the policies to improve data subject’s understanding and readability of polices. In the effort, Layered privacy policies notice [21] that provides a brief summary of the policies in well standardized headings were proposed. Yet studies on the effectiveness of the text based privacy presentation formats [22] found that these formats were not good to the tested participants. A proposal by Passera [23] suggest going beyond the wall of text by incorporating layout and visual design to achieve visibility and understanding of the policies. Text and images were combine to increase the understanding as hypothesized by the Cognitive Load Theory [24]. The approach provides some positive results but still challenged by lengthy policy documents. In tackling end user license agreement presentation, Key and Michael [25] employed Factoids, Vignettes, and Icons to a license summary that is presented at the end of the installation process. Their findings showed that the design has managed to increase user concern on the license terms of the software.

Category II involve those privacy policies presentation models that are presented on demand (*Timing*) throughout the use of the service. They can be accessed at any point in time of the use of the Online Service through a link or otherwise. The visual (*Modality*) presentation is improved by summarizing the policy using tables and icons to reduce the length of the policies and increase cognition respectively. The policy summary is decoupled (*Control*) from the main policy document as they provide an overview and cannot be a total replacement [26]. Inspired by the Nutrition Labels from the food industries, Kelly et al. [26] designed the Simplified Grid for privacy policies in a form of two dimensional table with nutrition labels like styles of icons representing different state of data policies. The tables are automatically generated using the P3P policy language. Privacy Policy Icons [27] have been also proposed in finding the cure for this problem of privacy policies understanding by the users. The problems with the privacy icons is that there are several implementations and it is difficult to have a set that is accepted by all. In addition to that icons interpretation may require a learning process especially for large and growing domain like privacy and therefore cannot guarantee the comprehension required for consent determination.

Category III encompass those privacy policy models that are presented periodically (*Timing*) in order to remind the customers and increase the odd of their understanding of the policies by frequently facing the same notification with the hope that if the user ignored the notice in one occasion, another occasion may find the user in a better mood to read the notice and consent. Factors such as time, action, or context can be used to set the notification frequency. However, users have the tendency to habituate [28] with frequent notifications by developing abilities to respond to them without even giving their full attention. Noticing this, Brustoloni and Ricardo [29] developed Polymorphic dialogs aiming in attracting enough user attention on their notice by having dynamic properties such as of color, positions of contents and buttons, and even disabled (*Control*) buttons with count down timer to give a user time to read the notification message and hence improve the chance of achieving informed consent, yet it is not assured.

Category IV covers the privacy policy presentation designs that presents a notification just in time (*Timing*) of an action associated with the policy section. The user may be blocked (*Control*) and required to make decisions in order to proceed with the service. The aim is to present the privacy notice to the data subject at time which is in the context of data processing action so that the validity of the consent is boosted. Patrick and Kenny [30] proposes the “Just-In-Time Click Through

Agreement” (JITCTA) which provides smaller agreements dialogs when a user performs an action that collects personal information.

Category V focus on the privacy presentation artifacts that aims to provide persistent (*Timing*) notification to an online service user. These model typically uses machine-readable (*Modality*) as they provide constant and persistent monitoring of the privacy settings match with the user’s predefined privacy preferences. The user is presented with visual (*Modality*) indication of the policy matching status. For instance, Levy and Gutwin [31] decided the notification should be taken to a more granular level and proposed the Integrated Privacy View (IPV) that used P3P policy language to map policy conflicts with their corresponding input fields on the web page form. As with other PET, the problem of prerequisite user knowledge on privacy preferences settings is a draw back with this model. Also the model only shows the conflict and not conveying the actual policy information. Hence, the consent provided by this design is not necessarily informed as the user can be warned without understanding the notice content. Table 2 illustrates the Comparison of existing proposed consent improvement models by their relevance and shortcomings in integrating consent in privacy notices. From the table it can be observed that still guide on consent and explicit integration is lacking as does assured informed consent.

Table 2. Comparison of existing proposed consent improvement models by their relevance and shortcomings in integrating consent in privacy notices.

Consent Proposals Modes	Relevance	Shortcomings
Conceptual Model	Tells what informed consent is	Does not guide on achieving practicality
Practical Guides	Guides on practical privacy notice design	Addresses consent implicitly
Artifacts	Reveal techniques used to achieve consent	Only lower levels of consents are addressed

2.4 Identified Research Gap

All the five categories use Timing and Modality dimensions to convey the policies and improve readability and comprehensibility of the policies. However, all these efforts do not guarantee that the user read and understand the policies and hence informed consent cannot be assured. In cases where the services are very critical and the user must be proved to read and/or comprehend the

policies. The model and the existing implementations do not provide a reliable means (dimension) to do so as illustrated in Table 2. Therefore, in addition to explicitly integrating consent in the design space, to achieve this extent of informed consent the privacy notice design space needs to be revised and extended to fulfil the following requirements.

- a) Assured processing of the information presented by the privacy notice to the user.
- b) Determine user's cognition/comprehension of information presented by the privacy notice.

2.5 Problem Relevance

None of the previous models which has been found by this study have met all the objectives and requirements listed above. They focus extensively on the notification part without involving the impact assurance of the design on the subject that is being notified. For instance, it is not theoretically correct to determine the consent of a reading activity by a click of a button or dragging around notification contents. In fact, a button may be clicked without even reading or comprehending the displayed information. But due to the limitation of the design space, even the designed artifact could not escape the same fate. The remainder of this thesis work dives in cognitive science domain in the search for realistic informed consent assurance design space artifact.

CHAPTER THREE

METHODOLOGY

3.1 Design Science Research Methodology

As opposed to customary scientific research methodologies that are used to explore and confirming hypothesis [32] this thesis work adopts a Design Science Research (DSR) [33] approach as its adequately align with its goal of designing an artifact as the primary output of the project. The thesis follows a DSR procedural model suggested by Peffers et al. [34] using a problem centered approach as its research entry point. The approach is super imposed with the design science research artifact evaluation guidelines by Sonnenberg and Brocke [35] that are used as feedback sources for the iteration between the build and evaluate processes. Figure 2 illustrate the six steps of Design Science Research employed for this research work and the rest of this chapter explain in detail how each stage was conducted in this thesis and grounded to befitting authorities to achieve the desired research rigor.

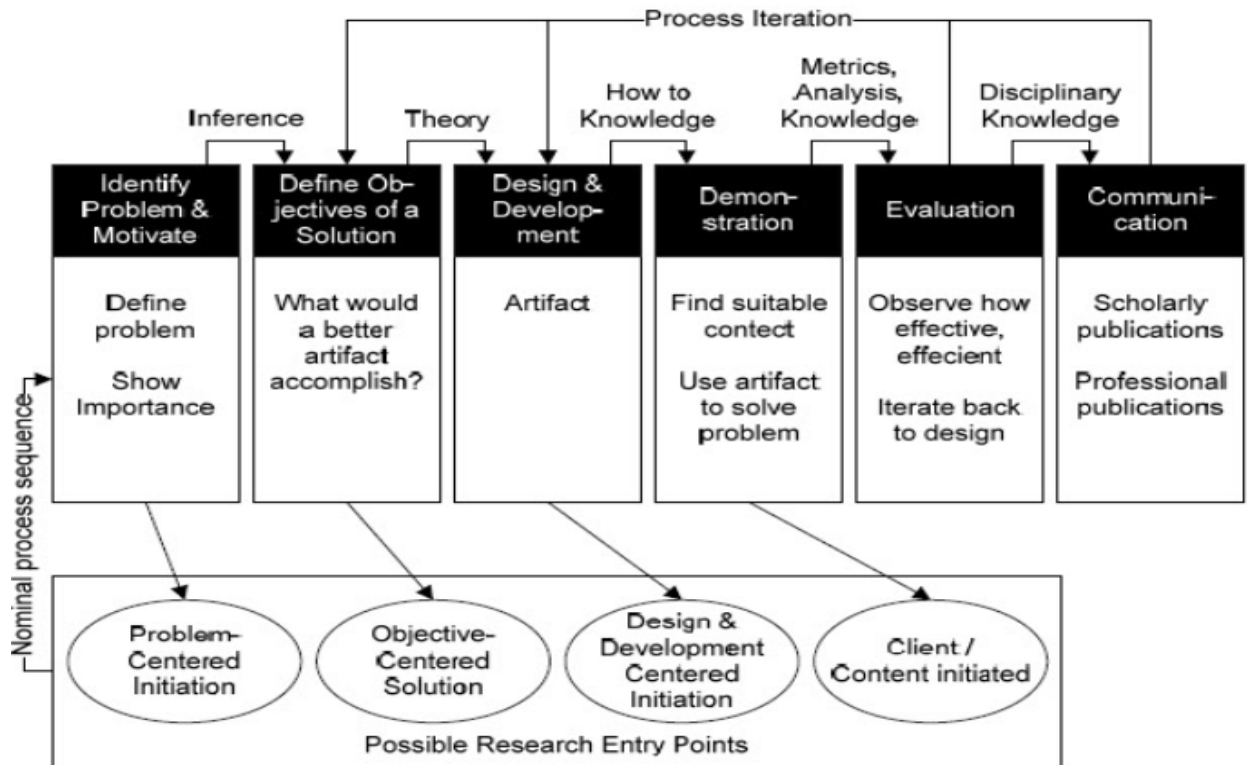


Figure 2. Design Science Research methodological procedures [34].

3.2 DSR Methodological Procedures

3.2.1 Problem Identification

Identification of problems has been achieved through literature search and brainstorming, and has been used as the entry point to the research. Several review stages have been conducted to arrive to the final problem definition. At first, the Privacy Policy domain was found of interest and furthers literature search was conducted. Second the problem of users not reading and understand privacy policies was found to be claimed by many. Finally, it has been found that even with the effort to present the privacy policies in an understandable way, there is still weakness in means for determining and approving user's consent in privacy notices.

3.2.2 Objectives of the Solution

Objective of the solution were achieved through an extensive review of literatures covering both design theories and instantiations as suggested by Gregor and Hevner [11]. The review focused on analyzing the design space and the existing artifacts in parallel to deduce the antagonistic drawbacks that exists between the artifacts and design theories. The literature review was conducted by performing key words search on Google Scholar. To maximize the cover of related works, a Cite-Up-Reference-Down (CURD) search technique was used in addition to key word search.

The Cite-Up-Reference-Down (CURD) work in recursive fashion succeeding the following steps of execution.

1. Using key word search, the Most Relevant Articles (MRA) are identified and listed.
2. For each MRA,
 - a. A Cite-Up operation is performed which checks for other MRA in the list of articles that cited this given MRA (best for old articles).
 - b. A Reference-Down operation is performed which checks for other MRA in the list of references of the current MRA (best for recent articles).
3. New MRAs found are added to the new MRA list.
4. The process is repeated for the new list of MRA until the researcher is satisfied.

```

1 void curd(List<MRA> MRAList){ //1
2
3     foreach (var MRA in MRAList) //2
4     {
5         //Look for MRA in the cyted by list
6         NewMRAList = LookInCitedBy(MRA); //a
7
8         //Look for MRA in the reference list
9         NewMRAList = LookInReferences(MRA); //b
10
11     }
12
13     if(NewMRAList.Count > 0){ //3
14         curd(NewMRAList); //4
15     }
16
17     return 0;
18 }

```

Figure 3. Pseudocode representation of CURD algorithm.

Figure 3 present the algorithmic description of the CURD technique for literature search in any given problem domain. CURD allows quicker identification of most relevant articles and enable covering a wider publication timeline.

The combination of CURD and keywords search allowed enough literatures to be acquired for the study of existing privacy presentation approaches to achieve improved readability and consent. The findings were mapped to a privacy notice design space developed by association of academic researches and practitioners from leading internet industry (Google, RAND), and used to outline shortcomings and propose requirements for new artifacts to solve the problem. But for the requirements to be fulfilled, an extension of the privacy notice design space is a necessity.

3.2.3 The Design and Development

Design and development stages has been carried out in four transitions each of which iterated multiple times and individually contributed to the design and development of the XPNDS. Figure 4 illustrates the four transitions and their evolution sequences as follows;

3.2.3.1 Iteration 1

In the first iteration, the design process started with the literature review (Chapter Two) where design theory, constructs, and instantiations from prescriptive knowledge were used to generate requirements for the proposed objectives.

3.2.3.2 Iteration 2

For the second iteration, a design search process was initiated as in Chapter Four where descriptive knowledge on theories of eye movements in reading were used to validate the proposed requirements.

3.2.3.3 Iteration 3

The design search continued by iterating back to prescriptive knowledge where existing academic artifacts and consumer products were used to determine the applicability of the requirements in the real world setting. The design search has been extended to both prescriptive and descriptive knowledge to add research rigor.

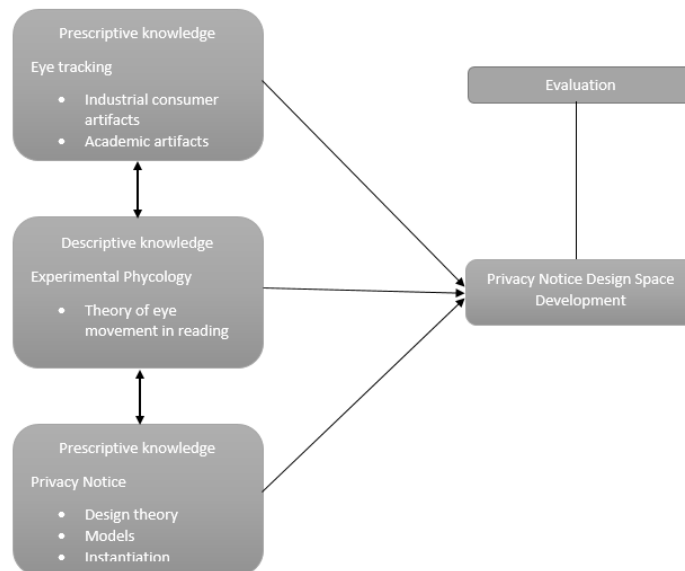


Figure 4. Design search's knowledge bases iterations for privacy notice design space development.

After these three transitions, a prototype of the XPNDS was ready for **Demonstration**, and hence evaluation and testing.

3.2.3.4 Iteration 4

The final design and development iteration involved the design feedback collected from the evaluation stage in Chapter Six. The evaluation involved expert reviews and application of the XPNDS in real world setting.

3.2.4 Evaluation

Evaluation of the XPNDS has been carried out following evaluation patterns for design science research as proposed in [35]. The pattern proposes four evaluation (Eval) activities from which the first two are ex-ante and the remain are ex-post as seen in Figure 5 below. Eval1 Activity serves to ensure that meaning full research problem is selected and formulated. This has been accomplished through the use of literature search and assertion to identify critical issues in privacy notice, research gap, objectives, and the requirements for bridging the gap. Eval2 Activity serves to show that an artifact design ingrains the solution to the problem in hand. A design search process has been used to demonstrate feasibility and accessibility of the requirements through mathematical proof and logical reasoning.

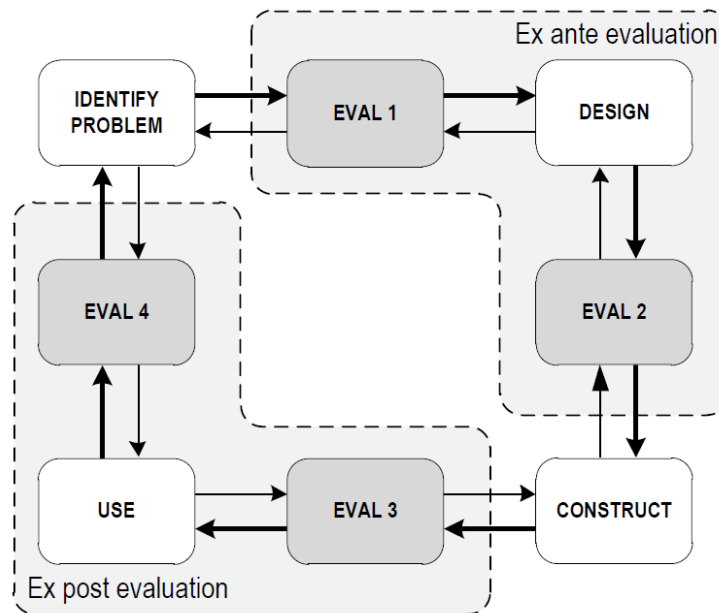


Figure 5. Evaluation activities within a DSR process [35].

Eval3 Activity serves to demonstrate how well the artifact performs while interacting with organizational element. In this activity the XPNDS's effectiveness and efficiency is demonstrated

by implementing it on use case scenarios that provides real tasks to the evaluation. More so, simplicity and understandability was determined through expert reviews. Eval4 Activity serves to finally show that the artifact is both applicable and useful in practice. For the XPNDS, a case study has been used to naturalistically determine the applicability, generality, and fidelity with real world phenomenon.

3.2.5 Communication

Communication of the XPNDS has been done first, through sending it to experts for reviews. Second, the work has been presented as a master's thesis research publication which is then made publicly available for references through the university library services.

CHAPTER FOUR

DESIGN REQUIREMENTS VALIDATION

4.1 Overview

Governing the design search for the new privacy notice design space are the requirements proposed to enforce the objectives in Chapter Two. The efforts for the establishment of the validity of the requirements lead for the search of theoretical grounding in several study domains to support the fulfillment of the requirements. The main promising domains that attracted the attention of the design search process of this work are those in Cognitive Science, Computer Vision, Human Computer Interaction, and Experimental Psychology. The goal of the design search is to find available knowledge in theory and practice that can support the effectiveness and feasibility of the proposed requirements and their inclusion in the development of the privacy notice design space in helping achieving the stated objectives.

In online services as it has been observed in Chapter Two, visual is the commonly used modality in design and presentation of privacy notice. Therefore, to assure that a subject comprehends notice contents, first it should be able to determine if the subject at least looked at, read, and comprehend the notice contents. Hence, the following sections dives in theories of eye movement in reading in search for possibilities of achieving processing and cognition consent levels requirements.

4.2 Eye Movement in Reading and Cognition

Studies on eye movement reports that an eye behaves differently during the reading of texts, scene (image) perception, and visual search [36]. This research work utilizes the laborious work done on examining cognitive processing tasks using eye movements to design implementable solutions for the proposed requirements for consent integration in privacy notice designs.

Eye movements has been widely adopted in investigation of cognitive processes during reading [36]. The research works on eye movement during reading are far ahead of those of scene perception and visual search. Eye movements consist of two main states, the saccades which is when the eye is in motion jumping from one location to another, and the fixation which is when the eye remain relatively fixed at a point [37] (see Figure 7). During fixation is when an eye is able

to acquire new information from the visual array. As information from different tasks like reading, scene perception and visual searching are also different with respect to cognitive mechanism involved, and hence fixation duration differs among them. Eye movements takes time to plan and execute as they are the simply motor responses [38]. The amount of time an eye takes to actually move is a function of the distance moved. Letters (most preferred as long as the texts are in a normal size [39]) or visual angels (degree) can be used to determine the distance. The average fixation duration of an eye during reading roughly lasts 200-250ms. From Table 3, in which FD and SL stands for fixation duration and saccade length respectively, it has been observed that fixation have a tendency to be longer in scene perception than in reading, also is longer in oral reading then in its silent counterpart. This observation is used by this research as has been used by many others to reach a decision that eye movements during reading can be distinguished from the one produced as a result of an eye engaging in other non-reading tasks. Most importantly, silent reading which is the most expected during the reading of policy notification, can also be distinguished from oral reading.

Table 3. The range of mean fixation durations and the mean saccade length in silent reading, oral reading, scene perception, and visual search [38].

	<i>FD (ms)</i>	<i>SL</i>	
		<i>Deg</i>	<i>Letters</i>
Silent reading	225–250	2	7–9
Oral reading	275–325	1.5	6–7
Scene perception	260–330	4–5	
Visual search	180–275	3	

Sophisticated devices such as high speed cameras are required to detect such fast movements. For experimental proposes, cameras with up to 1000 Hz (sampling rate/frame rate) and more are used in studying eye movements. These can capture changes within one millisecond which can be argued to be way more than what is required for tracking simple eye moment. However, for a camera to be considered high speed it needs the capability of frame rates in excess of 250 frames per second [40], which means it can take samples at an interval of 4 milliseconds. The speed is

continually increasing with other cameras having multiple times more frame rates than the original definition of a high speed camera.

Table 4. The effects of targeted cognition level on the experiment behavior.

Cognition Level	Eye Motion	Camera Power
Letter	Microscopic	Higher
Word	Small	Medium
Line	Significant	Moderate

Table 4 qualitatively illustrates how eye motion (saccade), and “relative” camera power requirements differ with respects to cognition level detection target of the experiment. Detecting letter by letter cognition requires more camera power than word by word cognition because it occurs very quickly. However, eyes make a more significant motion while scanning a line (words) than in reading an individual word. In the following section logical and mathematical proof are provided for possible determination of the suitable cognition levels.

4.3 Requirements Feasibility Proof Using Eye Movements Analysis

After having insight of eye movement theories above, this section uses mathematics, logic, and existing artifacts to set a proof of usability of these theories in adding assured informed consent in privacy notices. The section proceeds by searching and demonstrating what the theories have for each of the proposed requirements.

4.3.1 Processing

By “processing”, the recommendations require that the proof that the user is receiving and processing the appropriate notice using a suitable sense organ. The processing depends on the form of modality used to convey the privacy notice. Snice the focus is mainly on software services in this context, the common modality is visual.

The above findings from Table 4 suggest that the line cognition levels are more favorable to be used for determining user processing and cognition of the privacy notice with the available and future to come camera powers in mobile computing devices. For processing detection, a Gazing

technique which is based on line cognition level is proposed. The following subsections discuss the technique in details, and suggest their implantation.

4.3.1.1 Gazing

Gazing basically involves detecting where on the screen the user's eyes are pointing at. In the context of notice presentation, it does not give assurance that the user fully reads and understands the notice presented. However, it can at least assure that users sweep the eyes across and get a glimpse of the notice. This is important in fulfilling that the privacy notice has been processed with the appropriate sensory organ.

There are several implementation of gazing detection, most of which use gazing to detect what the user is doing (reading, skimming) [41], testing the usability of interface designs [42], implementing human computer interaction, and several others problem domains. This strengthens the concept of applicability of the gazing detection as it is assured that the algorithms exist and are implementable.

This research however, focuses only on eye motion (saccade) when it comes to gazing. As fixation is associated with cognition which is not the primary interest of the "processing" requirement. It is nevertheless understood that, even in gazing the user may stop and pick some of the words and skip a lot of them while searching for interesting parts of the texts, the user has to surely fixate at some points. Eyes move from start of the line to the end of the line (go-sweep) and jump back to the start of the new line below (return-sweep) and repeats to the end of the texts. For a notice with N lines of text, the normal number of sweeps (go-sweeps plus return-sweep) the eyes performs is given by the following equation.

$$f(N) = (N * 2) - 1$$

For determining "processing", it should not require that the eye should sweep the whole text document but instead an Appreciation factor (A) where $0 \leq A \leq 1$ should be introduced to limit the number of sweeps required for a notice to be considered processed. Hence the number of appreciated sweeps should be defined by the following equation.

$$f(N, A) = A(N * 2)$$

If quarter of the notice lines are required to be swept for the processing appreciation to be given, then $A=0.25$. Though the recommendation in this research is that the value of the appreciation factor should be 0.5 to allow half of the notice lines to be gazed. Any half line gaze should be ignored. Figure 6 illustrates a notice with $N=3$ and $A=0.5$. The order of which text lines are swept should not affect the appreciation of the processing. The user can skip some lines but should complete sweeping the minimum number ($f(3,0.5)$) required for appreciation to be granted, which in this case is 3.

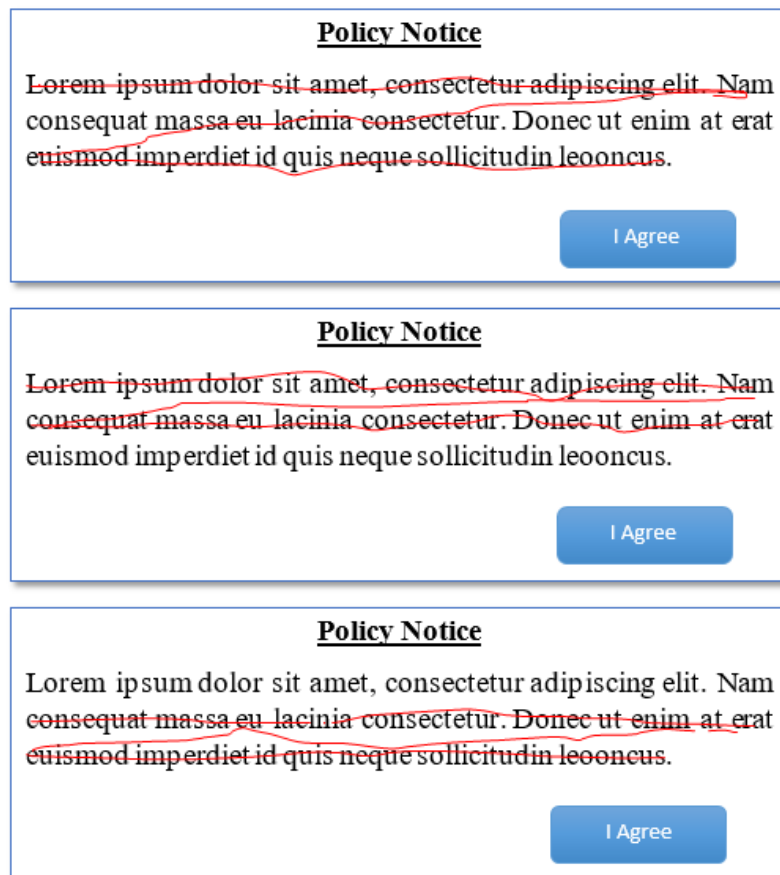


Figure 6. A sample illustration of acceptable gazing patterns for a notice with 0.5 Appreciation factor.

Finally using eye movements, the processing of a privacy notice can be achieved through gazing detection with a specified appreciation factor. This fulfils the first requirement for the improvement of privacy notice design to assure modalities are processed by their appropriate receiving organs. This design requirement engages the user more in determining informed consent

depending on the necessity set in the design of the notice. The following subsection examine the second requirement proposal for the objectives.

4.3.2 Cognition

The second requirement set for the objectives is a determinable cognition which requires the privacy notice design to include feature definition that can tell if the receiver of the notice comprehend the content of the notice so that the consent collected is an assured informed consent. Cognition involves mental action or process of gaining knowledge through thoughts, experience, and senses [43]. With online services as it has been noted earlier, the most commonly used modality in privacy notice design and presentation is the visual modality for which eyes are the subject's organs for sensing visual stimuli. Through reading, the cognition of privacy notice is mostly achieved and therefore the consent collected becomes assured informed consent. The following subsection examines the applicability of the reading process as an assurance to cognition of information presented by a notice.

4.3.2.1 Reading

Reading is a cognitive precise process involving a detailed sequential perception and identification of letters, words, spelling patterns, and larger language units [44]. During silent reading the eyes are engaged in unique characteristic behavior [45] composed of, as illustrated by Figure 7, saccades, return-sweep, regression, and fixation which is when the eye stops at a point and process the information. Almost all researches including [38] agrees that this is when cognition process takes place. This is supporting the regression concept in that, when a user finds a word difficult it is re-fixated to process it for the second time.

Findings shows that reading detection can be achieved in two ways. First by analyzing eye movement patterns through looking for fixations, saccades, regression and return-sweeps. This provide a one way reading confirmation as it can tell, in this context, if the user is reading but not necessarily tell what the user is reading or assure if the notice is the one the user is focusing on at the instance.

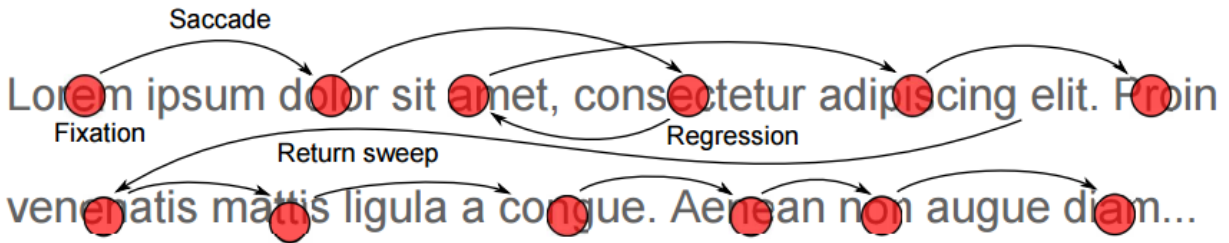


Figure 7. Eye movement during reading [46].

The second is by having a two-way confirmation by involving user's eye movement and gazing detection on the privacy notice canvas. This assures that the user is reading the specific privacy notice and that the specified notice is the one on the foreground. Detecting reading for a whole policy notice may be relevant for some scenarios but for others gazing should be enough.

This research's focus on reading detection is to reveal the subject's cognition process while reading the privacy notice. The frequent regression patterns and long fixations for example, can tell that the subject is having difficulties in understanding the words. However, it should be noted that the aim here is not to test the memory strength of the subject, but to assure that at that moment in time the subject comprehended what he was reading.

In addition, instead of just observing deviation of the fixation patterns from the average normal, the alignment of the fixation patterns to the generally expected pattern can also be used as determinant of user cognition of the privacy notice. Models for eye movement guidance [47] can be used to generate a pre-defined fixation patterns that will be matched with the real time user fixation positions to deduce the effectiveness of the reading. As concluded by Rayner, determining the next fixation position while reading is made on nonrandom basis [47]. More so, because factors such as conditional probability that a word will be fixated given that a prior word was or was not fixated [47], provides the requirement for the fixation order determination to be also conducted in real time and therefor established the pattern based on the user real-time fixation order by calculating probability of the next fixation point based on the previous and other essential factors such as word and saccade lengths. This approach of cognition determination is more appealing as it is localized to a specific reader instead of generalizing using pre-defined expected fixation patterns.

4.4 Practical Suitability of Eye Movements Detection Approach

It is common for people to access software services with their mobile computing devices such as laptops, tablets, and mobile phones. Desktop computers are also used especially in office and home environment. Therefore, the applicability of the above requirements fulfilling techniques needs to be possible on day to day user platforms used to access the services. In search for practicality of performing eye movement tracing using devices available on the market, as camera plays a key role in the service setting, a study for camera power in consumer divides devices was conducted. In the findings, a November 2015 released Apple 12.9 inch iPad Pro tablet was found to have slow-motion video support for 720p at 120 frames per second [48], which means it can take samples at an interval of 8.3 milliseconds with roughly half the speed of the of the definition of high speed camera. The March 2016 released Samsung Galaxy S7 has a slow-motion video support for 720p at 240 frames per second [49], allowing it to take samples at an interval of roughly 4.1 milliseconds with roughly the same speed as of the definition of a high speed camera. Although these particular cameras with such capabilities are the rear cameras that can't be practically used to capture the users face at the time of reading a privacy notice, such a powerful camera in less than 8-millimeter-thick devices proves the possible mobility of the service setup and ability to be used on demand while integrated within normal computing devices. It can also be noted that the frame rate doubled with in the relative four months between the two releases.

Conclusively, this section successfully prove that the processing and cognition requirements can be achieved using existing knowledge on eye movements, and consumer products capacity at an experimental level. That is, these features can be integrated in day to day products having the necessary requirements as discussed above. The research uses the claim of the requirements and the proof of the applicability as contribution in the design search for modification and extension of the privacy notice design space as the next section details.

CHAPTER FIVE

THE EXTENDED PRIVACY NOTICE DESIGN SPACE

5.1 Design Process

The Privacy Notice Design Space originally proposed by Schaub et al. [12] underwent a rigorous design process including iterations on multiple expert reviews to its release stage. Nevertheless, they still called for further extension of the design space to accommodate future technology expansion. The design process for the construct in this research work introduces two main changes to the original design space. First, the existing design space has been refactored (i.e. improve the contents of the control dimension without replacing the dimension itself). Second, the design space has been extended to explicitly accommodate consent in the design of privacy notice.

The design process traces back to the objective identification stage in which, as illustrated Figure 4, prescriptive knowledge from models, instantiations, and design theory were reviewed to propose requirements for the prospective improved design space. The demand of the requirements steered the search to descriptive knowledge from Experimental Psychology domain where theories of eye movements were used to approve the validity of the requirements. More so, the search iterated back again to prescriptive knowledge where academic and industrial instantiations were combined to prove the possible applicability of the requirements at an artifact instantiation level. The details gathered from each knowledge domain were used iteratively providing rigor to development of the new privacy notice design space construct.

The goal of the design and development has been to introduce the notion of consent in privacy notice design space so that engineers, developers, and managers can explicitly decide and understand the level of consent that their privacy notice should have or has respectively. All the iterated stages contributed to the design and development. The execution was not straight forward, instead, back and forth marches between the knowledge bases were active until the final acceptable design space was achieved.

5.2 Development Process Consideration

As it has been mentioned above, the development of the design space took contribution from different research steps. The development of the Extended Privacy Notice Design Space has been conducted in a way to fulfill the objectives and requirements initially proposed. Different design ideas were collected from the above research sections to arrive to the final design space construct. Figure 8 shows how these research components contributed to the design and development of the extended privacy notice design space construct and the development process is described as follows as numbered in the figure:

- 1) As consent was required to be integrated with in a privacy notice design construct, a robust existing privacy notice design space was selected to be the foundation of the new design space.
- 2) A consent dimension was added in the design space in response to the first objective that requires an explicit integration of consent in the design. The new design space has five dimension with that of consent explicitly identified.
- 3) From the literature review and artifact analysis, two consent levels were observed to be implemented, these include the “assumed” and those that demanded “interaction”. Hence, these levels were therefore included in the design as consent levels.
- 4) The literature study ended with proposing requirements for the new design space. After they were validated through design search process, the processing and cognition consent levels were added to the design space. Only these consent levels were taken through the design search because they were not found in literatures to be applied in privacy notices.
- 5) At his point, the four consent levels added to the design space fulfilled the second objective of defining different levels of consent in the new design space. These levels started from assumed consent to assured informed consent (cognition).
- 6) Finally, the control dimension was improved as part of design process through feedbacks from iteration processes. And hence optional and settled components were introduced to the design space.

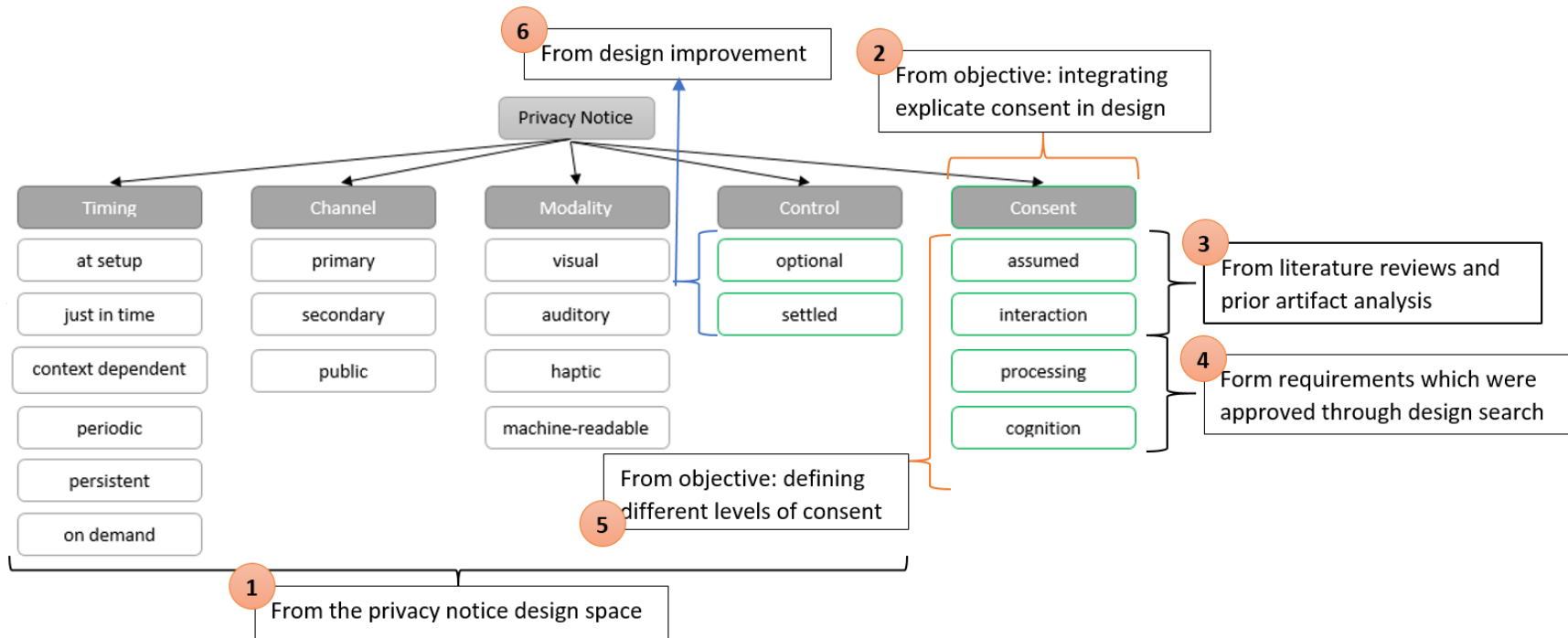


Figure 8 Contributions of different research steps/actions/iterations to the design and development of the XPNDS.

5.3 The Extended Privacy Notice Design Space Construct

Figure 9 presents the Extended Privacy Notice Design Space (XPNDS) from the last development iteration. It should be noted that most of the components remains from the original work by Schaub et al. [12] where full credits are attribute to them. The addition and modification contributed by this research work is highlighted with green outline. The control dimension remains from the previous construct but its components have been changed and a new consent dimension has been added along with its new four components.

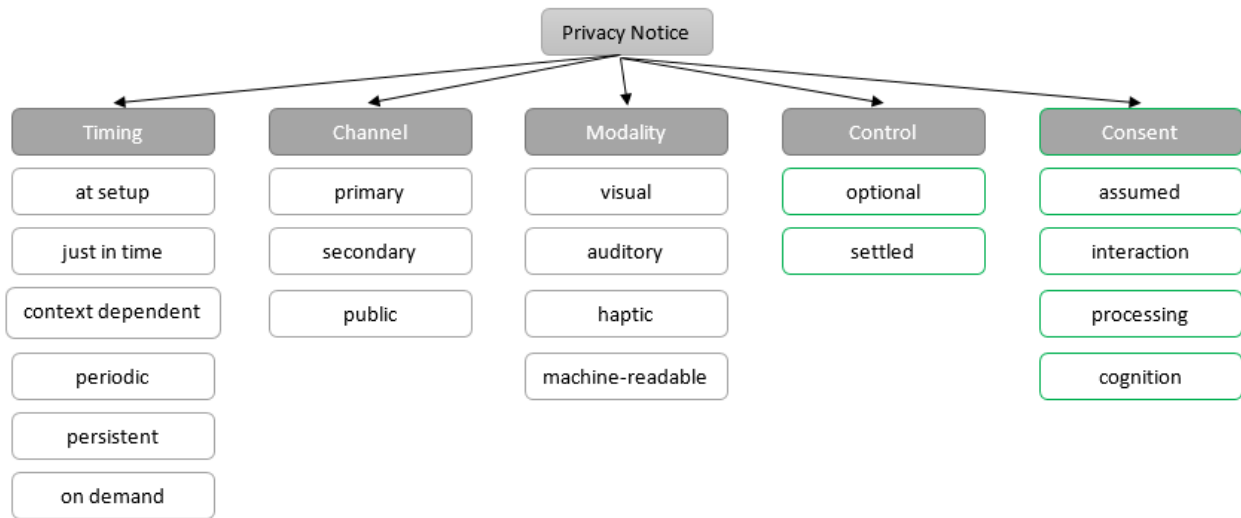


Figure 9. The Extended Privacy Notice Design Space.

The dimensions in the refactored design space are; Timing which tells when the privacy notice is presented, Channel which specifies the platform used to present the notice, Modality which specifies the interaction means provided to the subject, Control which specify what controls the subject has to notice, and Consent which establish the control that the notice has on the subject in assuring a desired level of consent is achieved. Timing, channel, and modality dimensions have not changed and therefore their discussion in Chapter Two holds. Also the original work may be referenced in need for further detailed description. Here the discussion focus mainly on the improved and added dimensions. The following subsections discusses the control and consents dimensions’ design features widely.

5.3.1 Control

In privacy notice design the Control dimension provides data subjects with certain level of negotiation on the way their collected data are stored, processed or shared by the service provider (customer-to-vendor privacy) or control over accessibility of their data by other users of the same service (customer-to-customer privacy). The former has been customarily (not necessarily) provided as a binary option opt-in or opt-out while the later can have more than two choices. It is a good practice to give users control of their data and as many options as the policy can supply, as this increased user's trust [50] to the service. However, still there are polices that find themselves unnegotiable.

Below are the two components of the Control dimension proposed by this research, unlike the original design space (see Figure 1), the proposed design space does not include "Decoupled" component which describes privacy controls that are separated from the notice as part of the Control dimension. This research argue that a privacy notice is a subset of a privacy policy and each privacy notice can apply the design space dimensions' components in parallel, both horizontally and vertically. Therefore, separated privacy options mean that part of the privacy policy (privacy notice) utilize a different Timing dimension component, for example a policy may provide notice "at setup", and also have the privacy options notice available "on demand".

5.3.1.1 Optional

Control is optional when the notice design gives a user options to control some of either usage, sharing, or processing of their data in a customer-to-vendor privacy agreement. The standard control options are the one brought forth by W3C's machine readable privacy policy languages such as P3P [17] that provides user with options to agree on data collection policy (opt-in) or deny a data collection policy (opt-out). These options can be presented to the user through "secondary" Channel using Privacy Enhanced Technologies [22] tools or browser privacy setting windows. The options may also be presented through "primary" Channel by being part of the software system.

On the other hand, there are also consumer-to-consumer privacy settings which gives more broad options to the users to establish control on what the other users sharing the same service with can

access among their data. A good example is the Facebook's privacy Public, Friends, and Private privacy notice control options available for the user data sharing on the platform.

The opinion of this research differ from the original work on placing of "blocking" and "non-blocking" components as part of Control dimension. This research argues that Control should explicitly provide what users can do to the system and not what the system can do to the user. In fact, blocking and non-blocking addresses the efforts in accomplishing user's informed consent. This is an example of cases where the consent in notice design is addressed implicitly.

5.3.1.2 *Settled*

Settled privacy notice do not provide the data subject with any options, the service provider requires the subject to agree with the whole policy notice requirements to use the service. In case the subject is not comfortable with the policy notice or some part of it, has to avoid using the service entirely in the first place. Most simple website and consumer devices use "settled" Control on privacy notice. But for complex data sharing platforms "optional" Control should be considered in the design of the privacy notice.

5.3.2 *Consent*

The Consent dimension of privacy notice design provides the privacy notice with certain control of the user. It allows the notice to specify the level of attention the user should provide to satisfy that an informed consent has been collected. Informed consent encompasses notifying users on the potential privacy notice and giving them explicit opportunity to consent or decline [5]. Assured informed consent focuses on both notice presentation and user understanding of the notice contents.

This design space proposes four design categories for consent determination in privacy notice design which are Assumed, Interaction, Processing, and Cognition. Consent design choices for privacy notice design should be determined by conducting privacy impact measurement of the service in question. This research work does not provide any privacy impact ratings, but the designers should consult appropriate authority for criteria to reach suitable privacy impact rating for each consent level in their context.

The design principles proposed by this privacy notice design space dimension explicitly implements four of the five components of informed consent as proposed by Friedman et al. [6] which are Agreement, Competence, and Comprehension. Disclosure is covered by other dimensions while Voluntariness still need more effort to assure and for now is just assumed. Also, the design space further guides privacy notice designers in helping users interact effectively with the notice so that they understand the notice and hence informed consent is collected. The following are the consent design categories in detail.

5.3.2.1 Assumed

A privacy notice Consent is “assumed” when the privacy notice design does not require any approved subject’s awareness of the privacy notice. That is, the notice does not have to explicitly assure that the subject is aware of its presence, is competent, or is engaging voluntarily. Instead, by just using the service itself it is assumed that the subject understands and agrees with the privacy notice.

Most of the time “assumed” Consent notice designs are applied in frequently used common services like consumer products and websites, in which the service providers do not necessarily know their service users (no user registration for the service). For instance, notice that uses “public” Channel are more likely to apply “assumed” Consent. An example is a public CCTV privacy notice; it does not guarantee the user is aware of it but it is only assumed so. Consequently, “assumed” Consent design practice should only be used for services that has as little privacy impact as possible.

5.3.2.2 Interaction

Privacy notice designs that implements “interaction” Consent requires the user of the service to perform an interaction with the privacy notice to prove agreement with the notice. The notice may require a user to perform interactive action like clicking an agreement button, scrolling down the notice content’s end, or drag and drop some of the notice contents [51] so that the assurance that the user is aware of the presence of the notice is achieved. It should be noted however, “interaction” Consent in a privacy notice design does not guarantee that the user has either read or understand the notice, instead assures that enough minimum attention to perform the interaction has been provided by the user. This minimum attention is what Bravo-Lillo et al. referred to as habituation

[28]. Frequent user's exposure to similar "interaction" notice designs increase their ability to interact with minimum possible attention. It is upon the designer of the privacy notice to use their creativity in crafting interactions that will take enough attentions of the user to achieve more than just interaction. A proper planned interaction can convince the assumption of user reading the privacy notice.

Interaction Consent is a widely used in personal data collecting services, although it can be argued that it is not fair for a legally binding agreements be depending just on interaction as it provides a loophole for service providers to abuse the customer's impatience of using services. It is recommended for the designers to act ethically and fairly in helping collecting a reliable customer's informed consent.

5.3.2.3 Processing

Processing Consent in privacy notice design requires the privacy notice to be processed by an appropriate recipient means based on the Modality used. The notice should also be able to confirm the occurrence of the processing action. The recipient means should be suitably selected based on the Modality used. For instance, "visual" Modality will require subject's eyes for determining processing. As "interaction" Consent cannot guarantee if the user at least looked at the notice, "processing" Consent aims to tell if the user processed the notice with appropriate means, in this case passing the eyes on the notice. In this way processing can also be used to assure the competence of the subject as required by [6]. If a policy requires the recipient to be in certain age group for example, facial recognition can be used to determine if the notice recipient really belong to the required age group.

The growth of technology and the spread of internet of things and everything in everyday life provides opportunities to improve interactions between the user and the services. "Processing" provides a reasonable consent claim and a good way to help users face the privacy notice and make informed decisions.

5.3.2.4 Cognition

The main goal of the privacy notice is for the service providers to be able to claim that the subject has read and comprehend the privacy notice. But this has not yet been affectively integrated in the

previous design space. Hence, “cognition” Consent in privacy notice design requires the privacy notice to be able to determine and study cognitive patterns of the subject while interacting with the privacy notice. This will allow the notice to be able to determine subject’s insight of the notice. For example, determining words, phrases, and sections of the notice that provides difficulty or ambiguity to the subject, identifying areas that most users face difficulties in comprehending, and generally being able to assess the effectiveness of the notice in conveying the message. This allows the privacy notice design consideration to also go deeper into the design of the contents of the notice themselves.

Cognitive Consent is mostly applicable in service domains where service users have much closer relation with the service provider. And thus, the service provider needs assurance that the user has read and comprehend the policy notices. This can be exemplified within organization domains in which the service provider (employer) provides privacy notice to the subject (employee). Surely the service provider has a comparatively closer relation with the subject (employer-employee) and therefore the employer may need to make sure on the employee’s cognition of the privacy notices. All in all, the privacy and legal impact of services should be used in determining the requirement of assured informed consent in the privacy notice design.

CHAPTER SIX

EVALUATION

6.1 Overview

Artifact evaluation is vital part of design science research used to demonstrate utility, validity, quality, efficacy, and fitness of the designed artifact as well as the rigor of the design process. This section documents the ex-post evaluation of the proposed Extended Privacy Notice Design Space. Never the less, other ex-ante evaluations such as literature review and review of practitioners' initiatives have been carried out prior the design stage. The evaluation stage itself also contributed to the design of the artifact and hence it is difficult to alienate it from the development process. Efforts were made to assure that both naturalistic (case study, use case) and artificial (expert review, research rigor) evaluations were involved so that a stronger proof of the artifact utility is established.

The section proceeds as follows: First, the evaluation uses a case study to determine the utility of the design space using a “real system” reality. Then, use cases with “real task” determines fidelity of the Extended Privacy Notice Design Space with real world phenomenon and its effectiveness. Furthermore, validity and quality of the design space is deduced from the reviews of the experts in privacy notice design from both the industry and academia. Finally, the research rigor is evaluated against the seven design science research guidelines by Hevner and Chatterjee [10].

6.2 Case Study Evaluation (ericsson.com)

Ericsson.com is a “website” for a Swedish multinational communication technology corporation. The website is used for publicizing the company information to the general public and does not require visitor registration. As with most websites, ericsson.com also provides it users with privacy policy through privacy notices. As study on the privacy policy communication by ericsson.com to its potential visitors revealed that the website implements three interlinked layers of privacy notices which are below analyzed and mapped to the Extended Privacy Notice Design Space as follows.

6.2.1 Privacy notice layer I

The first layer of privacy notice notifies the visitor on ericsson.com use of cookies. As a website that operates within the European Union, it is required by the law that the website should explicitly notify the user on the use of tracing cookies. Ericsson.com fulfills this by presenting visitors with a “persistent” (Timing) notice (Figure 10) blended at the top of every page of the website (“primary” Channel). The notice does not provide any options to the visitor (“settled” Control) and visitor’s consent on the notice is merely assumed by continuation of browsing the website. The notice also collects the visitor’s consent through clicking of “I Accept” button (“interaction” Consent). However, whenever multiple consent determination levels are used, the minimum consent level remains practical and therefore, in this case, even if the interaction consent is present, the assumed consent is the real consent of the privacy notice.

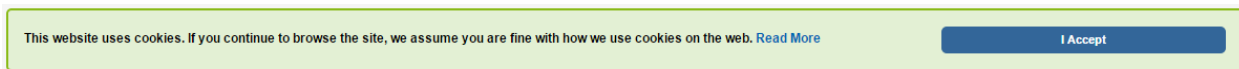


Figure 10. First Layer cookies privacy notice for ericsson.com

The use of multiple consent level is among the tricks used by some notice providers to demonstrate that an informed consent is collected from the user while in reality is not necessarily so. The notice however proved the visitor with a link to the next layer of privacy notice through “Read More”. Figure 11 below illustrate XPNDS model of the notice.

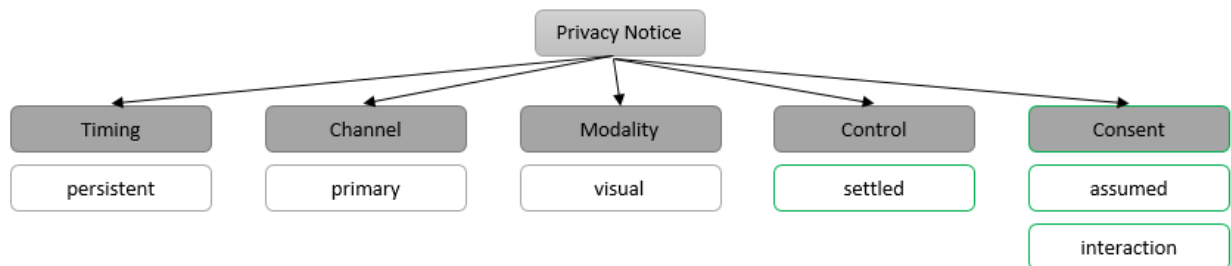


Figure 11. Layer I notice design interpretation on XPNDS.

6.2.2 Privacy notice layer II

The second layer of privacy notice provide detailed information on cookies and internet privacy policies. The notices are available for visitors to access them “on demand” (Timing) through hyperlinks leading to dedicated webpages on the website (“primary” Channel). Both notice

contains large content of “settled” (Control) policies and they neither provide user with any options over the policies nor does their consent collection is determined (“assumed” Consent). However, as with the first layer, the second layer also provides reference to the next layer of privacy notice. Figure 12 below illustrate XPNDS model of the notice.

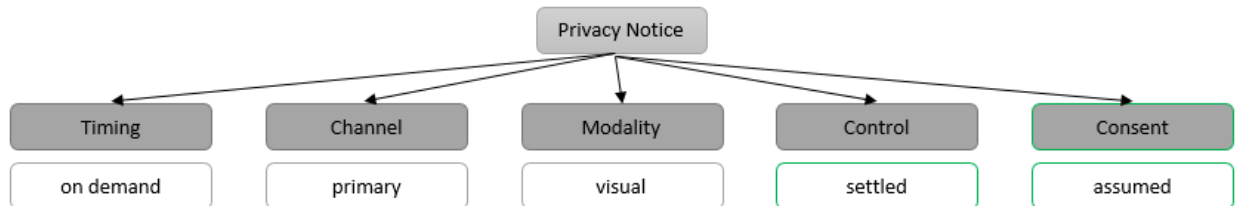


Figure 12. Layer II notice design interpretation on XPNDS.

6.2.3 Privacy notice layer III

The third layer of privacy notice is available “on demand” (Timing) from browsers privacy settings (“secondary” Channel). The notice provides the user with several privacy options (“optional” control) setting including whitelisting and blacklisting websites’ cookies through allow, block, or clear-on-exit options, specifying cookies life time, and view existing cookies. Figure 13 illustrates cookies settings as in Google Chrome web browser.

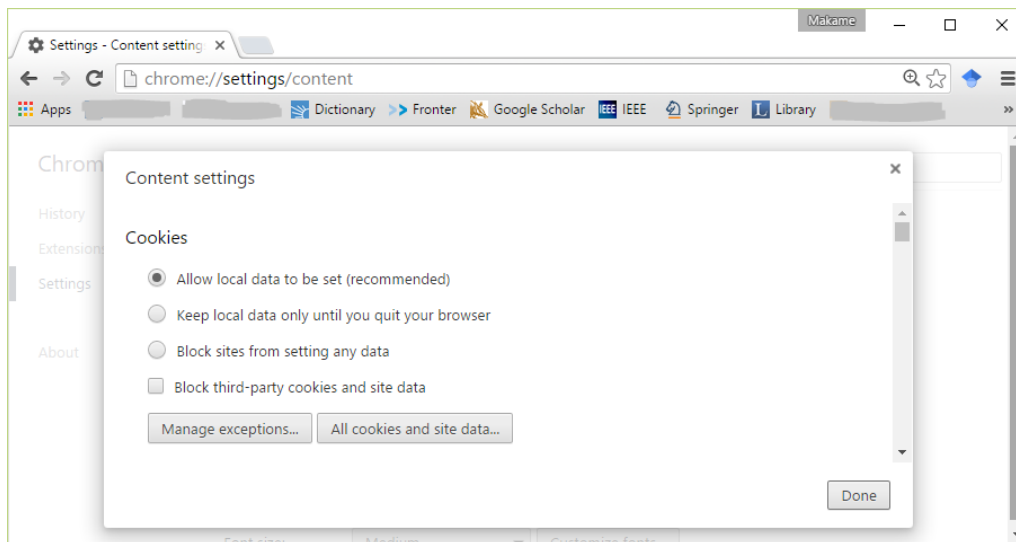


Figure 13. Cookies content setting in Google Chrome.

The user preferences are then communicated between the browser and the web server via “machine-readable” (Modality) and hence the web browser prevents the site from implanting or

accessing cookies on the user’s machine. Summary diagram below, conclusion on the fitness of the model on the architecture. Figure 14 below illustrate XPNDS model of the notice.

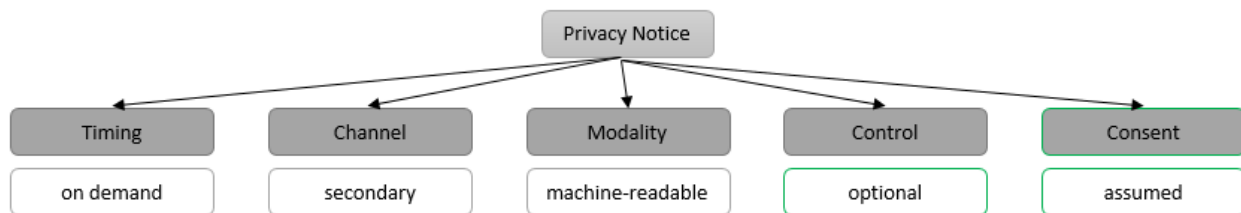


Figure 14. Layer III notice design interpretation on XPNDS.

6.3 Use Cases Evaluation

Here the XPNDS is evaluated by reflecting it in different real world use cases. Its suitability with the existing privacy notice designs is established to demonstrate its utility, efficacy and validity. Also, the ability for the design space to support new technologies for privacy notice presentation with a focus on applying appropriate informed consent. Since the privacy notice design space is intended not only for software services but all possible domains where privacy notices are applicable, here some of these domains are discussed as follows.

6.3.1 LinkedIn Profile Privacy Notice

The first use case is drawn from online software service. A notice design implementation from social networking platform LinkedIn is analyzed using XPNDS. LinkedIn.com provides it users with persistent (Timing) privacy notice on their profile page (“primary” Channel) that gives the users options (“optional” Control) on whether their profile changes are published to other users in their network or not. Figure 15 illustrate the notice appearance.

The notice has a default “yes” option and unfairly the notices is not visible to the user until the page is scrolled down (at least at 100% browser zoom level on a large screen device). The users may perform profile changes without being able to see the notice and their informed consent be assumed (“assumed” Consent). Hence, even if the user is given options, the consent level applied does not guarantee the user will be aware of the notice. Figure 16 shows the analysis using XPNDS construct.

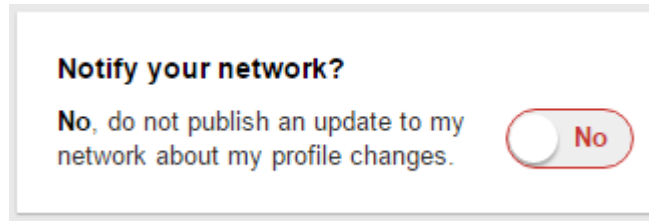


Figure 15. LinkedIn profile privacy notice.

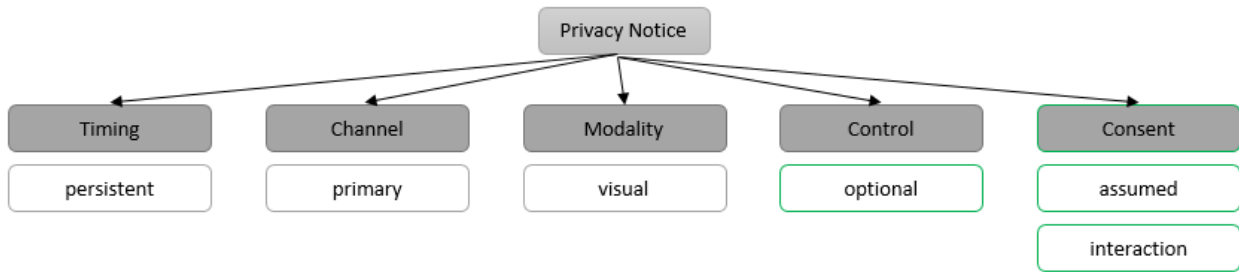


Figure 16. XPNDS analysis of LinkedIn profile privacy notice.

6.3.2 Windows 10 Phone Location Access Notice

Some mobile phone applications require location information of the device and hence of the user to operate orderly. Application accessing device location in windows 10 mobile provides a “visual” (Modality) notification only at the first time the application attempt to do so (“just in time” Timing). The user is presented with options to allow or deny the request (“optional” Control). Consent is collected by users’ interaction with the notice’s “yes” or “No” buttons (“interaction” Consent) and therefore user cannot use the app until the interaction is fulfilled.

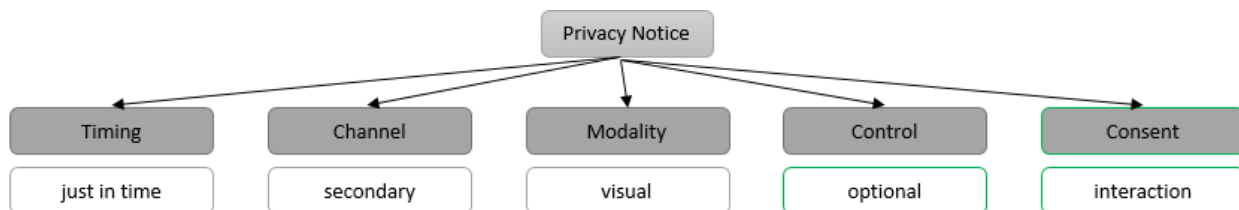


Figure 17. XPNDS analysis of Windows 10 mobile location access notice.

The notice design structure presentation on the XPNDS construct is as shown in Figure 17 above. On the next page, Figure 18 illustrates a Windows 10 mobile location access notice discussed above in action.



Figure 18. Windows 10 mobile location access interactive notice.

However, windows 10 mobiles also provide another layer of privacy notice on location access (Figure 19). A location icon (‘visual” Modality) appears on the task bar every time an application access device location (“just in time” Timing). Knowing the user has already allowed access to the application in the first place (“settled” Control), the notice does not require any additional user consent approval (“assumed” Consent). In Figure 19 the location icon pointed with the silver arrow. Finally, the analysis of the notice on the XPNDS is as in Figure 20 next page.



Figure 19. Just in time location access notification in Windows 10 mobile.

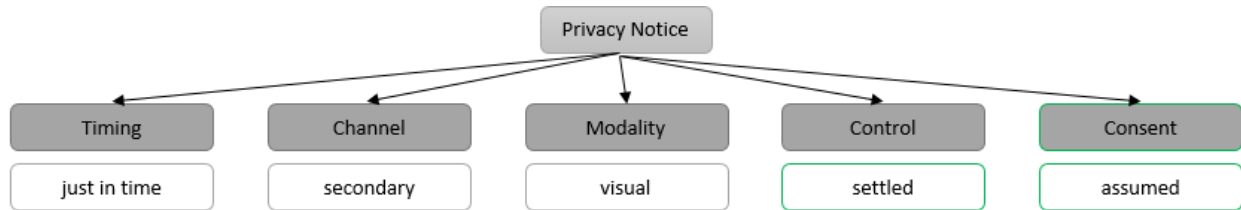


Figure 20. XPNDS analysis of Windows 10 mobile just-in-time location access notice.

6.3.3 Assured Informed Consent Use Cases

The last two Consent categories (processing and cognition) aims for bringing about assured informed consent in the designs. Although they extend “interaction” category, they specifically provide assured informed consent specific actions to the notice i.e. they add assurance of comprehension, competence, and agreement as suggested in [12]. This research has not come across a privacy notice design that takes consent to these categories. However, proof on implement ability of these categories exists in some Human Computer Interaction researches and artifacts as in [41, 52, 53] as well as in computer vision as proved by the design search process in Chapter Four.

Cognition can also be determined as theorized in eye moments research works [34, 54]. These categories have their place in privacy notices as described in the design space description above. Current devices (cameras power) capabilities are matured enough to support. The existing problem is the difficulty in implementation as not every developer has the resource to implement these complex algorithms. However, with the growth of cloud API services such as Microsoft Cognitive Services [55] which provides several cognitive service API easily for developers to integrate in their applications. And if assured informed consent determination service API are provided, assured informed consent in privacy notices will become the new normal. Their availability will also give chance for data regulators to push for higher consent requirement in notices. Processing and cognition API for assured informed consent needs also to be provided the same way to be widely adopted.

6.4 Experts Evaluation

As part of evaluation and communication, the XPNDS construct was communicate to four privacy notice design experts through email for reviews. This expert group involves the ones that

participated in the design on the initial privacy notice design space (which did not address consent explicitly) that was used as the foundation for the XPNDS. In general, positive reviews were received from the experts, in such, bellow is a comment from one of the expert after reviewing construct.

This is a very interesting idea. I encourage you to build out a few examples (like we did in the paper) that show how notices could fall into these additional categories and what they might look like.

The expert seems very interested with the XPNDS and asked for use case sample demonstration of the construct. In response, the use case samples were conducted. Despite the unfortunate events of some participant not replaying. In general, the XPNDS achieved additional face of validity form the available expert reviews.

6.5 Evaluation of Research

Previous sections extensively demonstrate the building and evaluation rigor of the Extended Privacy Notice Design Space (XPNDS) to clearly establish construct's utility, completeness, ease of use, and understandability. In addition to that, evaluation of research is conducted by following Hevner and Chatterjee's 2010 [10] guidelines for conducting and evaluating design science research in Information System. Seven guidelines are proposed and has been fulfilled by this research work as follows.

Guideline 1 calls on ensuring that the problem brought forward by the research has significant relevance in the field. This work presented the problem of lake of clear consent integration in privacy notice design to achieve assured informed consent, and the fact that there are no practical consent design guides allows unethical policy providers to provide illusive consent and claiming they are abiding with the regulatory standards. Therefore, it is important to have explicitly established consent in design space construct to help privacy notice designers integrate required level of consent in their notice and regulators to be able to analyze and identify applied consent levels in applied notices.

Guideline 2 is on ensuring the research process uses rigorous methodology in construction and evaluation of the design artifact. Following Peffers et al. [34] design science research methodology

the XPNDS has been achieved through multiple iterations between design and evaluation. Both build and evaluation processes were conducted with reference to respective authorities in design science research domain.

Guideline 3 is about implementing the design of the artifact as a search process. The development of the XPNDS involved design search from academic literatures and practitioners, testing relevance of requirements from eye movement theories, and proving of applicability of the objectives from consumer electronic artifacts. All these fields have been traversed in search of proper design for XPNDS.

Guideline 4 is about ensuring that the designed artifact is effectively presented, to enable application and implementation in appropriate environment. In this work the artifact has been presented as a construct which extends the vocabulary and taxonomy for privacy notice design to include desired consent levels. A detailed description of the model has been provided along with sample use cases that helps in demonstrating implementation of the XPNDS in different scenarios.

Guideline 5 is on ensuring well-executed evaluation methods are used to demonstrate the quality and efficacy of the design artifact. The evaluation of the XPNDS followed evaluation patterns as presented in [35], the process included observational evaluation methods such as Case Study to demonstrate the utility of the artifact. Also, analytical evaluation methods such as Static analysis (through Demonstration and Logical reasoning) and Architecture analysis (through expert reviews) have been used to examine the artifact quality, completeness, ease of use, simplicity, elegance, and understandability which are evaluation criteria suggested by March et al. [56].

Guideline 6 calls on presenting a clear contribution of the research. The contribution of this research work is clearly presented in the discussion chapter. This includes explicit integration of consent levels in the privacy notice design space as well as introducing additional vocabularies for consent in the design space that helps privacy notice designers and managers have the common tongue on consent design in privacy notices.

Guideline 7 requires presentation of design science research to management audience. Though expert reviews and feedback. The XPNDS construct has proven to be well presentable to managerial audience with less efforts. The construct is also provided to open source community

via GitHub and the research publication is made available online for academic search through university library.

CHAPTER SEVEN

DISCUSSION

7.1 Overview

This section provides the holistic overview of the achievements obtained throughout the research work in the development of the XPNDS construct. Though this work, several contributions can be claimed in practice, method, and theory. More so, the results from the evaluation of the XPNDS well proves the artifact utility and research strength. A detailed discussion proceeds by considering the following aspects.

7.2 Design Output Interpretation

The XPNDS has been proven to stand strong as a design science research product by multiple rigorous evaluation methods used. Case studies demonstrated the utility of the XPNDS and its fit with existing privacy notice designs, this is important as it validate backward compatibility of XPNDS to existing privacy notice designs. That is, the XPNDS can be used for analysis of existing privacy notice designs as well as a guide for development of new privacy notices. Furthermore, positives reviews form privacy notice design space expert evidences XPNDS acceptance by the research community and hence demonstrate the understandability and elegance of the XPNDS.

7.3 Objective Fulfillment

The XPNDS succeeded in accomplishing the initial objectives of the research, it successfully provides guidelines for privacy notice designs, integrate consent in the designs, and most importantly its categorize the consent implementation in different possible levels of user's consent determination. The design space provides opportunities in shifting from the olds ways of consent determination and support the embrace of new technologies in search for assured informed consent determination. The main contrast of XPNDS with previous models like that of Friedman et al. [6] is that its goes beyond telling what an informed consent is and also tells how a certain level of it can be practically achieve in a design. The use of Schaub et al. [12] privacy notice design space as the base foundation for XPNDS allows the construct to exceed research expectation by not only provide explicit consent in privacy notice but also resulted to a full flagged privacy notice design

space that inherits the rigor from its design foundation. Hence, the XPNDS is a synergy of the Friedman's informed consent conceptual model and Schaub's practical privacy notice design space.

7.4 Contribution to Practice

This thesis work contributed to practical knowledge that allows explicit integration of consent in the design of privacy notices. The significance of XPNDS to practice includes (1) practitioners are provided with explicit practical design guides for integrating consent in privacy notices, (2) managers are able to use the construct guides in determining the level of consent to be used in the design based on policy or privacy impact, (3), it provides the regulatory bodies with means of evaluating the level of consent implementation in privacy notices and ability to detect illusive consent design that circumnavigate the regulatory requirements and (4) it provides standard design communication platform between regulators, managers, and practitioners. This collectively bridge the prior existing gap on informed consent in privacy notice design.

Furthermore, the research works also provides some practical methodological contribution on effective implementation of literature review search. A CURD model for conducting literature review takes advantage of the modern features of academic search engines that provide "cited by" and "references" lists to quickly and widely cover academic domain literatures while overcoming the barrier caused by keyword or title mismatch.

7.5 Implication to Knowledge

This research argues that the XPNDS provides an addition to the body of knowledge by providing design guide that explicitly integrate consent in the design of privacy notice before which it was just implicitly assumed to exist. Its provide the "less-covered" practical guide instead of just stating what a good consent is.

7.6 Limitation of the Research

The XPNDS has been formally evaluated using case studies from the industry which demonstrated its applicability in the analysis of informed consent determination of existing privacy notice designs. However, further evaluation that will apply the model in the industry as a guideline for

designing privacy notice and have feedback from practitioners and managers should be done to firm the artifact utility in both areas.

The research also involved experts in the area privacy notice designs, four experts were approached. Despite the selected experts having stronger ties to the field and their academic and industrial diversity, the greater the sample size of reviewing experts the better the strength of the result.

Also, although the experts were approached individually, since the request was about the idea they have work on together before, they carbon copied each other on their response that lead to some of them assume they have the same opinion as the one suggested by their colleague and therefore did not provide their individual review.

Finally, despite the huge efforts invested in the design and development of the construct, still the construct is not complete or absolute and therefore needs further improvement and development iterations.

7.7 Lesson Learned

Much has been learnt from the research process experience including the difficulty of documenting design science research report incrementally during the research period. Due to the trial and error [10] nature of the design iteration process, it is much proper to spare a thesis scale report writing process after the build or evaluation processes are completed.

7.8 Future Works

This thesis has presented a design guide for privacy notices for explicit integration of informed consent. It provides different levels of consent, from assumed, informed consent, to assured informed consent. Despite the proof of concept of assured informed consent presented in this work, not all service providers have resource to implement these high level algorithms and it will be much easy to have such functionalities provided as cloud service APIs that can be easily integrated in in privacy notice designs. This will boost the adaptation of using higher level of consent determination among venders where necessary and will also allow the regularity bodies to have argument for asking for higher consent level implementation.

Moreover, the XPNDS has to incorporate voluntariness component of online informed consent achievement requirements. Further work is also required in this area to perfect informed consent online.

CHAPTER EIGHT

CONCLUSION

This thesis works addressed the need for explicit integration of consent in privacy notice designs by presenting the Extended Privacy Notice Design Space construct that explicitly guides on incorporating different levels of consent in privacy notices. Theories of eye movement in reading were used to establish and incorporate higher level of consent determination to an assured informed consent level. Unlike most works available in the literatures on consent, this work guides to the practicality of achieving assured informed consent in privacy notices and not only on theoretical opinion of what informed consent is. The developed construct can therefore be used by managers to communicate, practitioners to design, and regulators to analyze application informed consent in privacy notice designs. Hence, effectively fulfilling the prior established objectives.

The utility and effectiveness of the XPNDS have been proved with case studies and use cases from real world scenarios, and its understandability and completeness demonstrated with positive expert reviews. It is the hope of the author that the XPNDS will be useful to both practitioners and academicians in incorporating informed consent in privacy notice designs to an assured level.

REFERENCES

- [1] E Commission, “Commission proposes a comprehensive reform of data protection rules to increase users’ control of their data and to cut costs for businesses”, Reference IP/12/46, 2012.
- [2] Allen & Overy, “The EU General Data Protection Regulation is finally agreed”, London, Allen & Overy LLP. 2016.
- [3] Luger E, Rodden T. Terms of agreement: rethinking consent for pervasive computing. *Interacting with Computers*. 2013 pp. 229-41.
- [4] Bonnici CJ, Coles-Kemp L. “Principled electronic consent management: A preliminary research framework in Emerging Security Technologies (EST)”, in *International Conference on. IEEE*. 2010. pp. 119-123.
- [5] Friedman B, Khan Jr PH, Howe DC. “Trust online”, in *Communications of the ACM.*, vol. 43, no. 12, 2000, pp. 34-40.
- [6] Friedman B, Felten E, Millett LI. “Informed consent online: A conceptual model and design principles”, *University of Washington Computer Science & Engineering Technical Report 00–12*, 2000.
- [7] Recupero PR, Rainey SE. “Informed consent to e-therapy”, in *American Journal of Psychotherapy*, vol. 59, no. 4, 2005, p. 319.
- [8] Luxton DD, McCann RA, Bush NE, Mishkind MC, Reger GM. “mHealth for mental health: Integrating smartphone technology in behavioral healthcare” in *Professional Psychology: Research and Practice*, vol. 42, no. 6, 2011, pp. 505.
- [9] Agarwal S, Lau CT., “Remote health monitoring using mobile phones and Web services” in *Telemedicine and e-Health*, vol. 16, no. 5, 2010, pp. 603-7.
- [10] Hevner A, Chatterjee S., “Design science research in information systems”, Springer US; 2010.
- [11] Gregor S, Hevner AR., “Positioning and Presenting Design Science Research for Maximum Impact”, *MIS quarterly*, vol. 37, no. 2, 2013, pp. 337-55.
- [12] Schaub F, Balebako R, Durity AL, Cranor LF., “A Design Space for Effective Privacy Notices”, In *Eleventh Symposium On Usable Privacy and Security, SOUPS*, 2015 pp. 1-17.

- [13] Balebako R., “Mitigating the Risks of Smartphone Data Sharing: Identifying Opportunities and Evaluating Notice” 2014.
- [14] Egelman S, Tsai J, Cranor LF, Acquisti A., “Timing is everything? : the effects of timing and placement of online privacy indicators”, In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2009 pp. 319-328.
- [15] Good NS, Grossklags J, “Mulligan DK, Konstan JA, Noticing notice: a large-scale experiment on the timing of software license agreements”, In Proceedings of the SIGCHI conference on Human factors in computing systems. ACM. 2007, pp. 607-616.
- [16] Kay M, Terry M., “Textured agreements: re-envisioning electronic consent” In Proceedings of the Sixth Symposium on Usable Privacy and Security, ACM, 2010, pp. 13.
- [17] Cranor L, Langheinrich M, Marchiori M, Presler-Marshall M, Reagle J., “The platform for privacy preferences 1.0 (P3P1. 0) specification”, W3C recommendation, 2002, pp. 16.
- [18] Langheinrich M., “A privacy awareness system for ubiquitous computing environments” In UbiComp 2002: Ubiquitous Computing, Springer Berlin Heidelberg, 2002, pp. 237-245.
- [19] Ardagna CA, Bussard L, Di SD, Neven G, Paraboschi S, Pedrini E, Preiss S, Raggett D, Samarati P, Trabelsi S, Verdicchio M. Primelife policy language. 2011.
- [20] Ermakova T, Baumann A, Fabian B, Krasnova H., “Privacy Policies and Users’ Trust: Does Readability Matter?”, 2014.
- [21] The Center for Information Policy Leadership, H. W. L. “Multi-layered notices”.
- [22] McDonald AM, Reeder RW, Kelley PG, Cranor LF., “A comparative study of online privacy policies and formats” In Privacy enhancing technologies Springer Berlin, Heidelberg, 2009, pp. 37-55.
- [23] Passera S., “Beyond the Wall of Text: How Information Design Can Make Contracts User-Friendly”, “In Design, User Experience, and Usability: Users and Interactions” Springer International Publishing, 2015, pp. 341-352.
- [24] Plass JL, Moreno R, Brünken R. Cognitive load theory. Cambridge University Press; 2010.
- [25] Kay M, Terry M., “Textured agreements: re-envisioning electronic consent” In Proceedings of the Sixth Symposium on Usable Privacy and Security, ACM, 2010, p. 13.
- [26] Kelley PG, Bresee J, Cranor LF, Reeder RW., “A nutrition label for privacy”, In Proceedings of the 5th Symposium on Usable Privacy and Security, ACM, 2009, pp. 4.

- [27] Holtz LE, Zwingelberg H, Hansen M., “Privacy policy icons” In *Privacy and Identity Management for Life*, Springer Berlin Heidelberg, 2011, pp. 279-285.
- [28] Bravo-Lillo C, Komanduri S, Cranor LF, Reeder RW, Sleeper M, Downs J, Schechter S., “Your attention please: designing security-decision UIs to make genuine risks harder to ignore”, In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, 2013, p. 6.
- [29] Brustoloni JC, Villamarín-Salomón R., “Improving security decisions with polymorphic and audited dialogs” In *Proceedings of the 3rd symposium on Usable privacy and security*, ACM, 2007, pp. 76-85.
- [30] Patrick AS, Kenny S., “From privacy legislation to interface design: Implementing information privacy in human-computer interactions” In *Privacy Enhancing Technologies* Springer Berlin Heidelberg. 2003, pp. 107-124.
- [31] Levy SE, Gutwin C., “Improving understanding of website privacy policies with fine-grained policy anchors” In *Proceedings of the 14th international conference on World Wide Web*, ACM, 2005, pp. 480-488.
- [32] Bagozzi RP, Yi Y, Phillips LW., “Assessing construct validity in organizational research”, *Administrative science quarterly*, 1991, pp. 421-58.
- [33] von Alan RH, March ST, Park J, Ram S., “Design science in information systems research”, *MIS quarterly*, vol. 28, no. 1, 2004, pp 75-105.
- [34] Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S., “A design science research methodology for information systems research” *Journal of management information systems*, vol. 24, no. 3, 2007, pp. 45-77.
- [35] Sonnenberg C, vom Brocke J., “Evaluation patterns for design science research artefacts”, In *Practical Aspects of Design Science*, Springer Berlin Heidelberg. 2011, pp. 71-83.
- [36] Rayner K, Li X, Williams CC, Cave KR, Well AD., “Eye movements during information processing tasks: Individual differences and cultural effects”, *Vision research*, vol. 47, no. 21, 2007, pp. 2714-26.
- [37] Starr MS, Rayner K., “Eye movements during reading: Some current controversies” *Trends in Cognitive Sciences*, vol. 5, no. 4, 2001, pp. 156-63.

- [38] Rayner K., “Eye movements and attention in reading, scene perception, and visual search”, *The quarterly journal of experimental psychology*, vol. 62, no. 8, 2009, pp. 1457-506.
- [39] Morrison RE, Rayner K., “Saccade size in reading depends upon character spaces and not visual angle”, *Attention, Perception, & Psychophysics*, vol. 30, no. 4, 1981, pp. 395-6.
- [40] *Journal of the Society of Motion Picture Engineers, High Speed Photography*, 1949.
- [41] Biedert R, Hees J, Dengel A, Buscher G., “A robust realtime reading-skimming classifier”, In *Proceedings of the Symposium on Eye Tracking Research and Applications*, ACM, 2012, pp. 123-130.
- [42] Goldberg JH, Kotval XP., “Computer interface evaluation using eye movements: methods and constructs”, *International Journal of Industrial Ergonomics*. 1999, vol. 24, no. 6, pp. 631-45.
- [43] Oxford Dictionaries (2016, February 4). "cognition - definition of cognition in English from the Oxford dictionary"[Online]. Available: www.oxforddictionaries.com.
- [44] Goodman KS., “Reading: A psycholinguistic guessing game”, *Literacy Research and Instruction*, vol. 6, no. 4, 1967, pp. 126-35.
- [45] Buscher G, Dengel A, van Elst L., “Eye movements as implicit relevance feedback”, In *CHI'08 extended abstracts on Human factors in computing systems*, ACM, 2008, pp. 2991-2996.
- [46] Clifton C, Staub A, Rayner K., “Eye movements in reading words and sentences”, *Eye movements: A window on mind and brain*, 2007, vol. 27, pp. 341-72.
- [47] Rayner K., “Eye guidance in reading: Fixation locations within words”, *Perception*, vol. 8, no. 1, 1979, pp. 21-30.
- [48] Apple.com (2016, June 23), “iPad Pro Specification” [Online], Available: <http://www.apple.com/ipad-pro/specs/>, 2015.
- [49] GSMarena (2016, June 23), “Samsung Galaxy S7 Specification” [Online], Available: http://www.gsmarena.com/samsung_galaxy_s7-7821.php.
- [50] Brandimarte L, Acquisti A, Loewenstein G., “Misplaced confidences privacy and the control paradox”, *Social Psychological and Personality Science*, vol. 4, no. 3, 2013, pp. 340-7.

- [51] Fischer-Hübner S, Pettersson JS, Bergmann M, Hansen M, Pearson S, Mont MC., “HCI Designs for Privacy-Enhancing Identity Management”, *Digital Privacy: Theory, Technologies, and Practices*, 2007, pp. 229-52.
- [52] Hyrskykari A, Majaranta P, Aaltonen A, Rähä KJ., “Design issues of iDICT: a gaze-assisted translation aid”, In *Proceedings of the 2000 symposium on Eye tracking research & applications*”, ACM, 2000, pp. 9-14.
- [53] Campbell CS, Maglio PP., “A robust algorithm for reading detection”, In *Proceedings of the 2001 workshop on Perceptive user interfaces*, ACM, 2001, pp. 1-7.
- [54] Just MA, Carpenter PA., “A theory of reading: from eye fixations to comprehension”, *Psychological review*, vol. 87, no. 4, 1980, pp. 329.
- [55] Microsoft (2016, June 23). Cognitive services [Online]. Available: <https://www.microsoft.com/cognitive-services/en-us/apis> .
- [56] March ST, Smith GF. “Design and natural science research on information technology”, *Decision support systems*, vol. 15, no. 4, 1995, pp. 251-66.
- [57] Earp, Julia B., et al., "Examining Internet privacy policies within the context of user privacy values", *Engineering Management, IEEE, Transactions on*. 52.2, 2005, pp. 227-237.
- [58] Hochhauser, Mark., "Lost in the fine print: Readability of financial privacy notices", *Privacy Rights Clearinghouse*, 2001.
- [59] Gross, Ralph, and Alessandro Acquisti., "Information revelation and privacy in online social networks", *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, ACM, 2005.
- [60] Mohd Saad N, Alias RA., “New types of general consent in telehealth application usage”, In *Biomedical Engineering and Sciences (IECBES)*, 2012 IEEE EMBS Conference, IEEE, 2012, pp. 354-358.
- [61] Bonnici CJ., “An extended conceptual model of consent for information systems”, In *Computer-Based Medical Systems (CBMS)*, 2013 IEEE 26th International Symposium, IEEE, 2013, pp. 149-154.