UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PRIVACY AGENTS IN THE IOT: CONSIDERATIONS ON HOW TO BALANCE AGENT AUTONOMY AND USER CONTROL IN PRIVACY DECISIONS

JESSICA HELENA COLNAGO

ORIENTADOR: PROF. DR. HÉLIO CRESTANA GUARDIA

São Carlos - SP
Junho/2016

UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PRIVACY AGENTS IN THE IOT: CONSIDERATIONS ON HOW TO BALANCE AGENT AUTONOMY AND USER CONTROL IN PRIVACY DECISIONS

JESSICA HELENA COLNAGO

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação, área de concentração: Interação Humano Computador
Orientador: Dr. Hélio Crestana Guardia

São Carlos - SP
Junho/2016

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária UFSCar
Processamento Técnico
com os dados fornecidos pelo(a) autor(a)

C717p

Colnago, Jessica Helena
Privacy agents in the IoT : considerations on how to balance agent autonomy and user control in privacy decisions / Jessica Helena Colnago. -- São Carlos : UFSCar, 2016.
200 p.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2016.

1. Privacidade. 2. Interrupções. 3. Controle. 4. Agentes inteligentes. 5. Internet das coisas. I. Título.

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia

Programa de Pós-Graduação em Ciência da Computação

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a defesa de Dissertação de Mestrado da candidata Jessica Helena Carvalho, realizada em 22/06/2016.

Prof. Dr. Hélio Crestana Guardia
(UFSCar)

Profª. Drª. Vânia Paula de Almeida Neris
(UFSCar)

Prof. Dr. Cristiano Maciel
(UFMT)

Certifico que a sessão de defesa foi realizada com a participação à distância do membro Prof. Dr. Cristiano Maciel. Depois das arguições e deliberações realizadas, o participante à distância está de acordo com o conteúdo do parecer da comissão examinadora redigido no relatório de defesa da aluna Jessica Helena Colnago.

Prof. Dr. Hélio Crestana Guardia
Coordenador da Comissão Examinadora
(UFSCar)

Dedico essa dissertação aos meus pais por sempre me apoiarem e à minha avó Yolanda, por me ensinar que o melhor marido é um diploma na parede.

I dedicate this thesis to my parents who have always been there for me and to my grandmother Yolanda, for teaching me that the best husband is a degree on the wall.

Acknowledgements

I am most grateful to the invaluable advises, comments and support that was given to me by my thesis adviser Prof. Dr. Hélio Crestana Guardia. This field was something new for both of us and he showed me the curiosity, open-mindedness and patience that I now take to be fundamental characteristics of a great researcher.

I would also like to thank Prof. Dra. Vânia Paula de Almeida Néris for all the help and advices, inside and outside the scope of this work. Thank you for helping direct the research and refine the user studies at times that an expert insight in human-computer interaction was much needed.

I would like to thank Prof. Dr. Sérgio Donizetti Zorzo for being part of my proposal committee. Your observations were much needed and appreciated.

I would also like to thank the researchers that have been a part of my growth as a master student: Dr-ing. Sebastian Feuerstack, Dr. Gregor Miller, Prof. Dr. Sidney Fels and Prof. Dra. Junia Anacleto.

As nothing that is worth having or doing comes without some pain and obstacles, I would like to take a moment to thank those who helped me through them and have not been mentioned yet: Bruno Martins, Caroline Pagel, Thaís Ussami, Victor Gabriel Lacorte, Sylvia Levington and her amazing family, Gabriele Lamarck and Danilo Gasques

Finally, I would like to acknowledge the incredible part that my parents, Maria Caterina and Geraldo Colnago, and godparents, Neucidéia and Luiz Alberto Colnago, have played in this work. If not directly by reading iand commenting on it, they helped indirectly by giving me all possible and imaginable support. I most certainly could not have done this without you.

“The presence of those seeking the truth is infinitely to be preferred to the presence of those who think they’ve found it.”

— Terry Pratchett, Monstrous Regiment

Resumo

Este trabalho investigou aspectos que podem ajudar a balancear o nível de controle de usuários e de autonomia de agentes inteligentes de privacidade no contexto da Internet das Coisas. Entende-se que esse balanceamento proposto poderia ser alcançado considerando aspectos relacionados a “querer” ser interrompido para ter controle e “poder” ser interrompido para exercer o controle. Por meio de revisão da literatura de interrupções e privacidade, variáveis relacionadas a esses dois aspectos foram identificadas, embasando a proposta de um conjunto de variáveis para “Interrupções de Privacidade Inteligentes”. Para verificar e validar esse conjunto de variáveis, duas ações de pesquisa foram feitas. A primeira foi um questionário online que serviu como uma verificação inicial de que as variáveis são adequadas ao novo contexto proposto por esse trabalho. A segunda foi um estudo de amostragem de experiência com 21 usuários para se entender melhor como essas variáveis podem vir a informar o comportamento de usuários. Os resultados obtidos sugerem que as variáveis selecionadas apresentam relevância e que podem ser usadas para informar o desenvolvimento e design de agentes de privacidade. Embora os resultados ainda sejam limitados, principalmente pela duração do estudo e grupo e número de usuários, através da análise quantitativa dos dados coletadas no estudo com usuários e da análise qualitativa das entrevistas realizadas pós-estudo notou-se um processo mental comum entre os usuários participantes do estudo para as tomadas de decisão de reter o controle ou delegá-lo ao agente. Estudos futuros devem ser realizados, procurando verificar a possibilidade de expandir o relacionamento das variáveis para a criação de um modelo de comportamento e preferência dos usuários que seja integrável ao sistema de decisão de agentes inteligentes de privacidade.

Palavras-chave: privacidade, interrupções, controle, agentes inteligentes, internet das coisas, privacidade usável.

Abstract

This thesis explored aspects that can help balance the level of user control and system autonomy for intelligent privacy agents in the context of the Internet of Things. This proposed balance could be reached considering aspects related to wanting to be interrupted to have control and being able to be interrupted to exert this control. Through literature review of interruption and privacy literature, variables related to these two perspectives were identified. This led to the variable set “Intelligent Privacy Interruptions”. To verify and validate this set, two research actions were performed. The first one was an online survey that allowed us to perform a sanity check that these variables were acceptable in this work’s context. The second was an experience sampling user study with 21 participants that allowed us to better understand how user behavior is informed by these variables. Based on these two interventions it was possible to note that the selected variables seem to show relevance and that they can be used to inform the development and design of privacy agents. The limitations of the partial results notwithstanding, through a quantitative analysis of data collected form the user study and the qualitative analysis of the exit interviews, it was possible to note a common mental process between the participants of the user study when deciding whether to withhold or delegate decision control to the agent. Future studies should be performed to verify the possibility of expansion and creation of a behavior and preference model that can be integrated to the decision-making system of intelligent privacy agents.

Keywords: privacy, interruptions, control, intelligent agents, internet of things, usable privacy.

List of Figures

Figure 1. Context in which our research is developed. Our contribution is found in the intersection (in black) 21
Figure 2. Table of the evolution of privacy definitions extracted from (CHAN; HARMON; DEMIRKAN, 2012) 25
Figure 3. Illustration of Solove's privacy activities taxonomy in relation to a possible data flow and the FIPPs (GELLMAN, 2014) 26
Figure 4. Notice and consent three-dimensional space based on the framework for Attentive Notification Systems (MCCRICKARD; CHEWAR, 2003) 27
Figure 5. Four main areas to be considered for privacy protection (ITU, 2005) 34
Figure 6. Flemisch et al. (2012) representation of the interconnections of ability, authority, responsibility and control. 37
Figure 7. Description of the control continuum based on the notice plane previously described. 44
Figure 8. Classification of the Privacy Solutions presented by grouping and presence or not of intelligence either on the setup of preferences or during sharing stages. 54
Figure 9. Intelligent Privacy Interruptions 66
Figure 10. Activity Engagement representation considering the combination of the two variables that compose it: social engagement and workload. 69
Figure 11. On the left: an iOS 6 permission request notification. On the right: Android 6.0 permission request notification. Both identify: (a) the app requesting information (who); (b) what data they need access to (what); and, (c) why they need access to it (why)..... 75
Figure 12. Distribution of the overall trust scores considering eq. I. The highlighted bar has equal values for agreeing with trust-adding sentences and trust-subtracting sentences. Showing a neutral level of trust. 86
Figure 13. Heat map of the agreement with the interruption-related sentences. The darker the color the higher was the number of participants with that combination (MAX: 38, MIN: 0) 87
Figure 14. Average scores and standard deviations for individual desirability for control measures 89
Figure 15. Distribution of the scores for desirability for control 90
Figure 16. Comparison of computer literacy and number of privacy behaviors reported. 94
Figure 17. Graph showing the proportion of the number of privacy behaviors per group as defined by Westin's Privacy Segmentation Index. 95
Figure 18. User study interruption frequency distribution 103
Figure 19. Depiction of the workflow and screens (in Portuguese) with which the participant would interact. 107
Figure 20. Distribution of the overall trust scores for the user study compared to the overall trust scores obtained from the online survey. The highlighted bar indicates the neutral score. 110
Figure 21. Heat map of the agreement with the interruption-related sentences. The darker the color the higher was the number of participants with that combination (MAX: 5, MIN: 0) 111

Figure 22. Average scores and standard deviations for individual desirability for control measures 114
Figure 23. Distribution of the scores for desirability for control. Presented as percentages to allow side-by-side comparison. 114
Figure 24. Distribution of behavior per participant considering the 4 possible situations: delegate the choice directly (Delegated), see the scenario and decide to choose (Seen & Chosen), see the scenario and decide to delegate the choice to the agent (Seen & Delegated), and missed interruptions (Missed). 116
Figure 25. Distribution of the immediately delegated interruptions by study days (left) and study hours (right) 119
Figure 26. Number of changes in the control and sensitivity reported by each participant. 128
Figure 27. Mental process extracted from the interview..... 143

List of Tables

Table 1. Comparison between the pros and cons of automated and orchestrated solutions from the Internet of Things perspective and the user perspective. 50

Table 3. Demographic values from participants who answered the online survey 84

Table 4. Distribution of agreement with each of the four trust-related statements 85

Table 5. Distribution of agreement with each of the two interruption-related statements 86

Table 6. Engagement distribution between the five listed privacy protective behaviors. The behaviors are divided as passive and active behaviors. 88

Table 7. Proportion of previously enacted privacy protective behaviors grouped as passive behaviors, active behaviors, and total amount of behaviors. 88

Table 8. Privacy concern comparative table between this work and the results reported in (KUMARAGURU; CRANOR, 2005) 89

Table 9. Values for each variable (Activity Engagement was divided in Social Engagement and Workload). Variables in grey represent the ones related to the question “Can I be interrupted” (interruptibility variables). Variables in white represent the ones related to the question “Do I want to be interrupted” (receptivity variables). 91

Table 10. Distribution of participants for group IV and group V considering the difference in the amount of variables marked as relevant. 92

Table 11. Table comparing the privacy concern characterization obtained from PSI with the classification of computer literacy. 93

Table 12. Contingency table for PSI categories and different types of privacy behaviors 95

Table 13. Demographic values from participants of the user study in comparison with the values obtained from participants of the online survey (OS). 108

Table 14. Distribution of agreement with each of the four trust-related statements .. 109

Table 15. Distribution of agreement with each of the two interruption-related statements 111

Table 16. Engagement distribution between the listed privacy protective behaviors. The behaviors are divided as passive and active behaviors. 112

Table 17. Proportion of previously enacted privacy protective behaviors grouped as passive behaviors, active behaviors, and total amount of behaviors. 112

Table 18. Privacy concern comparative table between this work and the results reported in (KUMARAGURU; CRANOR, 2005) 113

Table 19. Shapiro-Wilk Normality Test (H_0: Data is normally distributed) and Levene’s Test for Homogeneity of Variance (H_0: Data is homogeneous) 117

Table 20. F-test values using ANOVA for gender, age group, computer literacy and privacy concern (with Welsh correction) 117

Table 21. Frequency of selection for each variable considering their associated statements when the participant selected to delegate directly. 118

Table 22. Distribution of explanation of why it was decided to delegate directly over the course of the user study 119

Table 23. Distribution of scenarios and certainty characteristics on the interruptions seen by the participants 120

Table 24. Distribution of pre-established and perceived frequency levels for the interruptions seen by the participants 121

Table 25. Comparison of effect of the variables Perceived Frequency (PF), Certainty (Ce) and Sensitivity (S) together on the decision to Choose (C) or to Delegate (D) . 122

Table 26. Comparison of effect of the variables Frequency (F), Certainty (Ce) and Sensitivity (S) together on the decision to Choose (C) or to Delegate (D) 122

Table 27. Coefficients for logistic regression with the decision made as dependent variable and perceived frequency, sensitivity and certainty as independent variables. Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1 123

Table 28. Self-report of motivators for the decision to choose or delegate 124

Table 29. Coefficients for logistic regression with the decision made as dependent variable and the selection for what, why, who and certainty as independent variables. Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1 124

Table 30. Characterization of context for all seen interruptions, interruptions that were seen followed by a decision to choose themselves, and interruptions that were seen followed by a decision to delegate it to the agent. 125

Table 31. Coefficients for logistic regression with the decision made as dependent variable and the selection for mood, workload, social engagement and social expectation as independent variables. Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1 125

Table 32. Reported influence of the different aspects considered on the exit questionnaire in comparison to the results obtained on the online survey. Some aspects were represented with a finer-grained that do not have corresponding values on the online survey. 126

Table 33. Minimum, average, standard deviation, and maximum values of changes in the sensitivity and control preference reported for the scenarios at the beginning and at the end of the study. 127

Table 34. User responses to the exit questionnaire about the used definitions of low, medium and high frequency interruptions 129

Table 35. User responses to the exit questionnaire over the user study format and agent behavior 129

Table 36. Classification of the different references for aspects that influence privacy sensitivity considering the 5W1H framework and subcategories. 175

Acronyms

ACM *Association for Computing Machinery*

APPEL *A P3P Preference Exchange Language*

EPAL *Enterprise Privacy Authorization Language*

ESM *Experience Sampling Method*

FIPPs *Fair Information Privacy Practices*

FTC *Federal Trade Commission*

IEEE *Institute of Electrics and Electronics Engineers*

IoT *Internet of Things*

IPv4 *Internet Protocol version 4*

ISO *International Organization for Standardization*

P3P *Platform for Privacy Preferences*

PbD *Privacy by Design*

PET *Privacy Enhancing Technology*

PSI *Privacy Segmentation Index*

SOC *Service Oriented Computing*

SOUPS *Symposium on Usable Privacy and Security*

W3C *World Wide Web Consortium*

XACML *eXtensible Access Control Markup Language*

Contents

Introduction 17
1.1 Objectives 20
1.2 Research Area and Audience 20
1.3 Contributions and Limitations 21
1.4 Structure 22
Conceptual Basis 24
2.1 Privacy 24
2.1.1 Privacy Approaches 26
2.1.2 Privacy Obstacles and Biases 31
2.2 Control 35
2.2.1 User Control in Automated Systems: A Balancing Act 36
2.3 Interruptions 38
2.3.1 Receptivity and Interruptibility 39
2.3.2 Dealing with Interruptions 40
2.4 Summary 41
Related Work 43
3.1 Privacy Solutions on a Control Continuum 43
3.1.1 Automated Solutions 44
3.1.2 Orchestrated Solutions 47
3.1.3 Choreographed Solutions 49
3.2 Approaches to Balancing Autonomy and Control 54
3.3 Managing Interruptions 58
3.4 Summary 61
Intelligent Privacy Interruptions 62
4.1 Basic Characteristics 63
4.2 Variables 65
4.2.1 Can I Be Interrupted? 67
4.2.2 Do I Want to Be Interrupted? 70
4.2.3 Variables not Selected 75
4.3 Summary 77
Online Survey 78
5.1 Objectives 78
5.2 Survey Design 79
5.2.1 Demographics 79
5.2.2 Personal Characteristics 80

5.2.3 Internet of Things Characterization and Preferences 83
5.3 Data Collection 83
5.4 Results and Analysis 84
5.4.1 Demographics 84
5.4.2 Personal Characteristics 85
5.4.3 Preferences 90
5.4.4 Secondary Findings 92
5.5 Discussion 96
5.6 Conclusion 99
User Study and Interviews 101
6.1 Objectives 101
6.2 User Study Design 102
6.2.1 Initial Stage: Questionnaire and Scenarios 104
6.2.2 Main Stage: ESM 104
6.2.3 Final Stage: Questionnaire and Scenarios 106
6.3 Results 107
6.3.1 Demographics 107
6.3.2 Personal Characteristics 109
6.3.3 Variable Analysis 114
6.3.4 Scenario and Preference Classification 127
6.3.5 Exit Questionnaire 128
6.4 Interview Results and Discussion 130
6.4.1 Threats to Validity 131
6.4.2 Mental Process for Delegating or Choosing 139
6.4.3 Agent Design Recommendations 141
6.5 Discussion 147
6.6 Limitations 152
6.7 Conclusion 154
Conclusion and Future Work 155
Bibliography 159
Appendixes 173
Variables that Influence Sharing Sensitivity 174
Online Survey 178
Informed Consent Form 188
User Study Application Screenshots 190
Scenarios 194
Brazilian Privacy-related Laws 196

Chapter 1

Introduction

> "When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole." NIKOLA TESLA, 1926 COLLIERS INTERVIEW

Since Mark Weiser's vision of Ubiquitous Computing, in which computers would effectually vanish in the background (WEISER, 1991), the field of Computer Science developed many technologies that allow this to come true.

With the continuous decrease in size and cost, and the concomitant increase in computer power in recent years, many everyday appliances are now embedded with computational abilities beyond those initially assumed. This creates the possibility of having networked and more interactive everyday appliances, such as cars, lights, thermostats and even bathrooms[1] and water bottles[2]. These appliances and devices are connected to the internet or to a user smart device. This phenomena is what is being referred to as the Internet of Things (IoT) (CALO, 2013).

Kevin Ashton believes that he first used "Internet of Things" in a presentation for Proctor & Gamble in 1999[3]. He used it to explain the concept of 'things' collecting and using data gathered without human interference. Six years later, in 2005, the International Telecommunication Union (ITU) released their Executive Summary on the topic (ITU, 2005) discussing the concept, technology involved, challenges, amongst other things. In 2011 CISCO estimated that the actual Internet of Things was born around 2008 and 2009, when the number of connected devices surpassed the number of people in the world (EVANS, 2011).

---

1 Yaniv J Turgeman, Eric Alm and Carlo Ratti. 2014. Smart toilets and sewer sensors are coming. Wired – Technology. Accessed on March 4th, 2016. http://www.wired.co.uk/ magazine/archive/2014/03/ideas-bank/yaniv-j-turgeman

2 Jac Saltzgiver and Davis Saltzgiver. Trago – The World's First Smart Water Bottle. *Kickstarter*. Accessed on March 4th, 2016. https://www.kickstarter.com/projects/905031711/ trago-the-worlds-first-smart-water-bottle/description

3 That "Internet of Things" Thing. 2009. RFID Journal. Accessed July, 2015. www.rfidjournal.com/articles/view?4986

Since the Internet of Things has no definite and overall accepted definition (FTC STAFF REPORT, 2015) and the task of generating one is non-trivial (VERMESAN et al., 2013), we will consider the description provided in (VERMESAN et al., 2013) that states:

> *"Internet of Things is a concept and a paradigm that considers* ***pervasive presence*** *in the environment of a variety* ***of things/objects*** *that through wireless and wired connections and unique addressing schemes are able to (automatically)* ***interact*** *with each other* ***and cooperate*** *with other things/objects to* ***create new applications/services and reach common goals****"*[4]

Many of the "things" do not have standard user interfaces for user to interact with, connect and use their services in the same way as with a computer or a smartphone. Furthermore, they have an inherently distributed architecture. For these reasons, a different approach to create this interconnection of "things" must be used. Such an approach can be designed considering service orientation.

Similarly to the IoT vision, service orientation promise dynamic and low-effort composition of individual services independent of organization and computing platforms to create dynamic processes and applications (PAPAZOGLOU et al., 2008) and reflects the trend of device heterogeneity and autonomy (HUHNS; SINGH, 2005)**.** In an ideal service-oriented system, the different nodes would automatically detect each other, identify if the services provided are what it is desired, exchange whatever data is necessary and only concern the end user with the results of this exchange.

This shows that reducing the number of user interactions is not desired only by the pervasive computing nature of the Internet of Things (HARDIAN; INDULSKA; HENRICKSEN, 2006), but also by one of its enabling technologies, service orientation (PAPAZOGLOU et al., 2008).

While this may be ideal from a computational and IoT perspective it raises concerns over privacy awareness and control. Imagine an ever-nearer future in which there are hundreds of nodes providing and collecting information in your city or even your home. If the user should interfere as little as possible in this node pairing and data exchange, how will

[4] Our highlights and parenthesis.

the user know what it is being shared, with whom, when, where and why? How will this user have control to decide upon these variables? On the other hand, if traditional privacy protection approaches are used, such as notice and consent, how will the computer vanish in the background if it constantly needs to notify the users of what it needs to provide them with the desired services?

It could be argued that the Internet of Things is still under development and concerns on more technological aspects, such as data storage, network or power consumption, still need resolving for it to become truly viable. However, privacy is a complex issue that needs to tackled from the start to (try to) be mitigated.

Privacy researchers have already started studying how to mitigate the inherent privacy issues of the Internet of Things. Their main goal is to aid users in keeping their privacy at a desired and appropriate level. Some traditional solutions are based on an initial definition of preferences and profiles, removing the necessity to interrupt and request consent from the user all together. These automated solutions, while good for the overwhelming number of devices expected to be present in the IoT, may end up alienating and stressing the user (HARDIAN; INDULSKA; HENRICKSEN, 2006; HEIJDEN, 2003) and not accounting for the dynamic nature of privacy (MILBERG et al., 1995; TURNER; ALLEN; WHITAKER, 2015). On the other hand, there are solutions that focus on making the user aware and informed before answering every data request. These solutions, here called orchestrated and mostly based on the concept of notice and consent, fall prey to the lack of scalability of human attention and inability to process information (ACQUISTI, 2013).

To serve these conflicting issues, different privacy solutions have been proposed. They are an evolution of automated solutions capable of learning and adapting to user preferences. These solutions act on the users' behalf as an agent, making the best guess possible of what they will decide. Because these agents are constantly learning, they also rely on continuous (though diminishing) user input. This adds the users to the decision loop, allowing them to become aware of what is happening. As a result, these privacy solutions can be thought of as choreographed, since the intelligent agent and the user have to act together, relying on each other in order to properly perform and achieve their goals (PELTZ, 2003).

Considering the use of privacy agents and thinking of the envisioned large number of interactions between users and things in the future IoT scenarios, user satisfaction should be taken into consideration. It dictates technology acceptance and adoption, needing to be

explored and accounted for if privacy agents are to be usable[5] and adopted. In this sense, this work extracts its motivation from the fact that even though developing privacy solutions have highly focused on enhancing their ability to efficiently and effectively make decisions for the users, there has been a lower priority to aspects that can influence user satisfaction.

1.1 Objectives

From a commonsense perspective, for a system to achieve user satisfaction the user must be pleased with the interaction taking place. In interaction and interface design an important principle to be followed is that the user should be able to understand and feel in control of the interaction (NIELSEN, 1995). Similarly, privacy research shows that consent without awareness is not valid and that it is important for people to be comfortable with the decision made.

Since it is not feasible for the user be in control of every decision, this work main objective is on identifying the dynamics of decision control between the privacy agent and user, balancing awareness and interruptions. This main objective can be divided in:

- Identifying relevant variables that can dictate when the user would want to have control and when the user would want to be left alone (Chapter 4);
- Identifying if these variables can be generally applied or if it is necessary to personalize their effects and applicability to different users (Chapter 5 and Chapter 6); and,
- Identifying how these variables should be applied (starting point in Chapter 6).

1.2 Research Area and Audience

This research is, first and foremost, inserted in the context of Computer Science. The perspective of Human-Computer Interaction is from where the knowledge of design issues and interaction necessities are drawn.

[5] ISO 9241. Usability definition. *W3C*. Accessed on March 4th, 2016. https://www.w3.org/2002/Talks/0104-usabilityprocess /slide3-0.html

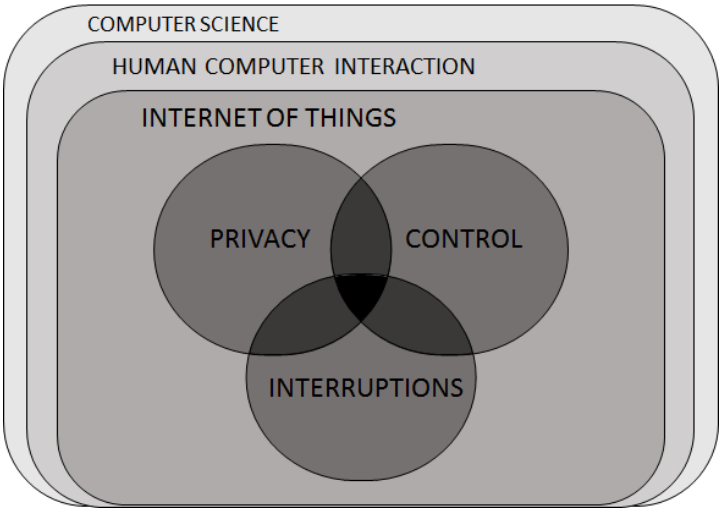


Figure 1. Context in which our research is developed. Our contribution is found in the intersection (in black)

Moving on to more application-oriented areas of this work, the focus is on the currently well-discussed topic of Internet of Things - based on Service-oriented Computing implementation. Within this perspective, where frequent data sharing is not only desired but necessary to sustain the vision, the focus is on exploring issues from privacy, control and automation, and interruptions research (visually represented in Figure 1) to help develop more usable privacy solutions.

The work proposed in this thesis is oriented to developers of intelligent privacy agents for the Internet of Things context. However, results from this thesis, such as the Intelligent Privacy Interruptions variables, could be used to guide developers that need to balance autonomy and user control over data privacy in other interruption intensive contexts.

1.3 Contributions and Limitations

The main contribution is the discussion of how to balance user control and system autonomy when considering an intelligent privacy agent in the Internet of Things. This thesis contributes with:

- The organization of literature extracted variables as presented by the Intelligent Privacy Interruptions (COLNAGO; GUARDIA, 2016);
- User classification as delegators, watchers or choosers given their most predominant behavior towards privacy interruptions;
- Insights as to possible improvements and refinements to the Intelligent Privacy Interruptions variable set;

- Mental process identification used by the participants of the user study to inform their behavior towards privacy interruptions, and its possible mutability;
- The identification of possible relationships between variables from the Intelligent Privacy Interruptions and actual behavior towards privacy interruptions; and,
- Some design recommendations for such privacy agents.

However, it is important to notice that this work suffers from some inherent limitations and some of the contributions suffers from limitations from the user study design. Nevertheless, it serves as a stepping stone towards better understanding how to balance awareness and interruptions in the context of privacy in the IoT. The results of this work are limited given that:

- The Internet of Things is not fully part of our reality;
- Prediction of behavior and preferences are inherently limited, especially for non-quotidian situations;
- The user study had a duration of only 10 days and 21 participants;
- The participants of the user study were very homogeneous and did not match the (already limited) baseline values from previous our study;
- There were different interpretations amongst participants of a few aspects of the user study;
- Some variables were considered more static by the research group than they proved to be.

1.4 Structure

This work is structured as follows:

- Chapter 2 presents the conceptual basis necessary to develop a knowledge base given the three distinct areas of research that are taken into consideration in this work. These areas are privacy, control, and interruption.
- Chapter 3 presents related work. To the best of our knowledge there was no previous work that approached the issue of balancing user control and system autonomy in the context of privacy agents for the Internet of Things. For this reason, this chapter presents a review of privacy solutions for the Internet of Things and Ubiquitous Computing, previous work that identified approaches to balance autonomy and

control outside of this work's context, and previous work that approached the issue of managing interruptions

- Chapter 4 starts by presenting the basic characteristics that a model to inform how to balance system autonomy and user control should have. This is followed by a discussion on the most relevant variables found throughout privacy and interruption literature. These variables compose the Intelligent Privacy Interruptions.
- Chapter 5 presents the initial user intervention, an online survey, used to collect baseline information from the Brazilian population, as well as to perform an initial validation of the variables extracted from the literature when brought to the context of privacy agents in the Internet of Things.
- Chapter 6 presents the main user intervention, an ESM user study, used to more deeply validate the selected variables, as well as try to identify patterns of behavior.
- Chapter 7 presents the conclusion and future work derived from this thesis.

Lastly, this work has a series of appendixes:

- Appendix A presents a review of variables that affect sharing sensitivity, which were used to determine what would be included in the user study scenarios.
- Appendix B presents the online survey that was used in Chapter 5 (Portuguese)
- Appendix C presents the Informed Consent Form signed by all participants of the user study reported in Chapter 6 (Portuguese).
- Appendix D presents screenshots of the different interactions the participants had with the developed application for the user study (Portuguese).
- Appendix E presents the scenarios that were used in the user study (Portuguese).
- Appendix F presents a review of Brazilian laws and regulations related to privacy.

The research conducted in this thesis was approved by the Internal Review Board of the Federal University of Sao Carlos, CAAE 48966215.8.0000.5504.

Chapter 2

Conceptual Basis

This research considers multiple views in its development and, as such, requires a varied and strong conceptual basis of what are the pros, cons and challenges of each of these views. In the previous chapter a short description was presented for the two underlying technological perspectives of this work: Internet of Things and its possible implementation architecture, Service-oriented Computing. This description is now followed by a discussion of the theoretical frameworks of privacy, autonomy and control, and interruptions. These topics provide the basis and arguments for the insights presented in this work.

2.1 Privacy

The concern over privacy is ancient and in the last decades there has been a pronounced focus in producing legislation to try and protect individual's privacy. After the Second World War, the United Nations adopted the Universal Declaration of Human Rights, which was followed by the draft of the European Convention for the Protection on Humans Rights and Fundamental Freedoms in 1950. In the 1970s, there was a great effort in generating legislation that would protect privacy. Examples are the 1974 Privacy Act, which enforces fair data processing and disclosure, the Fair Information Practice Principles (FIPPs), and data protection laws in Germany[6] and Sweden (a more comprehensive discussion on the history of privacy can be found in (HOLVAST, 2009)). In Brazil, the right for privacy is declared in the constitution as, "People's intimacy, private life, honor and image are inviolable, with assured right for compensation from material or moral damage resulting from its violation."[7] Furthermore there are several laws that protect and specify privacy in Brazil for different contexts (Appendix E).

[6] In German: Bundesdatenschutzgesetz (BDSG)
[7] Original text: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; " – Art. 5, inc. X, 1988 Federal Constitution

However, there is no unique definition for privacy (see Figure 2), leading to what McCarthy stated in *The Rights of Publicity and Privacy*[8]: "'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had". These variations could be explained by the fact that privacy means a plurality of things (SOLOVE, 2008) and varies from different points in time (BELLOTTI; SELLEN, 1993; WAREN; BRANDEIS, 1890), different contexts, different cultures and different individuals (BELLOTTI; SELLEN, 1993; MILBERG et al., 1995). However, these different definitions make it difficult to uniquely address and solve privacy violations since it is not clear what constitutes one.

Concept	Year	Author	Definition
The right to be let alone	1890	Warren and Brandeis [69]	"Right to be let alone" Principle of privacy is "that of inviolate personality"
	1958	Douglas [62]	"Right of privacy includes the privilege of an individual to plan his own affairs"
Limited access to self	1880	Godkin [26]	"The right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion"
	1970	Breckenridge [14]	"The rightful claim of the individual to determine the extent to which he wishes to share of himself with others"
	1983	Bok [11]	"The condition of being protected from unwanted access by others—either physical access, personal information, or attention"
Secrecy	1981	Posner [46]	"Concealment of information"
	1992	Inness [31]	"…[To] provide the individual with control over certain aspects of her life"
	1998	Posner [45]	"Right to conceal discreditable facts about himself"
	1999	Etzioni [20]	"The realm in which an actor … can legitimately act without disclosure and accountability to others"
Control over personal information	1967	Westin [70]	"[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"
	1969	Fried [22]	"[T]he *control* we have over information about ourselves"
	1972	Miller [38]	"[T]he individual's ability to control the circulation of information relating to him"
	1995	Information Infrastructure Task Force [47]	"An individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used"
Personhood	1964	Bloustein [10]	Protects against conduct that is "demeaning to individuality," "an affront to personal dignity," or an "assault on human personality"
	1989	Rubenfeld [51]	"The fundamental freedom not to have one's life too totally determined by a progressively more normalizing state"
Intimacy	1992	Inness [31]	"The state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking"

Figure 2. Table of the evolution of privacy definitions extracted from (CHAN; HARMON; DEMIRKAN, 2012)

Furthermore, solving the issue of privacy becomes even harder since different people will deal with it in different and nuanced ways (ACKERMAN, 2004). An approach try and start dealing with privacy violations is to break them into smaller and more well defined parts. By using identified privacy concerns such as a lack of control over personal information, anxiety over data collection, unfair discrimination and manipulation of data, unauthorized access, secondary use of data, etc. (ACKERMAN, 2004; BORGESIUS, 2015) it is possible to create a foundation of regulations and methods to address the issue.

[8] J. Thomas McCarthy, "The Rights of Publicity and Privacy", 5.59 (2nd ed. 2005).

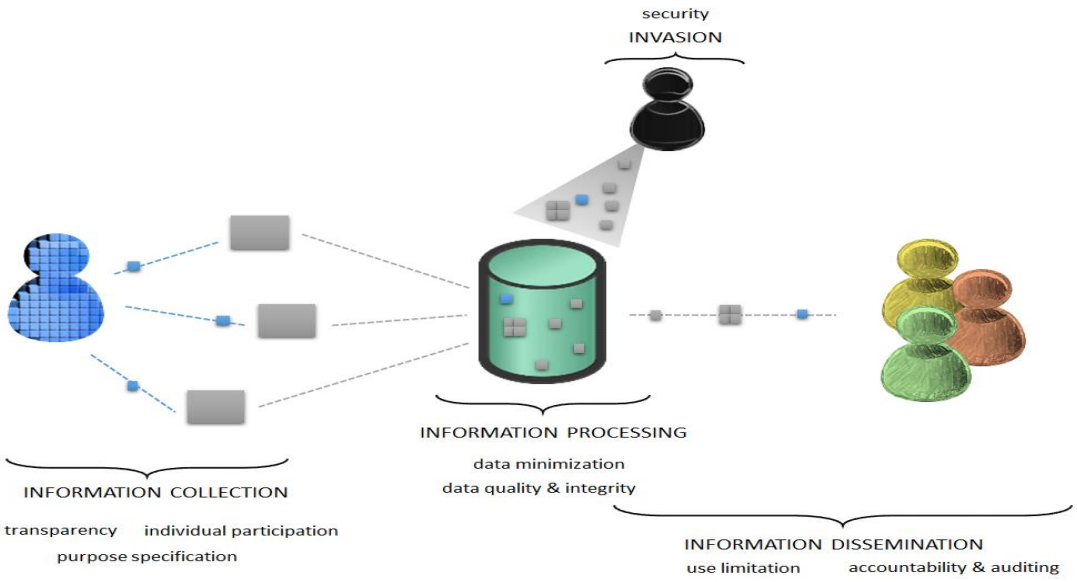


Figure 3. Illustration of Solove's privacy activities taxonomy in relation to a possible data flow and the FIPPs (GELLMAN, 2014)

In fact, in *Understanding Privacy* (SOLOVE, 2008, pg 101) a taxonomy of activities that create privacy problems was identified in order to facilitate the development of laws and regulations. The four main activities are related to: Information Collection, Information Processing, Information Dissemination and Invasion, and by mapping these activities to the Fair Information Practice Principles (FIPPs) (GELLMAN, 2014) (seen under each activity in Figure 3), it is possible to see methods to deal with each activity.

2.1.1 Privacy Approaches

As can be seen, there are many activities that will lead to a privacy breach. To simplify this discussion one can consider a privacy breach as occurring whenever the user's expectation of privacy does not match the reality of what has occurred. This simplification derives from the legal "expectation of privacy test"[9] used in the United States to decide upon matters related to the Fourth Amendment. From the technology and computer perspective, one can consider that a privacy breach occurs, for example, in an exchange of data between two parties whenever a third unannounced party eavesdrops on this transaction (invasion) or when the data is collected without both parties being informed (information collection). As such, privacy approaches derive from the attempt of bridging and enforcing the user's expectation of privacy with reality.

[9] Expectation of Privacy definition. Accessed on April 14th, 2016. www.law.cornell.edu/wex/expectation_of_privacy

2.1.1.1 Notice and Consent

From the users' side, notice and subsequent consent is a possible approach. Notice can be performed in a variety of ways varying format and moment of delivery (SCHAUB et al., 2015). However, it is important to note that for notice to be valid it needs to successfully interrupt the users, garner their attention, and inform them of details of the activity that will take place and its consequences. A successful notice must leave the users with a deeper comprehension of the reality of the situation than they initially had.

Consent follows as a direct reaction from notice and, though not what we currently experience on many of our online transactions, it should be given freely, i.e. there should not be a negative side-effect for denying consent (BORGESIUS, 2015). An example of an interesting method for delivering notice is through the use of privacy nudges (ALMUHIMEDI et al., 2015), which are behavioral interventions that support users in the process of making their privacy decision by making the risks clear and nudging the users towards a privacy setting better suited to their concerns.

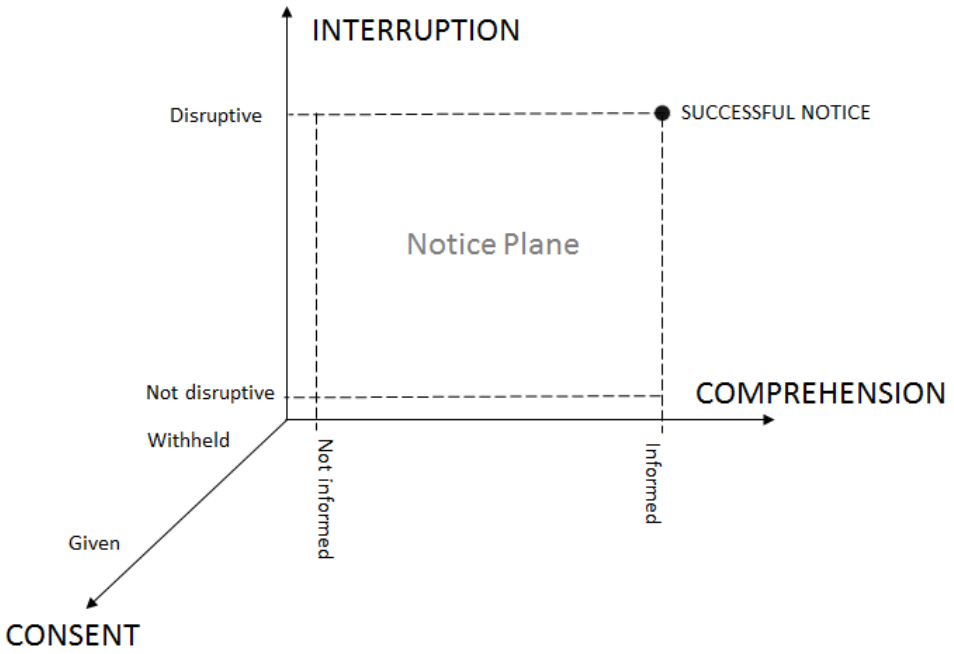


Figure 4. Notice and consent three-dimensional space based on the framework for Attentive Notification Systems (MCCRICKARD; CHEWAR, 2003)

Like the framework for Attentive Notification Systems (MCCRICKARD; CHEWAR, 2003), notice and consent can be thought as a three-dimensional space in which there are the interruption and comprehension axis that form the notice plane, and consent (instead of just reaction) is a discrete axis perpendicular to the notice plane (Figure 4). An ideal notice,

and subsequent consent action, would make the users aware of the interruption and informed over the situation they are currently in. It is worth mentioning that consent is a way through which people can actively enforce their decisions, but the real control in privacy solutions lies with who is able to make an informed decision.

2.1.1.2 Privacy Settings

An approach that offers users some preemptive control over their data flow is privacy settings. Commonly applied to social networks, these settings let users decide when, where, to whom or what they will share. Even though it seems reasonable from a human perspective and practical from a technological perspective, this requires that the users have time to configure a variety of setting, awareness of their desired level of privacy and the consequences of sharing their personal data (SADEH et al., 2009; WILSON et al., 2013).

A proposed way of working around the issue of configuring multiple settings is by using privacy profiles. These privacy profiles can either be associated with the definition of rules for specific groups and locations, or to the definition of aggregate settings that capture the preferences of a diverse group of users in distinct profiles. In the latter a user can select from a range of pre-defined profiles the one that is a best fit for him/her (WILSON et al., 2013). Either way, privacy profiles make the configuration of privacy settings a more amenable activity. Yet it has been shown that privacy protecting tools such as privacy settings may create an illusion of control and protection, making people more at risk of a privacy breach (ACQUISTI; ADJERID; BRANDIMARTE, 2013).

2.1.1.3 Privacy Policy

A privacy policy is a provider-created document that fulfills a legal requirement of informing the customer of all the ways the provider collects, uses, manages and discloses the customer's data. It is an important instrument that offers transparency and accountability and reduces the level of information asymmetry (MCDONALD; CRANOR, 2008). However, it is a static tool to inform the user; it has no means of negotiating terms or adapting to user preferences; it is famously hard to read and, consequently, never read or fully understood (BORGESIUS, 2015; LUGER; RODDEN, 2014; MCDONALD; CRANOR, 2008). Lastly, because the acceptance or not of a privacy policy terms leads to the use or not of the system, it has been argued that they do not actually offer appropriate means for consent (EVANS, 2014; LUGER; RODDEN, 2013).

Researchers have tried to tackle some of these issues such as readability and usability (ACQUISTI; ADJERID; BRANDIMARTE, 2013) and Privacy Policy Languages not only allow for machine readable policies, but also aid the negotiation and adaption of user preferences (ACKERMAN, 2004; MONIRUZZAMAN; FERDOUS; HOSSAIN, 2010). Some of these languages are:

- Platform for Privacy Preferences (P3P)[10], from the World Wide Web Consortium (W3C);
- A P3P Preference Exchange Language (APPEL)[11], P3P user-side complement;
- Enterprise Privacy Authorization Language (EPAL)[12], from IBM; and,
- eXtensible Access Control Markup Language (XACML)[13], from OASIS.

2.1.1.4 Privacy Enhancing Technologies

To encompass the variety of methods, techniques and technologies that exist to preserve and enhance privacy, the concept of Privacy Enhancing Technologies (PET) was coined. PETs include tools for encryption, anonymity, obfuscation and user control (AN; JUTLA; CERCONE, 2006; MCDONALD; CRANOR, 2008; PALLAPA; KUMAR; DAS, 2007) that do not hinder the functionality of the system (HOLVAST, 2009).

Many of the privacy middleware, architecture, frameworks and layers that exist in the literature can be considered a PET. They usually make use of one or more concepts of PETs (encryption, anonymity, obfuscation and user control) in combination with other privacy approaches (e.g. privacy policies). For example, Confab (HONG; LANDAY, 2004) is a toolkit that facilitates the development of privacy-aware ubicomp applications in which a higher degree of control and choice is given to the user since activities involving personal information are processed as much as possible in the user's device. They use a concept related to privacy policy languages called "infospaces", where different types of data are managed for each individual user.

Another example that makes use of PET concepts is SITA (ANDERSEN; KJARGAARD; GRONBAEK, 2013). Their model divides location privacy into four properties, namely spatial, identity, temporal and activity, and each property can be classified in one of 5 levels. Each level is associated with a technique to ensure privacy, for example level 0

[10] Specification available at: www.w3.org/TR/P3P/. Accessed on June, 18th, 2015
[11] Specification available at: www.w3.org/TR/P3P-preferences/. Accessed on June, 18th, 2015
[12] Specification available at: www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/. Accessed on June, 18th, 2015
[13] Specification available at: docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html. Accessed on June, 18th, 2015

means no information is shared and level 2 means obfuscation. The idea is to provide better location privacy by combining different levels and different properties, offering a finer and higher degree of control. A similar approach makes use of hierarchical masking, quantization, perturbation and randomization to obfuscate and anonymize user data (UKIL et al., 2012). A variety of examples of such systems, these three included, are further described in Privacy Solutions on a Control Continuum (pg. 43), but analyzed with a focus on user control of data sharing.

2.1.1.5 Regulation and Laws

There has been a great focus in producing legislation to try and protect individual's privacy. The Universal Declaration of Human Rights, the European Convention for the Protection on Humans Rights and Fundamental Freedoms, the 1974 Privacy Act, the Fair Information Practice Principles, data protection laws in Germany and Sweden, articles in nations constitutions such as Brazil and Switzerland are just some of the examples available. An approach that varies slightly from the concept of regulation and legislation are the online privacy seals introduced by the FTC offered by external providers TRUSTe and the Better Business Bureau (MCDONALD; CRANOR, 2008), which certify privacy policies.

Another regulatory perspective that is being discussed relates to "ephemeral data" (SHEIN, 2013) and the right to be forgotten (EUROPEAN COMISSION, 2014). The argument of ephemeral data is that in daily lives humans forget and human memory is modified during its lifetime. This provides a degree of privacy not available in technological interactions where, once data is collected, it becomes eternal. While this does offer a higher level of privacy and brings us back to an older norm of behavior in regards to privacy, as Shein (2013) points out, even in situations where data is supposed to be ephemeral, e.g. a telephone call and more currently, a Snapchat[14], there are still ways to bypass this inherent ephemerality, e.g. recording a phone call or taking a picture of a picture in Snapchat.

2.1.1.6 Design Guidelines

A normative approach to privacy that does not go as far as laws and legislation in their enforcement aspect is the use of design guidelines. The most known design guidelines in regard to privacy comes from the concept of "Privacy by Design" (PbD) (CAVOUKIAN, 2011). The PbD foundational principles are high level guidelines (e.g. "Proactive not

[14] Social media and texting app.

Reactive; Preventative not Remedial" and "Respect for User Privacy — Keep it User-Centric") that encompass both the technological side of privacy solutions and the business and physical infrastructure sides. They have been incorporated in frameworks (e.g. (MORTON; SASSE, 2012)) to help implement privacy practices in the whole process of privacy protection. Other guidelines have been proposed that focus on providing feedback and control in specific user and system behaviors (BELLOTTI; SELLEN, 1993) and on helping developers think and identify privacy risks (HONG et al., 2004).

There are many paths to dealing with privacy. They can be categorized as to how privacy is tackled, namely as confidentiality, control (access and/or content (BOYLE; GREENBERG, 2005)) and practice (GÜRSES, 2014); or as to the perspective of the solutions taken, namely computational, architectural or user interfaces perspectives (SADEH et al., 2009). Independent of these classifications, privacy solutions must consider the nuances between users and user expectations to be successful. This thesis aims at observing these nuances to help improve the design of privacy approaches for the IoT.

2.1.2 Privacy Obstacles and Biases[15]

When researching about and developing tools to protect privacy, as important as knowing current and available approaches is knowing which are the privacy obstacles and biases that exist. Privacy policies (a.k.a. "Terms and Conditions') are more often than not, hard to understand, long to read and, at times, not even promptly available (i.e. you have to follow a link to find them) (BORGESIUS, 2015; LUGER; RODDEN, 2014; MCDONALD; CRANOR, 2008). Privacy settings, another traditional approach, frequently require that the user goes the configuration part of the system and manually set or alter privacy preferences in regards to what data should be shared in individual contexts. For an average user, chances are that s/he will not go through the trouble of reading the privacy policy or setting the privacy preferences.

There are major obstacles users face when trying to maintain what they feel is an adequate privacy level. Privacy policies try to minimize the effect of one of them, *asymmetric*

[15] There are many obstacles and biases considering the privacy decision making process to be listed. In this section we will overview some of them and more information can be found, for example, in (ACQUISTI; GROSSKLAGS, 2005; LEDERER et al., 2004; PALLAPA; KUMAR; DAS, 2007)

information (ACQUISTI, 2013), by making all the information available to the user in once place. However, because of its form and length they face the obstacles of people not being able to process all that information (*bounded rationality)* (ACQUISTI, 2013) and, consequently, using *heuristics or rules of thumb* to make decisions (ACQUISTI; ADJERID; BRANDIMARTE, 2013; BORGESIUS, 2015). While these are not bad ways to make decisions, they could lead users to make choices that contradict their own interests. Another obstacle faced by privacy policies and privacy settings is that users have a *limited attention* (ACQUISTI; ADJERID; BRANDIMARTE, 2013) and that these approaches rely on the user figuring out the *trade-off between the effort of acting on security and privacy suggestions, the benefit of disclosing data and the cost associated with the potential leak of these data* (ACQUISTI, 2013).

Privacy settings can be improved by making use of privacy profiles and suggestions to remove some of the burden from the user and ameliorating the effects of limited attention, bounded rationality and figuring out privacy trade-offs. However, care must be taken when designing these suggestions and profiles because the way they are presented can lead users to make different decisions than they would normally do (*framing effect)* (ACQUISTI; ADJERID; BRANDIMARTE, 2013). Other obstacles that must be faced are that people are influenced by the *status quo bias*, i.e. the tendency to maintain default options (BORGESIUS, 2015; LEDERER et al., 2004); tend to *follow suggestions* made (JIN et al., 2013); and, can be influenced by initial privacy profile settings (WILSON et al., 2013). These obstacles can be leveraged in favor of the user. However, they can also be used, consciously or unconsciously, to mislead the user into less privacy than what is desired.

More generally speaking, approaches that rely on having the user define a priori his/her behavior towards privacy decisions, suffer from the *privacy paradox* (or Attitude/Behavior dichotomy (ACQUISTI; GROSSKLAGS, 2005)) and *hyperbolic discounting* (ACQUISTI, 2013; HUGHES-ROBERTS, 2013). They require the user to foresee an abstract situation in the future. The first refers to the mismatch between stated concern and behavior considering privacy behavior and could be linked to factors such as low level skills and lack of awareness of privacy issues. The second refers to users that may trade long term risk for short term gain (also known as, *present bias* (BORGESIUS, 2015)).

A different perspective of privacy obstacles come from when we consider the effect that a highly private life will have on an increasingly more connected society. As Langheinrich (2002) put “[u]nless we want to abandon our current social interactions completely and deal only behind digital pseudonyms in virtual reality with each other, we must realize that our

real-world presence cannot be completely hidden, nor perfectly anonymized." As such, an important obstacle to overcome is understanding the balance that should be struck between privacy and disclosure in different data hungry contexts.

Lastly, considering the perspective of giving the user more control over his/her privacy decisions some counter intuitive obstacles arise. On one hand, by giving users more choices and more control actually leads to them feeling more regret towards the decisions made (KORFF; BÖHME, 2014). On the other, the so called *control paradox* leads users who have control over the disclosure of their information (e.g. post on a Facebook page only to friends) to be less concerned about the information accessibility and possible use (e.g. being used to target products or Facebook pages) (ACQUISTI; ADJERID; BRANDIMARTE, 2013).

2.1.2.1 Privacy Obstacles in IoT

The Internet of Things suffers from trust issues. Mr. Weasley nicely expressed these issues in his phrase: "Never trust anything that can think for itself if you can't see where it keeps its brain."[16] Because in the IoT there is a large number[17] of distributed[18] data hungry devices[19] working autonomously[20], the way to deal with privacy decisions has been to do it automatically, not explicitly relying on the user. While this perspective has been argued as a positive thing for the users since it removes a burden (ELKHODR; SHAHRESTANI; CHEUNG, 2013), this perspective is influenced by the view that privacy is a constraint to IoT's requirement of offering services (UKIL et al., 2012). Moreover, because privacy is an extremely complex issue, it should not be solely treated by more machines.

There is no lack of privacy and security issues discussed in the literature which are specific to the context of IoT. Some inherent to the diametrically opposed objectives of IoT/ubiquitous computing and privacy. The first needs to gather as much information as possible in order to provide better services, but this higher knowledge increases the chances of a privacy breach (PALLAPA; KUMAR; DAS, 2007)

Some of the privacy and security issues are: collecting user consent, contextualization of risk, profiling, data ownership, data management, legislation and enforcement, heterogeneity and simplicity of devices and ability to stay up-to-date with

[16] Quote from Mr. Weasley, fictional character from the book 'Harry Potter and the Chamber of Secrets', by J.K. Rowling, referring to a smart (i.e. enchanted) diary.
[17] Hard to keep track of where your data went.
[18] No one point of accountability.
[19] High volume of data requests and necessity of data to prosper,
[20] Low level of control.

security issues and privacy norms (COPIGNEAUX, 2014; ELKHODR; SHAHRESTANI; CHEUNG, 2013; HENZE et al., 2014; O'HARA, 2014). The International Communication Union report (ITU, 2005) recognized the variety of problems to be tackled and suggested that in order to provide the necessary privacy protection, there needs to be advances and efforts from more than just a technical perspective. They present four different areas: technical, legal, socio-ethical and economic (as can be seen in Figure 5).

This work is focused on the technical area, so we concern ourselves with the technical challenges that exist. Some of these challenges are presented by Vermesan et al. (2013) and can be summarized as: there exists billions of IoT devices, which are usually resource scarce and with a great variety of interfaces and platforms amongst them that should provide solutions that must be intuitive and integrated into what we have come to expect from interactions in "the real world".

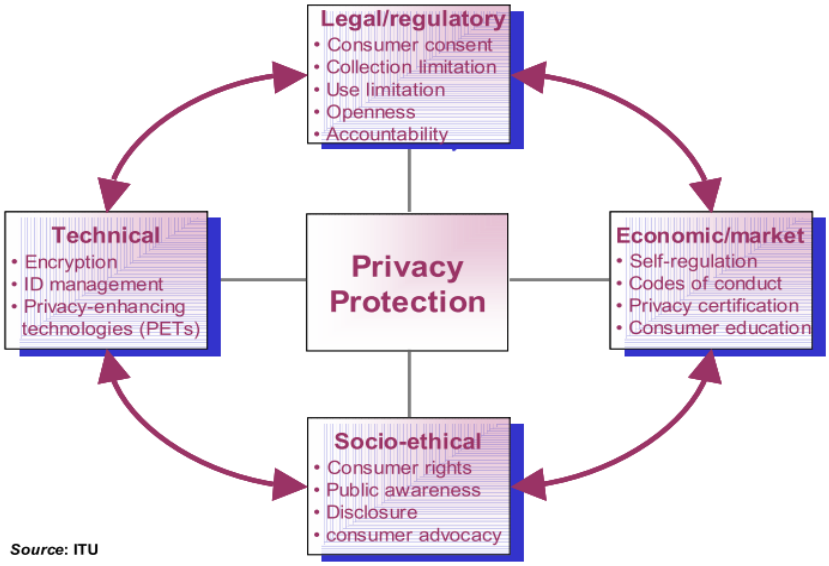


Figure 5. Four main areas to be considered for privacy protection (ITU, 2005)

Weiser and Brown (1997) stated that "[i]f computers are everywhere they better stay out of the way, and that means designing them so that the people being shared by the computers remain serene and in control." They argue that technology should be able to move from the center to periphery whenever necessary. This allows for awareness of what is happening without active participation (technology in the periphery) while exerting control when necessary or desired (technology in the center). Since in the real world we do not expect to be prompted for consent very often, but also do not expect or want to have our information shared without our consent, the IoT system should be able to move from the periphery to the center and back to match our expectations from this type of interaction.

2.2 Control

For privacy, control is a complex necessity. It considers the power to stipulate what information is shared, who it is shared with (BELLOTTI; SELLEN, 1993) and the power to ensure that the choice made will be respected (BOYLE; GREENBERG, 2005). Control has become a way to help users protect their privacies and it is necessary for users to keep their sense of privacy and identity management (TOCH, 2011). Yet too much control can be detrimental[21]. Control, as privacy, is a nuanced, individual, context dependent concept.

The Merriam-Webster dictionary defines control as “to direct the actions or function of (something): to cause (something) to act or function in a certain way.” Considering a controlled system, user control is the users’ ability to direct the behavior of a system in a preferred way (FLEMISCH et al., 2012).

Throughout human-computer interaction history, the methods and modes for users to exert control have multiplied and been perfected. Users can control computerized systems through basic command-line commands, menus, GUI widgets and physical buttons to voice, gesture and touch. However, having the means to exert control does not guarantee it. For control to be fully achieved a loop of *perception*, *action selection,* and *action* is necessary (FLEMISCH et al., 2012).

One commonly used way for the user to gain *perception* of what is happening, is to have the system offer information related to what is being done and why. Having feedback helps the user create a mental model (NORMAN, 2013, pg. 25) of the process and better understand and follow the process being done. Considering *action selection,* systems offer a variety of options. From complete control over the actions being taken to simply asking the user to correct or confirm system actions, the action selection must consider the system’s and the user’s goals and abilities, and also the limitation imposed by the current context. Finally, to provide *action*, systems may allow users to define behaviors directly through end-user programming and preference settings, for example.

In automated and intelligent systems, such as ubiquitous computing and the Internet of Things, the goal is to transfer some of the necessary intelligence to the environment and things (HEIJDEN, 2003). The tasks are usually menial and mechanical (e.g. brewing different coffees depending on how well you slept), which frees the user to focus on primary

[21] See Control Paradox in Privacy Biases and Obstacles.

and more relevant tasks. However, if the users are too far removed from the control loop, the lack of perceived control leads them to reject the system and increases user anxiety (HEIJDEN, 2003). Furthermore, by keeping the user in the loop it is possible to distribute goals, knowledge and competence, generating an effective collaboration (FALCONE; CASTELFRANCHI, 2001). In fact, one of the "ironies of automation" is that as complexity[22] increases, it becomes more crucial to have a human operator to collaborate with the system (BAINBRIDGE, 1983).

2.2.1 User Control in Automated Systems: A Balancing Act

Because of the necessity and gains of having users interacting with automated systems, user control can be thought as the user's ability to intervene when desired (HEIJDEN, 2003), as well as the necessity of such intervention for the system to properly function (HARDIAN; INDULSKA; HENRICKSEN, 2006). This makes the concept of user control become inherently tied to the autonomy level to be exerted by a system.

Defining the level of system autonomy and user control in automated systems is a non-trivial task. A previous survey on research that tackled this issue focused on context-aware systems that may need to perform this balance in real-time depending on context changes (HARDIAN; INDULSKA; HENRICKSEN, 2006). Though not directly related to privacy agents in the Internet of Things, the scope of balancing system autonomy and user control in real-time context-aware systems is a broader scope in which this work can be found. The discussed approaches to achieve this balance[23] were deemed either primitive or non-existent at the time (HARDIAN; INDULSKA; HENRICKSEN, 2006).

This balance was also discussed when considering shared and cooperative control situations with a focus on autonomous vehicles (FLEMISCH et al., 2012). While the scope is outside this work's focus on privacy in the Internet of Things, the associated risk makes it relevant. In both cases there is a heavy responsibility to avoid wrong decisions. With vehicles, the risk is more tangible: a bad decision can result in a car crash. With privacy the risk is more abstract, but can still have very real consequences, such as identity theft and fraud. Either way, the proposition that control cannot happen without ability and authority, and that exerting control is intrinsically connected to responsibility holds true (Figure 6).

---

[22] and the consequent desire for automation and reduction of 'human error'

[23] Namely ontologies, end-user programming, personalization based on preferences and a toolkit that makes it easier for designers to fine tune the behavior to context changes

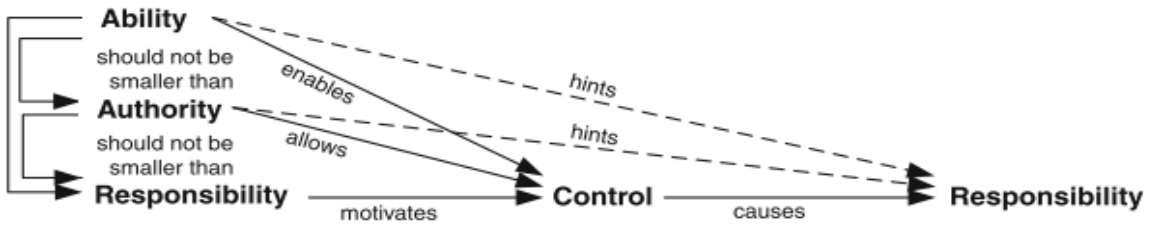


Figure 6. Flemisch et al. (2012) representation of the interconnections of ability, authority, responsibility and control.

Given the nature of the systems that need to balance system autonomy and user control, this topic has been specially explored by researchers of autonomous/unmanned vehicles and robotics. In these areas most systems focus on the performance benefits obtained from doing so (SCERRI et al., 2003; SELLNER et al., 2006) and on building architectures and approaches to deal with the behavior implication for these systems once a change in the autonomy level has happened (KORTENKAMP; KEIRN-SCHRECKENGHOST; BONASSO, 2000; PERZANOWSKI et al., 1999)

However, some interesting concepts arise depending on the approach used to balance the level of system autonomy and user control. *Mixed-initiatives systems*, as the name suggests, are those systems in which the current decision or objective can come from both the system or the user (HARDIN; GOODRICH, 2009; PERZANOWSKI et al., 1999). *Adjustable autonomy* (sometimes also called, *sliding autonomy* (SELLNER et al., 2006)) allows systems to dynamically vary the degree to which they can make decisions without human intervention depending on the current situation (KORTENKAMP; KEIRN-SCHRECKENGHOST; BONASSO, 2000; MYERS; MORLEY, 2001; PERZANOWSKI et al., 1999). A*daptive autonomy* is also a concept used when there is the possibility of balancing system autonomy and user control, but the locus of responsibility in making this decision varies. Goodrich et al. (2007) and Hardin and Goodrich (2009) consider that in adaptive autonomy the agent is given exclusive control as to deciding on this balance, and that in adjustable autonomy the supervisor retains this control.[24]

To achieve an effective balance, an autonomous system is required that can also give control to the user when performing specialized or difficult operations (KORTENKAMP; KEIRN-SCHRECKENGHOST; BONASSO, 2000). This means that a system should know when a human should perform the operation and when it can do it safely by itself. It should

[24] Even though these terms offer such nuances, they are not relevant to this work. The meta discussion of the level of control over the level of control is left unattended. As such we will continue to use the wordier version (“balancing system autonomy and user control”) unless in situations where the authors particularly used one term over the other.

also dentify when a prescribed control is no longer effective. Lastly, adjustable autonomy involves modifications considering the following aspects (KORTENKAMP; KEIRN-SCHRECKENGHOST; BONASSO, 2000):

- The complexity of the commands it executes and the constraints it enforces.
- The resources (including time) consumed by its operation.
- *The circumstances under which the system will either override or allow manual control.*
- *The circumstances under which the system will request user information or control.*
- The number of subsystems that are being controlled autonomously and how they are coupled
- *The allocation of responsibility to select, sequence, perform or terminate tasks among systems and users.*

Systems using some form of balanced system autonomy and user control have been shown to have a higher acceptance and performance. However, that makes it necessary for system designers to understand what is involved when users must be interrupted and prompted for information and actions.

2.3 Interruptions

The Merriam-Webster dictionary defines the verb *to interrupt* as (1) to stop or hinder by breaking in and (2) to break the uniformity or continuity of. Consequently, an interruption is something that comes in between and stops a primary action or situation. An interruption by itself is neither good nor bad, it merely stops the current status quo for a period. A phone call, an e-mail notification, a car crash on the street or someone calling your name are examples of interruptions we experience daily. They are considered interruptions because they break the continuity of our current state and invoke a reaction within a certain time frame (PEJOVIC; MUSOLESI, 2014). If we consider notifications alone (i.e. interruptions with content), it has been measured that we receive on a daily basis an average of 100 of them (MEHROTRA et al., 2015a).

However, not all interruptions were created equally (HO; INTILLE, 2005; MEHROTRA et al., 2015a; PEJOVIC; MUSOLESI; MEHROTRA, 2015; PIELOT; RELLO, 2015), and neither were the users receiving them (PIELOT; RELLO, 2015). Some users may feel anxious without interruptions, fearing they are missing things, while others may become more relaxed and focused. Some interruptions may just present useful information (e.g. e-

mail advertisement); others may require actions to be taken (e.g. e-mail from your boss requesting a report). Some may interrupt you for a second (e.g. car crash outside); others may interrupt you for an hour (e.g. phone call from your mother). Some may come in appropriate or desired moments (e.g. a co-worker asking if you want to take a coffee break when you have been working non-stop all day); others may be disruptive (e.g. an alarm clock going off in the middle of the night).

When one goes about designing a system that interrupts the user, it is desired that the interruptions be successful ones (i.e. garner attention) while being as good as possible (i.e. useful and appropriate). In a nutshell, interrupt but not disrupt.

2.3.1 Receptivity and Interruptibility

A way of avoiding that an interruption becomes disruptive is to guarantee that the benefits outweighs the costs of receiving it (SMITH et al., 2014). On one hand, one approach for increasing the benefit is to try and assure that the interruption will be of value, that is, the content is something relevant or interesting to the user in that moment. Previous research has shown the connection between content of an interruption and the users' classification of its disruptiveness (FISCHER et al., 2010; SMITH et al., 2014). The observation made is that when the users perceive the notification as being helpful, useful, or entertaining they have a higher *receptivity* towards the interruption. This concept focuses on identifying when the users desire an interruption to happen (FISCHER et al., 2010). On the other hand, to decrease the cost of receiving an interruption it is necessary to understand what they are.

Throughout the literature three concepts appear to be the most consistent when determining the cost of an interruption (i.e. time to resume and/or errors made on resumption of primary task): duration, complexity and moment of reception (BORST; TAATGEN; VAN RIJN, 2015; PEJOVIC; MUSOLESI; MEHROTRA, 2015). The first concept was perceived after observing that the longer a person is away from their primary activity the longer it takes and more mistakes are made when it is later restarted. The second and third concepts are also related to resumption times, more complex interruptions and interruptions in higher workload moments lead to longer resumption times (BORST; TAATGEN; VAN RIJN, 2015). As such, one should try to create short and easy interruptions, and avoid interrupting users on high workload moments.

However, workload does not cover the complexity involved when determining the best moment of interruption. An important and more complete concept associated with it is

interruptibility[25]. Previous research presented 8 definitions of interruptibility that vary from considering cost minimization (e.g. avoiding disrupting the primary task and burden of the notification) to benefit maximization (e.g. value of the notification and ability to facilitate decision making) (HO; INTILLE, 2005). Interruptibility is not related uniquely to the user's current state but to the trade-off from receiving an interruption.

Recently a literature review of interruptibility prediction in ubiquitous computing was presented that identified what it means to be interruptible (TURNER; ALLEN; WHITAKER, 2015). This can be thought from three different perspectives: physiological ability to switch focus, cognitive effect on task performance, and user sentiment towards the interruption. The latter has been considered by some a separate concept. Differently from interruptibility, which focuses on when it is best to interrupt a user to reduce the burden of the interruption, *receptivity* focuses on when the users desire an interruption (FISCHER et al., 2010).

2.3.2 Dealing with Interruptions

Approaches that help users cope with interruptions can be classified as: receiver scheduling, sender scheduling and mitigation (SMITH et al., 2014). The first is related to the concepts of interruptibility and receptivity. That is, if the moment is not favorable to the reception of that interruption, it is delayed until a better moment arises. Sender scheduling uses a similar concept as receiver scheduling, except that the point of retention is not on user device but on the device that generated the interruption. Since it involves third party knowledge of users' contextual details, it is computationally complex and privacy worrisome.

In the realm of mobile notifications a concept similar to receiver scheduling - bounded deferral - refers to when users decide to postpone a reaction to a more opportune moment (PEJOVIC; MUSOLESI; MEHROTRA, 2015). However, bounded deferral does not seem to reduce the annoyance of receiving a notification in an inappropriate time. In experience sampling method (ESM) studies receiving a notification in an inappropriate time may hinder the quality of the data collected (MEHROTRA et al., 2015b). As such, the authors go one step further and propose the use of a *current* interruptibility model and a *future* interruptibility model. This way it is possible to verify if it is indeed best to delay an interruption.

[25] An associated concept is *availability*, defined by Sarker et al. (2014) as "a state of an individual in which (s)he is capable of engaging in an incoming, unplanned activity".

Finally, mitigation is deeply related to managing the deliverance mode for an interruption. Instead of having an interruption being delayed, as per the two previous methods, in mitigation a sound notification, vibration or a blinking LED could be used to gain users' attention. This has been explored through the identification of the best mode (e.g. vibration, tone, light) and modulation (e.g. loudness) based on content importance, phone location, and user activity (LOPEZ-TOVAR; CHARALAMBOUS; DOWELL, 2015). On one hand, this approach is ideal for when an interruption cannot be delayed. On the other, it may lack the disruptiveness necessary to gain the user's attention. Nevertheless, this approach is the one most similarly to real user's behavior of setting a phone to vibrate or silence whenever they cannot or do not wish to be interrupted.

Lastly, the study of managing technology-mediated interruptions in the context of interpersonal communication (i.e. the interruption is generated by another person, not by another thing) has identified an extra approach that is "Interruption Preview" (GRANDHI; JONES, 2010). In this case the users are able, by themselves, to assess if they are receptive to an interruption. While this approach may be desired to avoid missing out on important interruptions, it was only viable in the presented context because the quantity and complexity of the interruptions were somewhat limited. When the quantity of interruptions becomes overbearing the users may not be able to make individual decisions on how to behave.

2.4 Summary

The goal of this chapter was to present the necessary knowledge to allow an informed discussion on the problems tackled by this work. In the Privacy section a brief overview of the different concepts and facets of privacy was presented, followed by a discussion of current privacy protective approaches. By understanding what has been done it is possible to see that traditional approaches (i.e. notice and consent, settings and policies) may not be directly appropriate to this work's context unless adapted to match its more dynamic and intense nature. On the other hand, it is possible to note that higher level approaches (i.e. regulations and guidelines) should be more broadly and intensively applied to develop more privacy-sensitive applications. Later, by reviewing some of the privacy biases and obstacles, both in general and in IoT, it became clear the complexity of the issue and the necessity to enter it well informed.

In the Control section, we presented some concepts of control, user control in privacy and why the user cannot be completely dissociated from computational systems. An

overview of concepts related to balancing user control in automated systems was also presented. As seen, there is a lot of effort in creating collaborative systems, especially in the autonomous vehicle and robotics area. The addition of the user in the control loop benefits the user (higher awareness) and the system (improved performance). In the last section, a discussion about interruptions was presented. The concepts related to how to determine when to interrupt a user, interruptibility and receptivity, were presented as seen in this work. These two concepts have informed the separation made in the variables selected for the Intelligent Privacy Interruption variables, as they represent the user's desire to be interrupted and the ability/acceptability of being interrupted. This section ended with an overview of methods that can be used to manage interruptions outside of the scope of privacy-motivated interruptions.

Finally, this chapter shows that even though these three topics - privacy, control and interruptions - are research areas in and of themselves, they are extremely interconnected once the topic of discussion is how to manage privacy-related interruptions in the context of the Internet of Things. In the following chapter, related work to approaches for privacy management in the Internet of Things is presented, exposing the intersection of these three research areas. The next chapter also presents related work on how to balance user control and system autonomy, and on the effort of doing so without disrupting the users.

Chapter 3

Related Work

In the previous chapter concepts related to the conceptual basis of this thesis were presented: privacy, control and interruptions. The investigation of these three areas have partially intersected over the years. For example, there have been privacy related solutions that consider aspects of adjustable autonomy or adjustable autonomy approaches that consider issues of interruptibility and/or receptivity. However, this is not an overlap that has happened frequently enough to constitute an area of research on its own or to yield a high number of publications. Because of this, this chapter attempts to identify relevant work that fits in at least a subset of this research area: *privacy solutions* that consider *interruptibility* and *receptivity* as aspects to inform *adjustable autonomy* rationale. This section does not provide an extensive review of each of these individual topics. They are all major areas of research with a variety of contributions in different context. The related work presented is a subset that is thought to convey a sufficient and necessary awareness of what has been done and how.

3.1 Privacy Solutions on a Control Continuum

A specific facet of privacy is related to deciding whether to share your information or to use services that will require you to do so. By examining literature related to this in the context of ubiquitous computing and the Internet of Things a common concept emerges: a control continuum. In context-aware research it is commonly accepted that this continuum will range from manual to fully automated decision-making with intermediate positions being possible in accordance to specific needs and situations (FLEMISCH et al., 2012; HARDIAN; INDULSKA; HENRICKSEN, 2006; RÖCKER, 2010). However, this work considers the notion of control not only as an active imposition of the user's preference through a decision, which in this works scope would refer to giving or withholding consent. Control is also related to the level of awareness the user has about what is happening.

Considering the previously seen notice plane (Figure 4), and if the difficulties related to the level of comprehension obtained from a privacy notice have been resolved[26], the notice plane becomes a notice line on which our continuum is defined. As seen in Figure 7, the axes inform the disruptiveness of the interruptions generated and the comprehension obtained from receiving them. The lower the level of interruption disruption the higher the level of system autonomy, the higher the level of comprehension, the higher the level of user control.

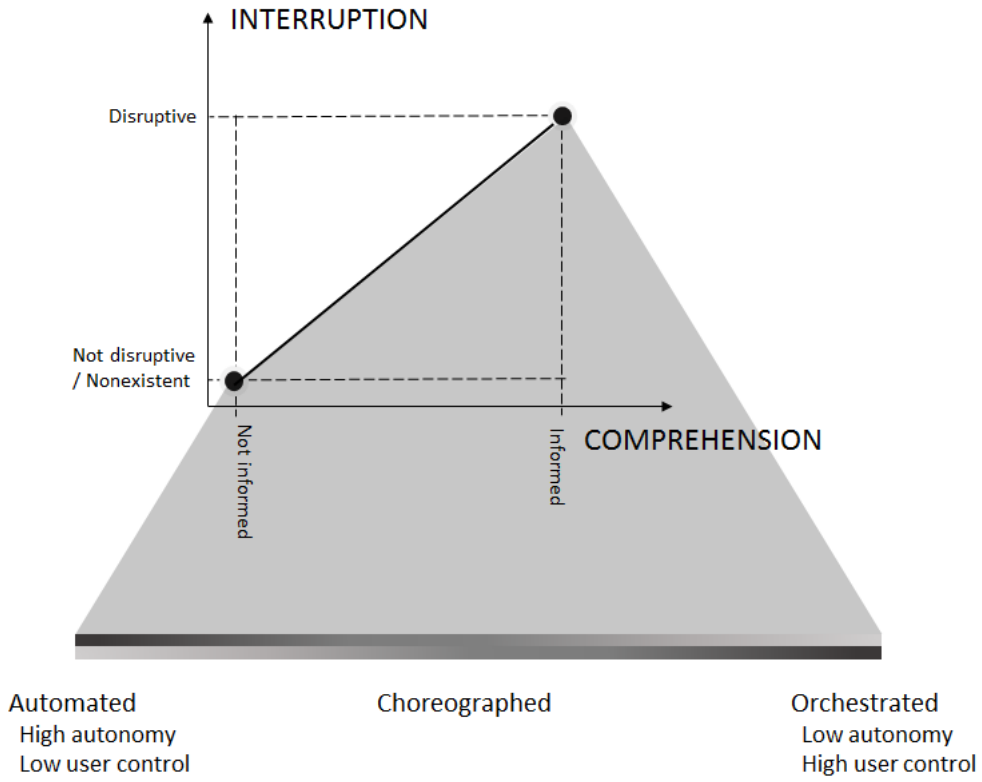


Figure 7. Description of the control continuum based on the notice plane previously described.

3.1.1 Automated Solutions

Automated solutions can be found on the left side of the continuum (Figure 7) in which the interruption is not disruptive or nonexistent. Consequently, the user is not informed and does not comprehend the situation. These solutions appeal to IoT developers given that, from an IoT perspective, the ideal situation would involve little to no user involvement in establishing and executing services. They can either be a pessimistic application where a user-defined (static or evolving) set of rules and preferences are used in order to make a

[26] Leaving the matter of being or not informed directly tied to the awareness of the existence of the notice itself.

decision, or an optimistic application in which a greater access to information is allowed and abuses are detected after the fact through logs (HONG; LANDAY, 2004).

The most basic form of automated solutions uses the definition of privacy rules and profiles to inform the automated decision on whether to share a piece of data. The applications differ on how to define these rules and profiles. For example the Privacy Studio (HÄKKILÄ; KÄNSÄLÄ, 2004) allows users to define privacy profiles with different sharing levels for specific groups; Faces (LEDERER et al., 2004) supports the specification of rules using the metaphor of the social face you put on to interact with different groups; Hull et al (2004) uses forms to collect user preferences which are then translated into rules; and Kim et al. (2010) propose to tackle the issue of managing privacy in ubiquitous computing environment by describing context using ontology and user profiles to identify preferred behavior in a specific context situation and data sharing necessities. Given that in automated solutions it is extremely important to collect valid and detailed information about users' preferences, it is also important to do so without it becoming burdensome.

Another approach that considers the definition of privacy rules proposes a privacy-by-negotiation solution for the Internet of Things (UKIL et al., 2012). The idea is to arrive at an agreement between the data producer (user) and the data consumer (service) on what data will be share and at which level of disclosure. The described activity flow is asynchronous. Whenever there is new data or information that the user is willing to share, s/he registers it with the negotiation module. This module is not only responsible for the negotiation between system and services, but also for negotiating with the user the level of information disclosure given the ability for that information to identify the user. Once an agreement is reached between the negotiation module and user, this preference is saved to a negotiation matrix. Later, when a service requires data, it contacts the negotiation module, which verifies if the request matches the user's preferences. Any modification to the data is informed to the service (e.g. noise was added to the data) and if this is accepted the desired sharing occurs. If not, the data is not shared. They also propose the use of SafeMask, which uses hierarchical-based masking, quantization approaches, perturbation and/or randomization to achieve the level of anonymization required/desired by the user.

Moving on to automated solutions that combine pessimistic and optimistic approaches, UEPCSI (HENZE et al., 2014), aims at protecting the users' privacy in a cloud-based services for the IoT environment. In that approach users can define policies for data sharing, using suggested privacy configurations made by a trusted third party, as well as have access to a detailed statement of data usage. Although it is not exactly clear whether

the privacy policies are defined once per service and automatically used from that point on, the description of the process leads to this conclusion, which characterizes it as an automated solution. However, this highlights one of the issues of automated solution since the policies are individual to each service and it is not possible to define beforehand every single policy, as services can be made available and unavailable dynamically. This requires that the user be prompted for new inputs on new services or allow over/under sharing.

In PeopleFinder (SADEH et al., 2009), although not directly applied to IoT, the issue of articulating privacy preferences a priori was noticed and the authors offer functionalities to allow modification of rules based on the requests that were submitted and how they were processed. This is already an improvement to more basic automated solutions, since it offers some post hoc awareness. Nevertheless, during the process of deciding whether to share information PeopleFinder relies on agents that operate based on policies specified by the user, without his/her participation. In fact, even when a request cannot be satisfied the user is not queried, instead an ambiguous message is returned to the requester without the information requested. Similar in this post hoc awareness and control offered by the PeopleFinder, pawS (LANGHEINRICH, 2002) uses privacy proxies to handle interactions between data subjects and collectors while also providing control capabilities such as data updates, deletes or viewing usage logs. These proxies use machine-readable privacy policies to match and enable or disable services based on user preferences. Although stated that it will keep track with or without the user's help, it aims to be a 'silent but watchful transparency tool' with the proxy apparently performing all necessary actions without user involvement. Another automated solution that allows the user to offer input in a post hoc manner uses an overall model description which does not consider any user interaction during the actual consenting moment (GOMER; SCHRAEFEL; GERDING, 2014). This is highlighted as a positive aspect since the users do not need to shift their attention from their tasks. The user participates only in phase 1 (preference setting phase) and phase 3 (review).

The next two reviewed automated solutions go back to basic automated solutions in which the user participates only in the definition of the preferences. Both deal with the privacy protection, in particular privacy related to sharing location data, through obfuscation. The Dynamic Location Disclosure Agent (DLDA) for the IoT context considers contextual elements associated with privacy preferences to generate a location output with the desired level of precision (ELKHODR; SHAHRESTANI; CHEUNG, 2013). Whenever faced with a context in which a privacy preference has not been specified, the DLDA enforces a default profile autonomously. Lastly, Agir, Calbimonte and Aberer (2014) present an intelligent system that depends on a model of the adversary (person or system trying to gain access

to information) and user privacy sensitivities to establish the appropriate level of detail to be divulged. A system feedback loop is used in which the Protection Mechanism obfuscates a new event. Once an obfuscated location is generated it is verified by the Privacy Estimation Module (adversary model) to check the expected privacy-level of the obfuscated location against the user's sensitivities. In case it needs further adaptation, the Protection Mechanism adjusts its parameters and does the steps again until the sensitivity preferences are satisfied.

However ideal from the IoT perspective, from the users' perspective it can be noticed that these automated solutions imply a great loss of awareness about the flow of information and, consequently, a loss control over their data sharing and privacy. With time, the consent process becomes opaque to the user either because of intelligent adaptations or because the user cannot remember or has changed his/her preferences (BUNNIG; CAP, 2009). Also, because privacy is deeply contextual and ever changing, the requirement that the user define preferences and behaviors in advance leads to many failed scenarios, either because the user did not know how he would behave or because a slight change in the context has created a new and different privacy context than what the system is aware of based on initial configurations (SCHAUB; KÖNINGS; WEBER, 2015).

3.1.2 Orchestrated Solutions

Orchestrated solutions try to mitigate this "black box" situation and are an alternative to automated solutions. They are represented on the right side of the continuum (Figure 7) where interruptions are disruptive but lead the user to a high comprehension of what is happening. They would be equivalent to common "notice and consent" where the user is fully in charge of understanding the situation and making the appropriate decision, or to a variation of this notion in which there is some pre-processing of the facts to aid the decision-making process. The term orchestrated was extracted from service-oriented literature for its reflection of having a central unit (the user) effectively responsible for making the correct decisions (PELTZ, 2003). It also implies the orchestra metaphor in which a maestro leading the individual players produces a more coherent outcome.

Because "notice and consent" is a known paradigm for privacy, we will only present Hong and Landay (2004) work as an example of how this approach is normally applied. Their work was selected because they build upon the notion of "notice and consent" and present Confab, "a toolkit for facilitating the development of privacy-sensitive ubiquitous computing applications". Confab considers requirements broader than "notice and consent"

such as a decentralized architecture that does as much as possible in local, user owned devices, and the existence of control and feedback mechanisms. They propose the use of *infospaces* to encapsulate user data, access control mechanisms and privacy preferences. Confab was used to build different applications, which shows its flexibility and generality. One of the applications presented was a location-enhanced messenger that represents its "notice and consent" roots. In that application, the user had to provide his/her preference to share location data whenever requested, unless there was a policy already in place that matched the current context.

To illustrate solutions that go beyond the traditional "notice and consent" approach, some orchestrated solutions are presented, which offer the user a pre-processed suggestion combining computational processing and human reasoning for a better result, or that follow a different workflow than the one expected from "notice and consent". One example is a method to reason about and suggest obfuscations that is not only capable of detecting when data has been obfuscated but it also helps the obfuscator make more adequate decisions (AN; JUTLA; CERCONE, 2006). In the described scenario, the user uses a preprocessed model of obfuscation suggestions and is responsible for making the appropriate choice given the person requesting the information, the circumstances and known facts by the requester. The user is then queried and must make the privacy decision of sharing and the accuracy of his/her location data. Another example of a privacy preserving solution that employs the user as a central unit while helping him/her make the decision requested is uses two Privacy Recommendation Engines (PRE) to suggest a subset of sharing actions in the moment of the data request so that the user can make a better informed decision (JIN et al., 2013). These suggestions are obtained by combining a default policy, obtained from anonymized and abstract sharing behavior of existing users, and the users' own sharing history.

Gaud, Deen and Silakari (2012) propose a more proactive workflow to protect privacy than the traditional "notice and consent". Once a request is made they present users with a preprocessed list of services available that fit their defined sensitivity levels. The user defines these sensitivity levels for groups of data so that the system can analyze how adequate available services are to those preferences, and then present them in a rank for the user to select desired services. Another example of a proactive orchestrated solution is the Privacy Coach (BROENINK et al., 2010). The Privacy Coach verifies if the policy of a RFID tag matches the privacy preferences previously defined by the user. Because it notifies the user in either case (match or no match), it qualifies as an orchestrated solution.

Even though orchestrated solutions provide the level of transparency necessary for the users to become aware of what is happening and able to exert control over their data sharing, orchestrated solutions do not scale well. They become increasingly less viable with the growth of the number of connected devices interested in having access to the user's data (ACKERMAN, 2004). In a world where there are more connected devices than people, it becomes clear the problems of these solutions: contrary to computers processing power, human attention and time are limited and expensive resources. The weight of this issue could be clearly noticed by the fewer number of solutions that follow this concept when analyzing the literature related to ubiquitous computing or IoT.

3.1.3 Choreographed Solutions

Automated and orchestrated solutions are direct opposites in both their pros and cons from the IoT and user perspectives (see Table 1). Each can prevail depending on the viewpoint (TOCH, 2011). As a tentative middle ground, intelligent context aware solutions arise. These choreographed solutions are constantly practicing and evolving using context cues and user input that, with time, makes their error rate smaller.

Much like the dancers in a choreography, choreographed solutions start with a small but significant set of information and rely on an instructor guiding them as to what to do or correct mistakes made. They also count on external input, such as physical and social context, to adapt accordingly to the "music" being played. Because they do not require users to predict behavior beforehand of as many situations as possible, the initial fine tuning problem (LEDERER et al., 2004) and the influence of the Attitude/Behavior dichotomy are diminished in these solutions. Also, these solutions continually require user input since they are constantly learning, which increases the level of user awareness and control. However, this required input diminishes with time, reducing the level of interruptions and the influence of the control paradox in the decisions made.

Before describing what is here considered a fully choreographed solution it is important to mention the initial steps that were taken to evolve privacy preserving solutions from their automated characteristics. Previous work shows the fundamental difference between choreographed and automated solutions: the involvement of the user, instead of default or best-effort actions, whenever a discrepancy is found when matching known privacy preferences and current situation (ORTMANN; LANGENDÖRFER; MAASER, 2007; PALLAPA; KUMAR; DAS, 2007; YEE, 2006; ZHANG; TODD, 2006).

Table 1. Comparison between the pros and cons of automated and orchestrated solutions from the Internet of Things perspective and the user perspective.

	IoT PERSPECTIVE		**USER PERSPECTIVE**	
	PROS	**CONS**	**PROS**	**CONS**
AUTOMATED	Gives the 'things' more autonomy to communicate		Low level of interruptions	Low level of control and awareness Requires fine grained tuning Plays into A/B paradox
ORCHESTRATED		Hinders 'things' communication by requiring constant user involvement	Full control and awareness over privacy Just-in-time decisions	Frequent interruptions Plays into control paradox

Yee (2006) presents a ubiquitous computing architecture that respects personal privacy preferences expressed through personal privacy policies. The behavior of the system is as follows. A policy module requests from the data sharer his/her privacy policy in regards to observers. When this policy is offered, the privacy module requests the data observer his own privacy policy. If inconsistencies are found, the privacy module notifies the data sharer and asks if a negotiation of the policy is desired. If there is an agreement, a sharing session is established. If not, the sharing does not happen and the system is idle until a new interaction happens. Another privacy respecting context aware architecture is presented by Zhang and Todd (2006), which provides support for collecting, storing, processing and dissemination of contextual information. Of interest to this work are the privacy components of the architecture: privacy policies repository and privacy agent. While the privacy policies repository serves as a historic knowledge base of all privacy agreements, the privacy agent both mediates the privacy-related interactions between context sources and context clients, as well as allows the user to have instant access to adjust privacy preferences. Considering the mediation aspect, the privacy agent would analyze the context requests it receives related to the user's privacy preferences and would either accept the request or, if a conflict occurs, notify the user and wait for the approval or rejection.

Focusing on passive collection of user data, an architecture is proposed that makes use of virtual sensors (i.e. a representation of a real sensor that can be sub-divided into

several regions to offer a finer grained control) to adapt the real sensors present in the environment to the users' privacy preferences (ORTMANN; LANGENDÖRFER; MAASER, 2007). In their approach, if the user is alone in a virtual sensor region, that user privacy preference is enforced. But if the user enters a region with previously registered users there are three cases to be considered: clear accept, clear reject and conditional accept. In the latter users are notified of inconsistencies in the region privacy policies and their own and are given the option to accept or not the policies.

Another simpler choreographed solutions is Precision (PALLAPA; KUMAR; DAS, 2007), a context-aware system for information fusion that is enhanced considering privacy aspects. In their system, they present the concept of a *privon*, which is a composite entity that encapsulates related information based on their privacy-sensitivity levels. To make a privacy decision, their system relies on checking if there are similar entrances on the *privon* cache and, if so, compares the created *privon* with that entrance. When there are differences between the *privon* generated and the one cached, the system prompts the user with suggestions for modifications to match the cached version. If the user overrides the suggestions this new version is cached and future suggestions will consider both entries.

Moving on to more complete choreographed solutions, i.e. they have some intelligence imbued in them; even though there is a hint of a desire to build a fully automated solution, Bunnig and Cap (2009) present statistical evidence that a choreographed solution is indeed viable for situations with varying contextual information. In their work, to relieve users from having to decide before hand on privacy aspects, for example by having to define privacy preferences, they propose an ad hoc privacy management in which users are only prompted for privacy decisions the moment they are really needed. As we have stated, they noticed the drawback that this orchestrated approach has: it requires a significant portion of the users' attention. To avoid this, they propose that services delay requesting information to make sure that an interruption will not occur unnecessarily and that assistance be provided to relieve the users of having to make frequent disclosure decisions. Because of the latter, the authors propose a disclosure decision module (DDM) that takes into consideration context and user preferences and emulates the user's privacy preferences to make decisions for the user or, at least, make suggestions. The authors also present a simulation of this module considering a small training set with six different techniques and conclude that it is possible to correctly identify the preferences for most cases, but this is not enough to allow for a completely automated solution.

Following Bünnig and Cap steps of adding intelligence to choreographed solutions, Super-Ego is a privacy framework for privacy-sensitive bounded context-awareness in which it is possible to vary the level of automation or user interruption (TOCH, 2011). The author openly discusses the fact that people have different privacy preferences and profiles, which makes them desire different user experiences regarding the level of automation and control. In Super-Ego, this variation was defined by two thresholds: manual threshold and disclose threshold. The thresholds can define a full manual solution, fully automated, semi-automated with fixed interval or semi-automated with variable interval. In the latter, the interval is the standard deviation for the historical decision of disclosure for that location. Like other works, these thresholds were used considering system certainty on a certain disclosure, or as they put it, historical ratio of disclosure for a location (r). The user would be interrupted if, and only if, the ratio was between the two threshold values. While this threshold values can be user-defined to better adapt to her preferences, this is still far from ideal. For example, because Super-Ego only deals with location variables, the authors do not consider the fact that different data types will have different sensitivities, which may also lead to a variation in these thresholds.

Considering a more complex characterization of privacy implications when sharing data, Schaub et al., (2012a) present a model for privacy adaptation that takes into consideration the context in which the user is found and the ongoing privacy related activities. This model is based on the consideration that privacy is not only related to information and data sharing, but also to the “right to be left alone”. They consider three main entities: user, environment, and activities in relation to dynamic and static information as well as disturbances. Although their paper is mainly theoretical, they state that the proposed model can support both autonomous reconfiguration of privacy (automated solutions) as serve as user support in privacy decisions by offering warnings and recommendations (choreographed solution). In fact, they propose a privacy decision engine (SCHAUB et al., 2012b) that will adapt to individual users’ privacy preferences over time using previous knowledge and dynamic knowledge obtained through explicit or implicit interaction with the system. The decision process involves collecting contextual information that can be used for privacy decisions in such a way that whenever a context change happens that makes it necessary to review privacy policies, the privacy decision engine makes use of its knowledge base (preferences and policies) to adapt the privacy policy. If the confidence score on the adapted privacy policy is below a certain threshold, the system triggers the user for further input adding him/her to the decision loop. In another paper the authors add that the results

obtained from the adaptation can be provided as recommendations tailored to the user to help in the decision process (SCHAUB; KÖNINGS; WEBER, 2015).

Lastly, in the context of the Internet of Things, Copigneaux (2014) introduces a choreographed solution that combines rules, context-awareness, behavior modeling and community based reputation systems. The rules are defined considering the action to be performed on the data, the type of data, the person performing the operation and context information, and can have three outcomes: allow, deny or prompt. This is particularly interesting because so far the user had only been prompted case the system was not sure of the action to take. However, in this system the user can define how and when to be contacted by the system on top of being contacted whenever the system is confronted with a situation not specified in any of the rules. In the latter situation, the system also differentiates itself from the others by gathering insights from behavior modeling and the community based reputation system to provide options to the user.

This type of solution seems to be the ideal situation for dealing with privacy decisions in an IoT environment; it balances both the users' needs and IoT needs. However, current solutions are too much alike automated solutions in their effort of providing high accuracy with little user input from the start, falling into some of the same issues of automated solutions. They also fail to acknowledge that there are several factors that may influence the users' decision to prefer a more automated or orchestrated solution and consider only the system's confidence in the inference made as to decide towards which side of the continuum it will sway. Finally, the majority does not consider that users differ from one another more than just in the privacy preferences they have, but also on the level of awareness and control they desire, leading to a lack of higher personalization in aspects other than privacy preferences.

Figure 8 presents a comparison of the discussed privacy solutions considering the continuum and the presence of intelligence in the system. The intelligence was considered only on the setup of the preferences or during the sharing stages and it means that the system did more than just relay information or follow pre-defined user instructions. It is important to remember that non-intelligent orchestrated solutions were filtered out of this chapter because they are too alike "notice and consent", so the lack of "not intelligent" solutions in the chart does not necessarily reflect the field.

Figure 8. Classification of the Privacy Solutions presented by grouping and presence or not of intelligence either on the setup of preferences or during sharing stages.

3.2 Approaches to Balancing Autonomy and Control

Related to the concept of choreographed solutions, which balance user control and system autonomy, the works presented in this section focus on adjustable and adaptive autonomy. They try to identify aspects and/or present models that can inform agents and their developers as to when a human operator should be interrupted for input.

Falcone and Castelfranchi (2001) present a theoretical framework with the necessary vocabulary to discuss variations in approaches of adjustable autonomy. More than just the conceptual instruments defined, it is of interest to this work the criteria of when and why autonomy adjustments should be made. They suggest that the timely performance of the delegated task, the accuracy, the overstepping of its role, and the presence of obstacles are reasons to reduce the delegee's autonomy (in our case, the agent). Per the authors, increase in autonomy should happen when there are increases in task quality perception; favorable external conditions; proven ability to do more than previously assigned; and, if the system is being limited by the lack of autonomy. On the delegator's side (in our case, the user) a low confidence in the performance of the task and the presence of unforeseen events are reasons to limit one's own autonomy. Finally, the belief that one could do a better job, the permission to do so and the acceptance of this increase in autonomy from the delegee are reasons to expand one's own autonomy.

While these are reasonable and valid reasons to modify the level of autonomy, once they are brought to the context of a privacy agent some of them become more than just common sense, but should be considered in the design of the agents. For example, the notion of a privacy agent overstepping its boundaries is not a reason to reduce its autonomy, but to rethink the whole design of that system. Other examples are that, by design (as in accordance to perspective of this thesis), users should not need permission nor worry about the acceptance of the agent when thinking of increasing autonomy. However, this is important when the agent is thinking of interrupting the user. Later in the paper the authors summarize the remaining reasons as a matter of trust. When thinking in the case of privacy agents this trust relationship can refer to the user trusting the agent (e.g. accuracy, overall trust and acceptance of risk), the user trusting him/herself (e.g. believing in one's capabilities of making the right choice in that moment), the agent trusting itself (e.g. certainty on their decision), and the agent trusting that the user can make that decision at that moment (e.g. cognitive and contextual workload and interactions).

Myers and Morley (2001) present a framework for human directability of agents that allows the creation of policies to adjust the level of autonomy and the selection of strategies. The framework was built considering two premises that do not fit the context of privacy agents, namely that it is a permissive environment and that the agent has all the information necessary to perform its tasks. However, many of the concepts and ideas presented can be adapted and considered in the privacy agent context. They consider that an agent has a library of plans that define the range of activities it can perform. Each plan will have a cue, preconditions and body, which in the privacy agent context can be considered as the request being made, the user's privacy preferences and the action to be taken. Furthermore, they also consider the concepts of *permission* and *consultation requirements.* The first defines when the agent must request authorization to perform an action. In this work's scope, it would be equivalent of the privacy agent requesting confirmation of possible decisions to share or not data. The latter defines when the agent should defer the decision to the human supervisor, which has the exact equivalent for privacy agents. Nevertheless, this paper only offers a high level model to inform how an agent should behave and to allow the user to define this behavior. When considering the scope of this work of informing when the user should be interrupted, it lacks specificity and fine-grained suggestions to inform what would be the permission and consultation requirements. This is most likely caused by the difference in focus between both works.

Scerri et al. (2001) explore the use of teams of agents to manage meetings and presentations schedules. This is similar to the context of the Internet of Things with multiple

agents coordinating in order to provide a service and in which a wrong decision or long delay may cause miscoordination and associated risks. The authors tackle three challenges that arise from adjustable autonomy: coordination, team decision, and safe learning. They approach these challenges by using an adaptive model that considers the cost of waiting and/or miscoordination versus the cost of an erroneous autonomous decision and/or interrupting the user. Their model considers rewards based calculation taking different factors into account: the presence of the user, the number of delays versus the number of attendees (cost of making repairs), the elapsed time since the start of the meeting, the importance of the user for the meeting, and the actual start of the meeting. Individual differences are added to the model through weights. The challenges presented, the lessons learned and the approaches used can be similarly used within this work's context. However, the aspects taken into consideration do not fit the challenge of agent-based privacy decision-making. Some of the aspects considered can be somewhat directly translated. For example, the importance of a user (role) for a meeting to calculate the reward could be considered as the sensitivity of a particular sharing occasion when calculating the possible risks. However, it is still largely necessary to examine the aspects that should be taken into consideration when considering adjustable autonomy in the context of our work.

Bradshaw et al. (2005) offer three main contributions to the issue of adjustable autonomy in agents. They present a common vocabulary that can be used to discuss adjustable autonomy solutions; they propose Kaa, which is an extension of a previous work (KAoS) that provides policy-based adjustable autonomy; and they present a comparison of the two previously discussed works[27] in relation to theirs. To briefly present the first contribution, autonomy is presented as a multi-dimensional concept that involves two main dimensions: descriptive, related to self-sufficiency; and, prescriptive, related to self-directedness. Associated with these dimensions, the concepts of potential actions, possible actions, performable actions, permitted actions, available actions, achievable actions, obligated actions, and required actions are discussed. Finally, adjustable autonomy is said to be achievable through adjusting permissions, obligations, possibilities, and capabilities.

The second contribution, Kaa, is a component that allows for automatic adjustments of autonomy based on policy. Their implementation uses an influence-diagram-based decision-theoretic algorithm to decide whether to make changes in the autonomy level. In this diagram, the available adjustment options, capabilities/conditions for these options and their costs are accounted for. While Kaa operates as a broader adjustable autonomy module

[27] Though they based their discussion on a later work published by Myers and Morley: Directing Agents (2003)

that takes into consideration previous higher-level aspects into consideration, it is interesting to note that there is also the presence of a classifier that is responsible for determining who (if anyone) should be consulted. Unfortunately, the behavior of this classifier was not thoroughly described. But it is said to work on a policy-to-policy basis, since some situations can be delegated to the Kaa, others may only be trusted to be resolved by a human operator and others may need to be resolved quickly and an attempt to contact a human operator will only be performed once.

Lastly, the authors compare previous works (TRAC and AA) based on the party taking initiative for the adjustment, rationale for adjustment, type of adjustment, default modality, duration of adjustment, party who is final arbiter, locus of enforcement. For the focus of this work it can be said that none of the discussed solutions were ideal in their entirety. This was expected given they were developed with different applications in mind, which does not diminish their contribution.

Finally, based on Parasuraman, Sheridan and Wickens (2000) ten levels of automation and four-stage model of human information processing, Fereidunian et al. (2007) propose a methodology for adaptive automation with a finer-grained granularity as to when to adjust the level of automation required in the context of power distribution automation. This finer granularity is obtained by using expert judgment to identify ten performance shaping factors. The factors were the most influential ones related to the performance of the human operator and decision maker. They were quantified as binary values to allow the characterization of different possible situations and to inform the level of automation necessary in each of the four stages. Given the different contexts, the type of “performance shaping factors” identified using expert judgement is not applicable to the context of this work. However, the we used a similar approach. In this thesis, the expert judgement was obtained through the identification of relevant variables (or factors) throughout literature. Nevertheless, the variables identified in this work are more nuanced than what a binary representation can offer. They are meant to be continuously analyzed instead of in a one-off manner and the focus of automation adjustment is different. For this thesis, the balancing of autonomy and control was considered in a longitudinal sense. That is, while each situation was analyzed as being binary in nature (desire to be interrupted to exert control or not be interrupted and delegate the control to the agent), the balance would come from knowing throughout multiple interactions when the control should be given back to the user or not. The approach used by Fereidunian et al. (2007) is considered the adequate level of automation in an immediate sense. That is, for each individual interaction a level of cooperation between system and user was decided.

As could be seen, there are different approaches to balance system autonomy and user control. While they vary greatly in granularity and context, the underlying premises that inform when to change the level of autonomy tend to be similar: an analysis of costs and benefits of making this change.

3.3 Managing Interruptions

Having reviewed previous privacy solutions on a continuum of user control and autonomy and existing research on adjustable autonomy solutions, two things become clear: it is important to avoid burdening the user with interruptions but it is necessary to balance interruptions and awareness. This section reviews related work that have explored different ways to manage interruptions and ways to avoid the issue of burdening the user.

The work of Ercolini and Kokar (1997) presents a Desktop Agent Manager (DAM) which is used to decide when software agents (i.e. “background processes that notify a computer user of certain predefined events”) can have access to the user. They present the architecture of the DAM but focus on the decision mechanism, the point of interest of this thesis. Their mechanism uses aspects from the user as well as the agent to decide if the user should be interrupted or not. From the user perspective, his/her self-declared status is used as an interruptibility threshold variable with four levels - bored, flexible, busy, do-not-disturbed. From the agent perspective, the authors consider the agent priority, the presence of keywords and keyword priority, the time limit to process the interruption-related task and the priority of the result (defined by the interrupting agent). Even though the system was only initially validated, this paper is interesting because it considers individual differences to optimize the decision (through allowance of user adaptation of the user threshold and selection of keywords) and even propose allowing the user to weight their own parameters. Thus, they concluded that the parameters for deciding whether to “filter” or not an agent cannot be considered in isolation. They point out that when the threshold level was low (interruptibility related) the priority of the agent was the only parameter that was critical (receptivity related). This shows that while interruptibility and receptivity (as described in Chapter 2) are important concepts, they cannot be considered alone.

Differently from the simulated approach used by Ercolini and Kokar (1997), Dabbish and Baker (2003) explored decision models by observing the behavior of administrative assistants. Aligned with the argument of this thesis that suggests the need of systems that consider aspects related to the users instead of just the interrupting system, Dabbish and

Baker (2003) define a model that can "aid in building systems more sensitive to the actual needs of the user". In their context, they identified four actions to be taken after analyzing the importance of the interruption and the interruption threshold: allow the interruption, inform about the interruption but act based on what's answered, schedule a meeting[28], and take a message. In their straightforward paper, the proposed models were extracted from interviews with outstanding administrative assistants but the results still lacked validation. One important aspect they highlight, however, is that in the real world, there is more to consider than the user interruptibility (in the paper referred as "interruption threshold"). The main flow of their proposed model is very similar this works proposal: it considers both receptivity (importance of the interruption) and interruptibility (interruption threshold). Nevertheless, this paper is very specific to its context and lacks a higher granularity that can be expected from the interaction between human users and computational systems.

Grandhi and Jones (2010), as mentioned in Chapter 2, studied management of technology-mediated interruptions in the context of interpersonal communication. They propose the categorization of the approaches in two paradigms of interruption management: interruption impact reduction (i.e. reducing the negative impacts on the social and cognitive space) and interruption value evaluation paradigm (i.e. optimizing individuals' decision making process about how to respond to interruptions). On top of presenting these two paradigms, arguing for the second, and showing the importance of relational context, they propose a formula to calculate the predicted interruption value (PIV). PIV is used to "guide an individual's interruption response decision making" and it balances out the perceived benefits and costs considering the users' current context and individual differences. The PIV is used to determine *if* the user will engage with an interpersonal technology-mediated interruption outside the scope of privacy. A similar approach could be used to decide if the user *should* be interrupted when considering privacy related interruptions. That is, an approach in which the benefits and costs of the interruptions are compared and weighted against one another.

Aiming to assess which variables influence users' availability to engage in just in time interactions (JITI) that promote health well-being, Sarker et al., (2014) analyzed collected physiological and self-report data in order to identify which factors had greater influence in predicting availability. Data collected from 30 participants during one week of study allowed them to conclude that location, affect, activity type, stress, time and day of the week play significant roles in predicting availability. Similarly, to other studies, their work does not focus

[28] In the context of system generated interruptions, this could be seen as post-pone to be dealt with.

on privacy and so differs from this work. However, their focus on health relevant notifications displays a similar interest in providing interruptions that are not merely informative but beneficial and at times necessary, and that "require appropriate engagement of the user". However, they did not consider the broader perspective of interruptibility and receptivity. This is probably because receptivity is associated with the benefit of receiving the interruption and for health-related interruptions it could be expected that people would always be receptive. One final caveat to be considered is that their work assesses availability considering the time interval between the interruption and response. But because they offered monetary incentives for responses it could be that people were more "available" than they would normally be.

Finally, there are two previous researches that are extremely relevant for this thesis, both for their goals and insights. The work of Pejovic and Musolesi (2014) and Mehrotra et al. (2015a). Both works present the development of intelligent interruption mechanisms, such as the one proposed by this thesis. Both are also extremely relevant for this thesis as they show the possibility of modeling the acceptance of interruptions considering aspects of receptivity and interruptibility, as this thesis proposes. In fact, Mehrotra et al. (2015a) show that such model can outperform user-defined rules. The main difference between those works and this thesis arises from the context of use. While this work is interested in understanding when to intelligently interrupt the user so that him/her can make an informed decision related to privacy, their work focus on general mobile interruptions. For this reason, they will be presented comparing the differences in their approaches and how they fare when considered in this thesis' context.

From the receptivity perspective, while both explore the influence of the user's current state (i.e. emotions), Mehrotra et al. (2015a) also explore the interruption content, while Pejovic and Musolesi (2014) explore the effect of social engagement. As a rule of receptivity, both content and social engagement are relevant variables, and because these aspects have been individually examined, this current work can build upon their results and explore them combined. However, it is important to note that when brought to a privacy context content poses an even more important role, since it is not only used to decide on the usefulness of the interruption but it also involves managing possible risks. From the interruptibility perspective both explore common aspects such as workload, location, activity and time of interruption[29], but Mehrotra et al. (2015a) adds system-related data, such as phone status and ringer mode. This is interesting because in the context of privacy-related

[29] With location, activity and time broadly characterizing the user's context.

interruptions, system-related data (e.g. system certainty) becomes extremely important. However, it is used to define receptivity, not interruptibility. Finally, both were performed “in-the-wild”, with Mehrotra et al. (2015a) collecting data from actual mobile interruptions, and Pejovic and Musolesi (2014) making use of ESM. Because the IoT is not yet available to its full potential, this work uses an approach more like Pejovic and Musolesi than that taken by Mehrotra et al., even though the latter would yield results with a higher chance of representing actual behavior.

As mentioned, these selected papers are not a thorough review of research that explores different ways to manage interruptions to avoid the issue of burdening the user. In fact, in the following chapter, many other papers are referenced when discussing the variables considered in this thesis. However, these previous works were selected because they show different approaches to develop a model to inform interruption delivery, as well as they show how receptivity and interruptibility should not be considered separately. The approaches vary from system-based with later validation (ERCOLINI; KOKAR, 1997), to mathematical approaches (GRANDHI; JONES, 2010) and data-guided approaches. With the later varying the format of the studies, from in-situ observations (DABBISH; BAKER, 2003), to remotely and automatically collected data from real interactions (MEHROTRA et al., 2015a) or simulated interaction (PEJOVIC; MUSOLESI, 2014; SARKER et al., 2014).

3.4 Summary

Because this work is in the intersection of privacy, autonomy and control, an interruptions research selected previous work in each of these fields have been presented. From the privacy perspective, it was noticed that choreographed solutions seem to be a better fit for the context of the Internet of Things, but that they rely too heavily on the system’s certainty to adjust their own level of autonomy. From this observation, previous work that explores how and when to adjust autonomy was reviewed. They present possible approaches and methodologies, but even with different contexts and specific goals the main goal remains: optimizing the overall performance by considering the benefits and costs of varying the level of autonomy. Finally, because systems that rely on user input require the user to be interrupted whenever this input is necessary, which is one of the major costs associated with a lower level of autonomy, it becomes vital to understand when to generate such interruptions as to minimize this cost.

Chapter 4

Intelligent Privacy Interruptions

"IN THIS GREAT CHAIN OF CAUSES AND EFFECTS, NO SINGLE FACT CAN BE CONSIDERED IN ISOLATION" – ALEXANDER VON HUMBOLDT

This work has two areas of research that serve as fundamental conceptual bases: interruptions and privacy. Previous interruptions research has mainly focused on understanding the effects that interruptions have on on-going tasks and trying to mitigate them. This mitigation is based on the concept of user interruptibility and receptivity to incoming interruptions so that interruptions are delivered with the most appropriate timing and mode. However, these works focus greatly on interruptions that are not time sensitive and/or that have no significant consequence to the person being interrupted. This reflects on the use of techniques such as delaying notifications as a way to make the interruption less disruptive and in frequently considering aspects from the social, physical and cognitive contexts, but not the content of the interrupting message to the same extent (see FISCHER et al., 2010; MEHROTRA et al., 2015a for works that consider content).

While interruption research has a consistently focused view of its problem and possible solutions, privacy research has broad and fuzzy boundaries that are expected from a multi-faceted issue such as it is. The focus ranges from exploring privacy in a conceptual level, with its implications and challenges, to ways of sustaining it, from both a legal and technological perspectives. These views are relevant when trying to understand and design with privacy in mind. In this work, however, the focus is on exploring systems used to aid users' data sharing decisions.

In chapter 3, choreographed solutions were identified as best for the IoT context, in which the number of devices requesting access can increase exponentially. They are based on Boyle and Greenberg (2005) statement that, "[t]here is no need for complete control in order to experience privacy" and they try to balance the level of interruptions and the user's need to

exert control. While there is the need to consider the user's interruptibility or receptivity for interruption management (FISCHER et al., 2010), previous work on choreographed solutions has mostly considered the system's certainty as a relevant variable for informing the system's interruption decision.

We believe this is because their focus has been on privacy modeling, in such a way that the systems can accurately infer privacy decisions so that the user is interrupted as little as possible and because such systems by themselves are already immensely complex. However, this neither considers the issue of interruptibility and that a single interruption in an inopportune moment can be worst that multiple interruptions in other moments; nor that there may be other factors that will influence users' choices to yield their decision power. Current solutions are a better fit with the notion of attentive notification systems (MCCRICKARD; CHEWAR, 2003) than with the complementary notion of adaptable notification systems (BELCHER et al., 2005).

In Chapter 3 it was shown that there have been approaches that tried to balance user control and system autonomy in the context of intelligent/automated systems. However, previous research has either offered finer-grained details but in a different context, or presented results in such a high-level and abstract way that it fits well in most contexts but does not have the level of detail necessary to achieve what is expected in this work.

Interruptions literature has explored interruptibility and receptivity, and some have indicated the need to develop ways of appropriately interrupting the user in the context of privacy decisions (PATIL et al., 2015). To the best of our knowledge, no previous study explored the best moment to interrupt the user considering more than the users' interruptibility in the context of privacy-related interruptions. It is in this point, where privacy research intersects with interruptions research, that this work aims at contributing.

4.1 Basic Characteristics

First and foremost, this work aims at helping designers of privacy agents in delivering relevant privacy-related interruptions at the appropriate moments. It considers "designing for consent" and that the system must be designed to be seamless and responsive but must allow users "to make meaningful, informed and timely choices about sharing of their data" (LUGER; RODDEN, 2013).

The main considerations made were that human attention is a finite resource (SIMON, 1971 apud KIM; CHUN; DEY, 2015)[30] that should be used parsimoniously and the users' need for feedback. At the same time that the latter consumes users' attention it increases transparency and helps users make more informed privacy decisions (PATIL et al., 2015). Previous research has shown the value of offering privacy-related interruptions and the need for it to be salient and informing but not annoying nor overwhelming (ALMUHIMEDI et al., 2015; LEDERER et al., 2004). This elucidates one of the necessary aspects for privacy interruptions to become intelligent:

> *Interruptions need to interrupt users and gather their attention, but this must be done at the right moments to avoid unnecessary burden.* [31]

This brings to light another issue that needs to be examined: which are the right moments? Researchers exploring ways to unburden the user from making privacy decisions have noted that even though interruptibility can help answer this question, it can be a limitation imposed to possible interaction strategies between the privacy decision support system and its user (SCHAUB; KÖNINGS; WEBER, 2015). This is because, in its current state, it does pose a limitation when taken into the context of privacy related interruptions.

When we consider interruptions that arise from a choreographed solution where an agent makes privacy decisions for its user to participate in a service, the "right moment" is not only when it will disrupt the user's current task the least. It is when it will help the user become comfortable with the decision that will be made, i.e. the user is confident that neither oversharing nor under-sharing will happen [32]. Because of this broader need, previous research on interruptions serve as a base for deciding when to interrupt a user or not, but new aspects must be extracted from privacy research. These aspects can influence the outcome of the decision to interrupt the user, making the interaction between agent and user is as adequate as possible.

There are many factors that affect the need for privacy and privacy decision making (ACQUISTI; GROSSKLAGS, 2005) and interruptibility research has conceded the limitations

---

[30] Simon, H.A. (1971). Designing organizations for an information rich world. In Computers, Communications, and the Public Interest: 37-72

[31] It is important to note that, while not in the scope of this work, the information presented by the interruption should have meaningful information so to be useful to the user.

[32] While oversharing leads to privacy breaches, under sharing can lead to missed opportunities to use particular services or misbehavior from used services.

that sensors have on determining user interruptibility by themselves (FISHER; SIMMONS, 2011; ZÜGER; FRITZ, 2015). Also, a holistic view is needed on the issue of interruptibility (even outside of privacy interruptions) (HO; INTILLE, 2005; MEHROTRA et al., 2015a) since many variables, by themselves, do not fully identify availability and interruptibility (SARKER et al., 2014). As such the following aspect also becomes necessary:

> *It is necessary to consider a combination of different variables that stem from both privacy research and interruption research to create a comprehensive model of user interruptibility when considering privacy-related interruptions.*

The combination of these variables serves a dual purpose: it offers a more holistic view of what affects users' desire to (not) be interrupted; and, it allows for this desire to be adapted to the different users' and situations. While the need to maintain control over different aspects of oneself is common to the definitions of privacy, different users have different preferences when considering the level of automation and interruptions that they desire (ALMUHIMEDI et al., 2015; SCHAUB; KÖNINGS; WEBER, 2015). The level of preference for control or automation also varies in accordance to context variables (HARDIAN; INDULSKA; HENRICKSEN, 2006; SCHAUB; KÖNINGS; WEBER, 2015). Lastly, in extreme situations, context might be the sole factor in deciding this level (HOLVAST, 2009). As such, the final aspect to be considered is:

> *The level of autonomy and control users desire from their interaction with an application varies accordingly to different situations and different users, so such application should strive to balance these levels accordingly.*

4.2 Variables

As previously mentioned, the most prominent variables were extracted throughout the literature about interruptions and privacy. These variables were selected considering the frequency of studies that identified and/or mentioned them and the strength and consistency of the results throughout the literature. The literature review was performed in stages and based on an exploratory approach. The first step consisted on examining the past 10 years of relevant publications such as Communications of the ACM, IEEE Security and Privacy, and IEEE

Pervasive Computing, and relevant conferences, such as CHI, Ubicomp and SOUPS. From these publications references were obtained. The second step was based on reading follow-up literature and references found in the works from the first-pass. Lastly a broad search using “privacy”, “privacy solutions” and “interruption” keywords was performed using ACM and IEEE digital libraries to reduce the chance of having overlooked significant literature.

From the knowledge obtained from this review it was identified that intelligent privacy interruptions are guided by variables that answer two common sense user-asked questions when dealing with an interruption: (a) can I be interrupted now, and (b) do I want to be interrupted? (see Figure 9) The first deals with issues of interruptibility and receptivity to an interruption and is strongly focused on interruption research. The second, with privacy related aspects that influence the users’ desire to have control and awareness over privacy decisions.

As such, a wide range of possibilities are covered so that users can better personalize their own agent-based IoT systems. The fact that this set of variables was not extracted from a single experiment, but through observation of several and diverse literature, affords it a high generality. However, this is only an initial exploration of relevant concepts and it has not been tested in the scope of a real privacy agent making decisions for a user in a real IoT environment.

The work of Ho and Intille (2005) served as this work’s starting point for this set of variables and the recent publication of Turner, Allen and Whitaker (2015), though only focused on reviewing interruptibility research, served as validation that a common vocabulary and set of characteristics is extremely important to this area of research.

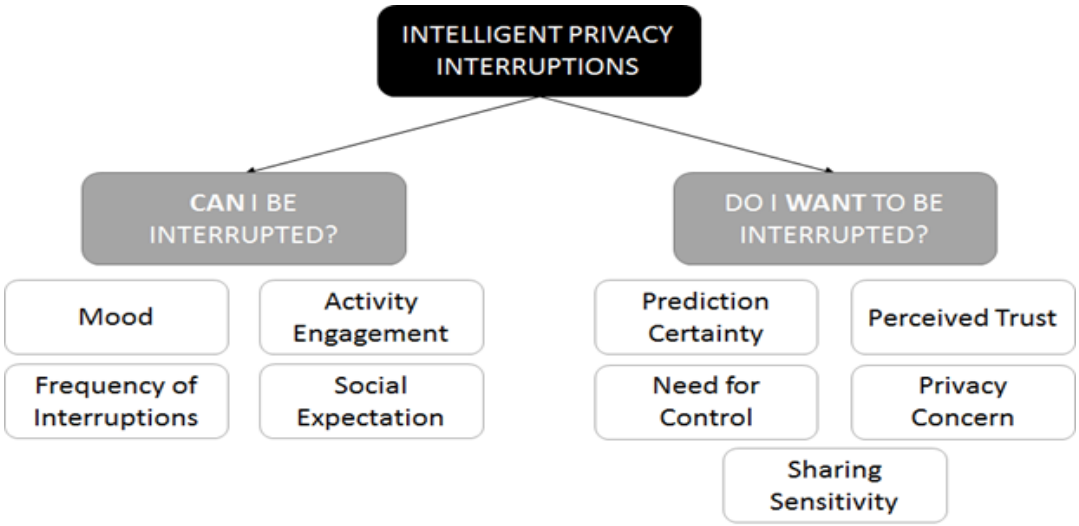


Figure 9. Intelligent Privacy Interruptions

4.2.1 Can I Be Interrupted?

As the question used to categorize the variables in this group shows, these variables are related to aspects of interruptibility and have a bigger focus on interruptions research. These variables are highly contextual and dynamic and are related to the user context (mood and the perception of frequency), activity context (activity engagement), and social context (social engagement). When describing them, we added the privacy perspective and discuss how they might affect and/or be considered in the context of privacy interruptions.

4.2.1.1 Mood

The user's emotional and internal state, here referred as mood, has been considered an influential aspect in a user's interruptibility and availability in several previous works (DABBISH; BAKER, 2003; HO; INTILLE, 2005; OULASVIRTA; SALOVAARA, 2004; PEJOVIC; MUSOLESI, 2014; SARKER et al., 2014). For Dabbish and Baker (2003) the relation is less direct and made through a connection of their observed variable of "interruption threshold" defined as varying in accordance to context and external cues. Oulasvirta and Salovaara (2004) suggested that stress should be considered in intelligent environments when deciding on interruptions. On the other hand, Ho and Intille (2005) and Sarker et al. (2014) mention "emotional state of the user", "affect" and "stress" directly as variables that influence the definition of interruptibility and availability, respectively. Finally, Pejovic and Musolesi (2014) go one step further in their specification and list the set of emotions they considered in their exploration, namely happy, sad, angry, frightened and neutral.

When considering the effects that a person's mood has on daily life activities and as seen in previous literature, it seems reasonable to consider that it will also affect their preference for being interrupted or not. If the user is in a negative mood it is less likely that s/he will interact with an interruption or welcome it, than if his/her state was neutral or positive. On top of this, for privacy-related interruptions the presence of an altered state of mind may lead the user to make a different decision then if his/her mood had been different (CONSOLVO et al., 2005). It might not be in the user's best interest to be interrupted to offer feedback.

4.2.1.2 Frequency of Interruptions

A factor that has been frequently noticed throughout literature is the frequency of interruptions. It has been considered a factor that influences user interruptibility (HO; INTILLE, 2005) as well as one of the challenges considered for privacy feedback (ALMUHIMEDI et al., 2015; PATIL et al., 2015). It may also influence the user's privacy concern over sharing a piece of data (GAUD; DEEN; SILAKARI, 2012; HONG; LANDAY, 2004). When we consider privacy-related interruptions in the context of IoT this becomes an even more important factor because without an intelligent actor to mediate the reception and decision the frequency of interruptions can be superior to what we are used to and feel is acceptable.

The work of Pejovic and Musolesi (2014) hypothesizes that the recent exposure to an interruption will influence and determine the user's frustration. With this in mind, when an agent has to make the decision on whether or not to interrupt a user for input, it should be important for it to factor in the time since the last interruption and if a new interruption will not be perceived as negative because of that.

4.2.1.3 Activity Engagement

One of the most complex variables is the user's activity engagement. It represents a combination of two contexts that have been identified as relevant factors in previous literature: the social and cognitive contexts (FISCHER et al., 2010; GRANDHI; JONES, 2010). This work combines these two aspects that have been previously considered distinct (KERN et al., 2004) since reports of similar behavior towards notifications happened in situations where there was a high workload but low social engagement and when there was a high social engagement but low workload (CONSOLVO et al., 2005).

For this work's consideration of activity engagement the user's cognitive context, which was defined to "encompass the interruptee's cognitive level of involvement in tasks and how it affects task performances" (GRANDHI; JONES, 2010), is adequate and adopted. In fact, the user's cognitive context is one of the factors that has been thoroughly considered in the literature of user interruptibility (HO; INTILLE, 2005; OULASVIRTA; SALOVAARA, 2004; PEJOVIC; MUSOLESI; MEHROTRA, 2015).

However, the definition of the user's social context in the sense that it "encompass the interruptee" physical environment as understood in a social sense", which relates to the place

the user is in, the people around him/her and the nature of the social task engaged (GRANDHI; JONES, 2010), is more related to a different variable considered in this work: social expectation. For this reason in the definition of the activity engagement variable we consider from the social context only the social participation of the user in his/her current task, i.e. his/her social engagement (HARR; KAPTELININ, 2012; HO; INTILLE, 2005).

The activity engagement variable is related to what has been previously considered as interruption threshold (DABBISH; BAKER, 2003; ERCOLINI; KOKAR, 1997) which relates to the current activity type (SARKER et al., 2014). It is interesting to notice that Ercolini and Kokar (1997) four levels of interruptibility threshold, namely bored, flexible, busy, do-not-disturb, can be combined to the four levels of activity engagement, when we consider both workload and social engagement as having either a high or low level (see Figure 10).

Lastly, it is important to point that in InterruptMe (PEJOVIC; MUSOLESI, 2014) one of the factors measured was named “activity engagement”. However, differently from ours, the factors they consider when measuring it are mainly related to the user cognitive context and the aspects of the activity without consideration for the social involvement the user may have[33].

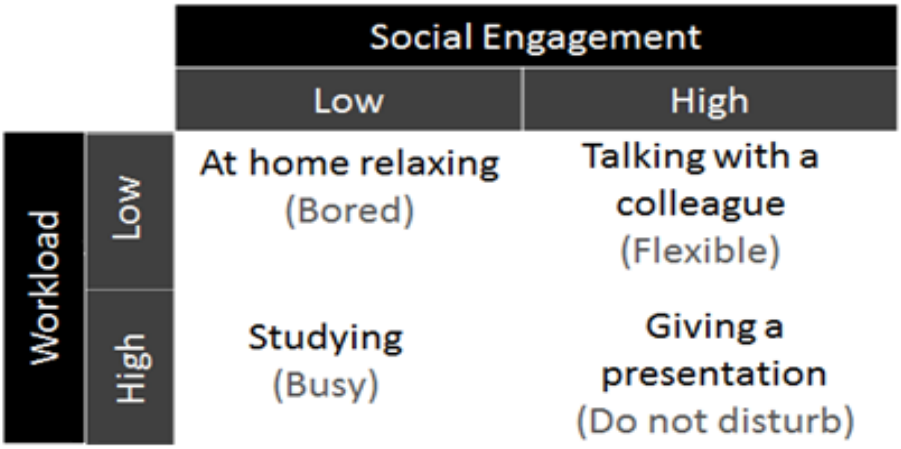


Figure 10. Activity Engagement representation considering the combination of the two variables that compose it: social engagement and workload. [34]

[33] Features considered: Descriptive activity: “Work related”, “Leisure”, or “Maintenance”. How important is the activity? How interesting is the activity? How challenging is the activity? How skilled is the user at the activity? How concentrated the user is? User’s desire to do something else.

[34] It is important to notice that the definition of where an activity fits in this matrix and the associated threshold level from *(ERCOLINI; KOKAR, 1997)* may vary from user to user.

4.2.1.4 Social Expectation

The user's social context (GRANDHI; JONES, 2010) is deeply related to the Social Expectation variable. This variable reflects the known importance that the social environment (i.e. the people around us, how our actions are perceived by them, the social norms associated with a given context, etc.) has on user behavior and decisions.

From the perspective of user interaction with technology, the Technology Acceptance Model (TAM) (DAVIS; BAGOZZI; WARSHAW, 1989) has added the factor of subjective norm since it became apparent through a number of studies that the acceptance of technology seems to be influenced by the views of others (SVENDSEN et al., 2013). The influence of the broad social context includes culture and social norms (BARKHUUS, 2012; BOYLE; GREENBERG, 2005; WESTIN, 1967), the presence and opinions of others (BARKHUUS, 2012) and social interactions (PALLAPA; KUMAR; DAS, 2007). The social context also affects user behavior, decisions and expectations towards privacy, including how much control over data sharing may be desired (LUGER; RODDEN, 2013).

Furthermore, the social context affects the user's interruptibility. Aspects such as the possibility of interrupting others and the social engagement (described in the Activity Engagement variable) have been shown to be important when people are making the decision to interrupt somebody else (HARR; KAPTELININ, 2012). The social surrounding (presence of others), expectation of group behavior (social norms), and organizational and cultural norms have also been considered when examining the effects of interruptions (CONSOLVO et al., 2005; FISCHER et al., 2010; HO; INTILLE, 2005; MEHROTRA et al., 2015a; PEJOVIC; MUSOLESI, 2014).

4.2.2 Do I Want to Be Interrupted?

With a different perspective from the previous variables that dealt with aspects of interruptibility, the variables under this question explore the necessity and desire of the user to be interrupted to make a sharing decision. As such it considers aspects from the data requests perspective (sharing sensitivity), the system perspective (prediction certainty), user characteristics (need for control and privacy concern), as well as user and system dependent characteristics (perceived trust).

4.2.2.1 Prediction Certainty

Unlike the system's accuracy, i.e. the history of right decisions, which is an evolving variable, prediction certainty relates to the decision for an interaction. Throughout choreographed solutions it is the main variable considered when deciding to interrupt the user for further input. This is known as uncertainty sampling and is a common way of selecting when to query an "oracle". Some variations of this concept exist. For example, Fisher and Simmons (2011) consider a density-weighted version of uncertainty sampling, where the queries occur for data points that inform a higher number of future decisions. But even though this is a very important variable to be considered, by itself it is not enough.

The prediction certainty is defined solely by the system and relates to the system's ability to correctly infer the user's privacy preferences. Depending on the user and context its role may vary greatly. The user may not require a high level of certainty in exchange for a lower level of interruption in a social context that does not afford interruptions. Or if the user is in a situation where s/he could be interrupted without any incurred burden, s/he may desire a higher level of certainty on the prediction, since s/he could make the decision by him/herself with complete certainty. It is hard to consider this variable by itself because when considered in isolation it is not expressive of the user's preferences, only of the system's needs. However, it can be used as an indicator that an interruption may be *necessary* whenever it is below a certain threshold.

4.2.2.2 Perceived Trust

Trust is a variable that has long been studied in human-computer interaction. It is an important aspect of technology acceptance as the user should always trust the system being used. In particular, when considering automated systems in which the automated task is one the user can perform in a manual manner, the influence of trust increases significantly (HOFF; BASHIR, 2013) and, as highlighted by Bainbridge (1983), the perception of the computer's abilities in automated systems influences the user's decision to allow the automation to continue or to override it.

Trust is a complex notion with many variables influencing how much of it the user bestows on a system. While a theoretical model of trust may consider dispositional, situational and learned trust, where each of these subcategories of trust are influenced by the user, environment and system (HOFF; BASHIR, 2013), in this work we do not aim at defining what

influences trust and how to quantify it. Trust is viewed as a subjective user-dependent and dynamic variable which is perceived by the user in the moment of the interaction. As TAM, the users' perception is what we consider for the evaluation of this variable.

Considering one's behavior in relation to trust in interpersonal relationships it is common that whenever a person does not trust someone s/he feels more ill at ease at letting this person make decisions on her/his behalf that might affect his/her life. However, if we trust someone we may "trust them with our lives". For this reason, the agent must monitor aspects that may influence the user's trust on it, such as the user's overall trust on technology, how often the user has checked the decision history and/or system accuracy, and account for its effect on the user's preferences when making the decisions of interrupting or not the user for further input.

4.2.2.3 Need for control

Control, as trust, is an important aspect of human-computer interaction. Its lack increases anxiety and stress when dealing with computational systems. Moreover, the perceived control over the interrupting device (authority level) has been identified by Ho and Intille (2005) as a factor that influences the user's perceived burden of the interruption. It is easy to see control as a system characteristic that is outside of the user's influence. Nevertheless, control is also a "personality trait that reflects individual differences in the appreciation of choice in life" (HEIJDEN, 2003).

Some people have a stronger desire and need for control than others. Schnorf, Ortlieb and Sharma (2014) classified users as "care" and "don't care" users in accordance to the questionnaire that examined the user's desire for control and transparency in the context of inferred user interest models and how these variables influence trust in a given company. However, they considered control and transparency as binary variables which we believe, given the options available in the questionnaire, is not an accurate portrayal of reality. While some users expressed no desire to have any sort of control over their information, the users who did care could be divided into those who care for direct control, and those who care for knowledge control. Previous research has identified that there is a variety of nuances of desire to exert control, in particular in interactions with an agent (SCHIAFFINO; AMANDI, 2004).

The need for control is intrinsically associated with a particular user and it may be influenced by different factors, such as personality (HEIJDEN, 2003) and experience with

technology (SCHIAFFINO; AMANDI, 2004). However, this variable seems to have a logically higher influence on the user's desire to (not) be interrupted by a decision-making agent and has to be taken into consideration when making such decision.

4.2.2.4 User's privacy concern

Moving on to variables that are directly related to privacy, the user's privacy concerns should play a significant role in determining not only the disclose decision when considering the context of a privacy-related decision making agent, but on whether the user should be interrupted for further input. Previous work has tried to identify scales to measure individuals privacy concerns (KUMARAGURU; CRANOR, 2005; MALHOTRA; KIM; AGARWAL, 2004). They found that people have varied levels of privacy concerns and, while it does not directly correlate to privacy behavior[35], understanding that there are different levels and motivations behind how a person perceives privacy is a variable important to be aware of.

A high-level categorization of privacy concerns is: fundamentalist, pragmatist, and unconcerned (KUMARAGURU; CRANOR, 2005). A fundamentalist is generally distrustful, worried about accuracy of computerized information and additional uses of this information. They tend to prefer privacy controls over consumer-service benefits. This can be extended that they will prefer to be interrupted in most situations and that variables as privacy sensitivity and perceived trust will play a more significant role than other variables. A pragmatist weighs the pros and cons and, in consumer matters, would want the opportunity to decide to opt out of uses of their personal data. Although, as a fundamentalist, the pragmatists do want some level of control over their data and it is possible that other factors, such as social context, will play a more significant role in opting for being interrupted for further input or not. Finally, the unconcerned are generally trusting and do not mind losing privacy claims to obtain benefits from interactions. The people who fall into the latter category will most likely have an overall preference of low interruption and a high level of trust on the system; letting it perform in a more automated way.

[35] See Attitude/Behavior Dichotomy.

Because of the more static aspect of this variable and the influence it may have on the weight given to other variables, privacy concern could be used to inform the behavior in situations not previously specified on top of influencing the decision to interrupt or not.

4.2.2.5 Sharing Sensitivity

The last variable considered in the 'want to be interrupted' category is an important factor that influences how much a user will accept and want an interruption: sharing sensitivity. In interruption literature the perceived utility and importance of the content of the interruption has been highlighted and the observation is that interruptions that provide useful information are viewed more positively (BARKHUUS; DEY, 2003; DABBISH; BAKER, 2003; HO; INTILLE, 2005; MEHROTRA et al., 2015a; PEJOVIC; MUSOLESI, 2014). In the context of privacy, this balancing of benefits and costs has been noticed when considering the exchange of information for rewards: as long as the reward outweighs the cost of sharing, it seems rational to do so (ACQUISTI, 2013).

In this work, the content of the interruption is the presentation of a data access request by an IoT device. Such content should always be considered important and worthy of triggering an interruption; however, some requests can have a higher risk or possible costs than others and be perceived as more important to be dealt with personally. For this reason, this work adapted the commonly considered utility and importance of the interruption to the sensitivity of granting access to the requested data. The agent must evaluate if the user finds a request to be sensitive to decide if it should interrupt the user for further information.

This work associates that higher privacy concerns when sharing data within a certain context indicates a higher sharing sensitivity in that context. A literature review related to user's privacy concern when sharing data has elicited many variables, as can be seen in Appendix B. These variables were categorized as aspects of the 5W1H framework for contextual information (KIM; SON; BAIK, 2012), namely *what, who, why, when, where, how*; with the addition of a *context* variable, which is further explain in the appendix.

Because the broader variables *when*, *where* and *context* can be implicitly and better identified on the go by the user and because some of these variables have been shown to have a higher impact on the user's concern when sharing data than other ones (CONSOLVO et al.,

2005; COUGHLAN et al., 2013; LEDERER; MANKOFF; DEY, 2003a; MURAKAMI, 2004[36] *apud* PALLAPA; KUMAR; DAS, 2007), the subset of *who* is requesting the data, *why* they need it and *what* they need is what is used to classify the sharing sensitivity of a situation. Not surprisingly this subset is what it is commonly used in mobile platforms when giving privacy notifications and requesting consent for their applications (Figure 11).

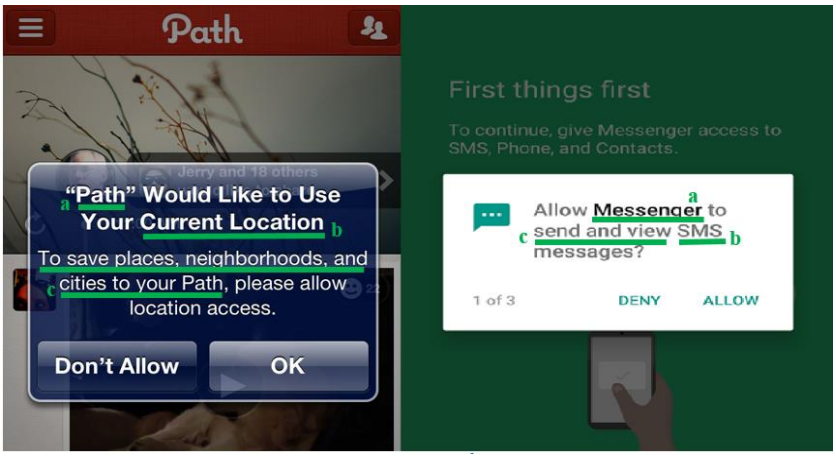


Figure 11. [37] *On the left: an iOS 6 permission request notification. On the right: Android 6.0 permission request notification. Both identify: (a) the app requesting information (who); (b) what data they need access to (what); and, (c) why they need access to it (why)*

It is important to notice that the *how* variable and its aspects are extremely relevant when informing the privacy scope of a sharing decision. However, the choice to not consider it was also because it may confuse people with low computer literacy, who may be more disturbed than informed by it. Further work is necessary to explore the benefits of adding this variable and if it outweighs the cons.

4.2.3 Variables not Selected

Some factors found throughout literature that may influence the desire to be interrupted, the user's interruptibility, or even variables previously described, have not been selected to be part of this work. However, because they have been already identified as important in their own niche, this subsection covers them and explains why they were not considered.

---

[36] Murakami, Y., (2004) Legal issues for realizing ubiquitous information society, SICE Annual Conference Vol. 2, 1751 – 1755

[37] Image obtained from: http://goo.gl/7NoLXO on November 19th, 2015.

One factor that has been found to influence the user interruptibility and that should be defined by the user as to be set in an appropriate way is the *modality of the interruption* (ALMUHIMEDI et al., 2015; HO; INTILLE, 2005; PATIL et al., 2015). In fact, it was also used to justify the need to differentiate personal and social interruptibility, since when the interruption mode is non-obtrusive (vibration) these two aspects do not correlate. However, this result does not hold for when the mode is obtrusive (audible ring) (KERN et al., 2004) and given the context of this work of delivering privacy-related interruptions it is not considered as a relevant variable. This is because for this context the interruption must always be salient enough to garner the user's attention – falling into the situation where personal and social interruptibility correlate, which further justifies the need the activity engagement variable – and because of this necessity of always gathering user attention the obtrusiveness of the mode is constant.

Moreover, even though one of the main factors that make interruptions disruptive is the interrupting task *complexity* and *duration* (BORST; TAATGEN; VAN RIJN, 2015) and that this has been considered as a factor that influences the user's interruptibility (ERCOLINI; KOKAR, 1997; HO; INTILLE, 2005) this is not a factor this work considers when deciding when to interrupt or not the user for further input. This is because the complexity of making a privacy decision, which is the task the user must perform in case s/he is interrupted by a choreographed solution in this work's context, is somewhat constant even though it is high. Albeit there are some situations that may have a higher complexity and associated higher time to decide on, we consider that this difference between situations becomes less significant when faced with the complex and multi-dimensional issue that is making a privacy decision, where every decision has a high complexity. We leave the work of making this task easier and faster to be performed by other researchers because it would not fit within the scope of this work.

Finally, there has been a variety of research that has tried to tie aspects important to our research to personality factors. However, the inconclusiveness of research that associates personality factors [38] to aspects such as privacy concern (BUSCH; HOCHLEITNER; TSCHELIGI, 2014) and the influence that particular types of technology and situations can have

[38] It is important to note that while individual preferences and behaviors are important, the point being made here is that the user of personality models that consider factors and/or traits, such as openness, extroversion and neuroticism, have been inconclusive in determining preferences and behaviors and, for this reason, will not be used.

when trying to establish relationships between different factors and personality traits (SVENDSEN et al., 2013) leads us to believe that using a personality trait model, such as the Big Five (MCCRAE; JOHN, 1992) might lead to inclusive results and only add noise to future research based on this work.

4.3 Summary

In this chapter the variables for Intelligent Privacy Interruptions were presented. This set of variables was extracted and collected from scattered and diverse privacy and interruption literature. This affords it a high generality since in different contexts and groups of users they were observed as being relevant variables. At the same time, however, it becomes necessary to have its validity verified in the context of an intelligent privacy decision-making agent for the Internet of Things. The results of initial validations are discussed in the following chapters.

Related to interruptions literature, the variables were classified depending if the users **can** be interrupted (interruptibility) and if they **want** to be interrupted (receptivity). However, while receptivity in interruptions mostly deals with the content of the interruption, in this work the content (privacy sensitivity) was considered in combination with system aspects (prediction certainty) and user characteristics (need for control, privacy concern, perceived trust). This is not a complete review of variables that could influence the users' desire to be interrupted to make the privacy decision themselves or to delegate this control to an agent. In fact, some factors that have been previously considered were purposefully not thought as relevant variables because they were either a source of noise or not applicable for this context. The goal of this chapter was to identify a minimal and significant subset of variables so that it can later be used to inform the creation of a model for intelligent privacy interruptions. This was done to satisfy the first step to fulfilling this thesis main objective.

Chapter 5

Online Survey

The set of variables presented on Chapter IV was extracted from diverse privacy and interruption literature, affording it a high generality. At the same time, however, it becomes necessary to have its validity verified in the context of an intelligent privacy decision-making agent for the Internet of Things. As an initial step in doing so an online survey (in Portuguese) was created. It presents a description of a scenario of a day in the Internet of Things and the concept of an intelligent privacy agent capable of predicting their preference to share (or not) the requested data. The participants had to express their opinion on whether or not each of the individual variables would influence their preference of being interrupted to make a data sharing decision, or delegating this control over to the intelligent agent. The survey was approved by our institution's Internal Review Board.

5.1 Objectives

This survey had two main objectives. The first one was to examine how people expected to be influenced by the different variables presented in Chapter IV. The second was to verify if their preferences could be used to group participants to identify preference profiles.

For the first objective, since the variables were obtained from results in previous literature it was expected that there would be a significant agreement amongst the participants. However, because the variables were extracted from literature not directly related to the context at hand and because people naturally have different opinions and views, it was not expected that any variable have a high agreement amongst participants. For the second objective, even though people are different, it was expected that there would be 3 major groups with approximate equal relevance. This expectation arose from the fact that we had two groups of variables (**can** and **want**) and so, people could be grouped as:

- those who thought that variables related to if they **can** be interrupted were the most relevant;
- those who thought that variables related to if they would **want** to be interrupted were the most relevant; or,
- those who had mixed opinions, i.e. did not present a more distinct preference to either variable grouping.

It was also expected that there would be some participants who rated all variables as relevant, those who had no opinion about all of them, and those who thought none would be relevant. However, they were not thought to be frequent enough to be considered as a major factor.

As secondary goals it was desired to identify base values for some of the variables (e.g. desire for control and privacy concern) based on the Brazilian population and to verify if there were interesting correlations among the variables.

5.2 Survey Design

As an initial validation of the selected variables it was desired to verify if people would generally agree to what each variable stood for. To achieve this, an online survey format was chosen because: (a) it permits an easier and faster dissemination so that answers are obtained from a broader audience; (b) it allows that participants answer it in their own time and pace, without the pressure of having someone from the research group present; and, (c) it makes the computer aided data analysis easier and with less chance of input errors.

With this survey, each participant was initially presented with a small text explaining the purpose of the research, the researcher contact address, and general guidance about the survey. After reading this and agreeing to share the answers for the research purposes stated in the text, the participant started answering questions arranged into different sections: demographics, personal characteristics, and preferences. The survey can be found in Appendix B.

5.2.1 Demographics

In this section participants answered common demographic questions. The data collected was related to the participant’s nationality, age, gender, computer literacy,

computer usage, and hours using computers daily. Because culture influence privacy perspectives (UR; WANG, 2013), nationality was collected with the purpose of being a control variable. Age served both as a demographic variable and as a control variable. All responses for non-Brazilians and/or minors (under 18 years old) were discarded.

5.2.2 Personal Characteristics

In this section participants answered questions related to their opinions and behaviors regarding technology trust, acceptance of interruptions, privacy, desirability for control, and personality. The first two subsections, *trust* and *interruptions*, were completely generated by the research team. The subsection about *privacy* was divided into privacy behaviors (obtained and translated from question 45 from Leon et al. (2013)) and privacy concern (obtained and translated from the Privacy Segmentation Index reported by Kumaraguru and Cranor (2005)). The *desirability for control* subsection was a subset of statements extracted from Burger and Cooper (1979) Desirability for Control Scale. Finally, for the *personality* subsection a subset of statements from Goldberg (1992) Big Five Factor Markers was used.[39]

5.2.2.1 Trust

In order to analyze how much the participants trusted technology, they stated their agreement (1-5, completely disagree-completely agree) to each of the following statements.

- "I have files and/or important documents on my computer/tablet/cellphone without backup."
- "I rely on my cellphone/tablet/computer to be reminded of important events."
- "The more technological something is, the more concerned I become that something will go wrong."
- "I do not trust in technology in general."

The first two statements were meant to identify trusting behaviors that people may display with technology. The last two were used to detect trusting opinions.

[39] The statements were obtained from http://ipip.ori.org/newMultipleconstructs.htm > Goldberg's (1992) Big-Five Factor Markers > Scoring Keys on November, 2015.

5.2.2.2 Interruptions

To understand a little better how much the participants accepted interruptions, they were asked to mark their agreement (1-5, completely disagree-completely agree) with the following two statements. They were selected because they would indicate a low acceptance threshold for interruptions and both behaviors have been previously observed in interruptions literature.

- “I do not like to be interrupted when focused”
- “I shut off the notifications on my phone/tablet/computer at every opportunity.”

5.2.2.3 Privacy Behavior and Privacy Concern

In the Privacy section in Chapter 2 the Attitude/Behavior Dichotomy was presented. This dichotomy is related to the fact that people believe they would behave in a certain way and have an opinion, or attitude, towards privacy that does not match their actual behavior. Because of this, the survey contained both a section that asked people about their actual past behaviors as well as one that measured their attitude and opinions towards privacy.

In the first section related to privacy, the participants had to answer if they had previously engaged in one of the following behaviors: refusing to share information online because it was not necessary or too personal; deciding not to use a website/app/software for being unsure on how the information being collected would be used; reading the privacy policy of a website/app/software; clearing cookies from the browser; and, turning on the “do not track” setting of the browser.

In the second section the participants answered Westin’s Privacy Segmentation Index (PSI), which is composed of three statements with which the participants can pick one of four options (from Strongly Disagree to Strongly Agree, 1 to 4, without a neutral option). The statements are:

- “Consumers have lost all control over how personal information is collected and used by companies.”
- “Most businesses handle the personal information they collect about consumers in a proper and confidential way.”
- “Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.”

These three statements are used to classify the respondent in one of the three categories: fundamentalist, pragmatist, or unconcerned. A respondent is classified as a Fundamentalist if s/he agrees with the first statement and disagrees with second and third; Unconcerned if s/he disagrees with the first statement and agrees with the second and third; and, Pragmatist if s/he fits any other combination of answers.

5.2.2.4 Desirability for Control

In the Desirability for Control section, a subset of 10 statements was selected from Burger and Cooper (1979) Desirability for Control Scale. This selection was done in order to keep an acceptable length for the survey. The selection criteria were to pick the statements that were closer to the focus of this thesis or presented a broad view of desire for control without being too repetitive. The statements selected were:

- "I prefer a job where I have a lot of control over what I do and when I do it."
- "I enjoy political participation because I want to have as much of a say in running government as possible."
- "I try to avoid situations where someone else tells me what to do."
- "Others usually know what is best for me."
- "I enjoy making my own decisions."
- "I enjoy having control over my own decisions."
- "I consider myself to be generally more capable of handling situations than others are."
- "I wish I could push many of life's daily decisions off on someone else."
- "There are many situations in which I would prefer only one choice rather than having to make a decision."
- "I like to wait and see if someone else is going to solve a problem so that I don't have to be bothered by it."

The second statement (political participation) is one that seems out of place when compared to the focus of this study. However, it represents an overall desire for control over impacting outcomes, as well as a higher abstraction level for decision control and future risks of exerting, or not, such control (as in privacy decisions).

5.2.2.5 Personality

As mentioned, personality was added as a verification of its relevance to the previously defined set of variables. The tool used to collect personality data was a subset of Goldberg (1992) Big Five Factor Markers. However, given the lack of verification for the subset selected and the inherent complexity of generating valid tools to examine personality, the results obtained will not be analyzed in this work.

5.2.3 *Internet of Things Characterization and Preferences*

In this final section the participant would read the excerpt "A day in the Internet of Things" presented in Chapter 1 as a way to familiarize him/herself with what is and what can be expected from the Internet of Things. Following this, a brief description of the two motivating issues of this thesis, privacy and interruptions, was shown and the proposed solution of a privacy agent was described. The last act of participation involved answering if s/he thought each individual variable would influence, or not, his/her desire to be interrupted to make the decision or to delegate this decision to the agent. There was also an open text question. For the multiple choice questions, the participant could say that s/he did not know or have an opinion.

5.3 Data Collection

The survey was available for 6 weeks[40] through Google Forms and the link was distributed using social media and mailing lists. There were two moments in which the link was shared. The first one occurred right at the end of the semester and before the start of the summer vacation. The second one was after the holiday season had past. This second moment gave those that were too occupied during the end of the semester the opportunity to participate in the research. There was no financial or any other tangible benefit given to those who participated. The full survey can be found in appendix B.

[40] December 3rd, 2015 through January 12th, 2016.

5.4 Results and Analysis

Over the course of 6 weeks, 262 responses to the survey were collected. But because we only considered the ones given with direct consent of being used for research purposes, from Brazilians (to control cultural differences), and from participants over 18 years old (legal age in Brazil), 12 of these responses were discarded (7 without explicit consent, 2 from non-Brazilians and 3 from minors).

5.4.1 ***Demographics***

As can be seen on Table 2, gender was well distributed within the participants (42.00% female and 58.00% male). However, age was not. There was a majority of participants under 35 years old, with 44.40% being in the 18 to 25 years old bracket, and 35.20% in the 26 to 35 years old bracket.

Similarly, for computer literacy and daily computer use, a majority of participants (56.40% for both) declared themselves as computer experts (described as being able to program new functionalities in a computer) and stated that they spend more than 8 hours on the computer per day. Also, no participant self-declared as having a low computer literacy (described in the survey as needing help to use computer, tablets, smartphones, etc.). Positive responses related to computer use is generally over 90%, with the exceptions being “work” (85.60%) and online banking (77.20%).

Table 2. Demographic values from participants who answered the online survey

	N = 250	**%**
Gender		
Female	105	42.00
Male	145	58.00
Age		
18 - 25 years	111	44.40
26 - 35 years	88	35.20
36 - 50 years	24	9.60
50+ years	27	10.80
Computer literacy		
Expert	141	56.40
High	71	28.40
Medium	38	15.20
Low	-	-
Daily Computer Use		
Less than 2 hours	7	2.80
2 and 6 hours	49	19.60
6 and 8 hours	53	21.20
More than 8 hours	141	56.40
Computer Use		
E-mails	247	98.80
Study	241	96.40
News	240	96.00
Social Networking	235	94.00
Entertainment	233	93.20
Shopping	227	90.80
Work	214	85.60
Online Banking	193	77.20
Others	12	4.80

5.4.2 ***Personal Characteristics***

The personal characteristics results were divided into smaller groups to facilitate data representation.

5.4.2.1 *Trust*

The participants were well divided between agreeing (44.00%) and disagreeing (48.40%) with the statement that they had important documents without back-up on technological devices (Table 3, Trust #1). However, there was a clear trend that showed that people rely on technological devices to remind of important events (Trust #2, 68.60% agreed, 16.40% disagreed); that they don't worry more when something is more technological (Trust #3, 59.60% disagreed, 16.40% agreed); and, that they don't distrust technology in general (Trust #4, 81.20% disagreed, 4.40% agreed).

Table 3. Distribution of agreement with each of the four trust-related statements

Agreement	**Trust #1**		**Trust #2**		**Trust #3**		**Trust #4**	
N = 250	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Strongly disagree	49	19.60	18	7.20	61	24.40	102	40.80
Disagree	72	28.80	23	9.20	88	35.20	101	40.40
Neutral	19	7.60	37	14.80	60	24.00	36	14.40
Agree	59	23.60	97	38.80	33	13.20	9	3.60
Strongly agree	51	20.40	75	30.00	8	3.20	2	0.80

To analyze individual answers, the overall trust was calculated as the sum of the values for the first two answers, which had a positive influence on trust, and the subtraction of the last two answers, which had a negative influence on trust (see section 5.2.2.1 for the statements). This calculation is represented in Eq. I. This way it is possible to see the combination effect of each statement per person (Figure 12).

$$T_i = NoBackUp_i + Reminder_i - Worry_i - NoTrust_i \quad (Eq.I)$$

where,

T_i = Overall trust score for the i^{th} participant, $i \in [1, 250]$
$NoBackUp_i$ = Answer of the i^{th} participant, $i \in [1, 250]$, for the Trust #1 statement.
$Reminder_i$ = Answer of the i^{th} participant, $i \in [1, 250]$, for the Trust #2 statement.
$Worry_i$ = Answer of the i^{th} participant, $i \in [1, 250]$, for the Trust #3 statement.
$NoTrust_i$ = Answer of the i^{th} participant, $i \in [1, 250]$, for the Trust #4 statement.

With this equation an end value of zero represented a neutral consideration of trust, that is, the person neither trusted technology too much or for too many things nor was the person too distrustful of it. Analogously, positive values represented a more trusting relationship and negative values a more distrusting relationship. Given the respective values of 1 and 5 attributed to “strongly disagree” and “strongly agree” and Eq. I, the maximum value for trust would be 8 and the minimum would be -8.

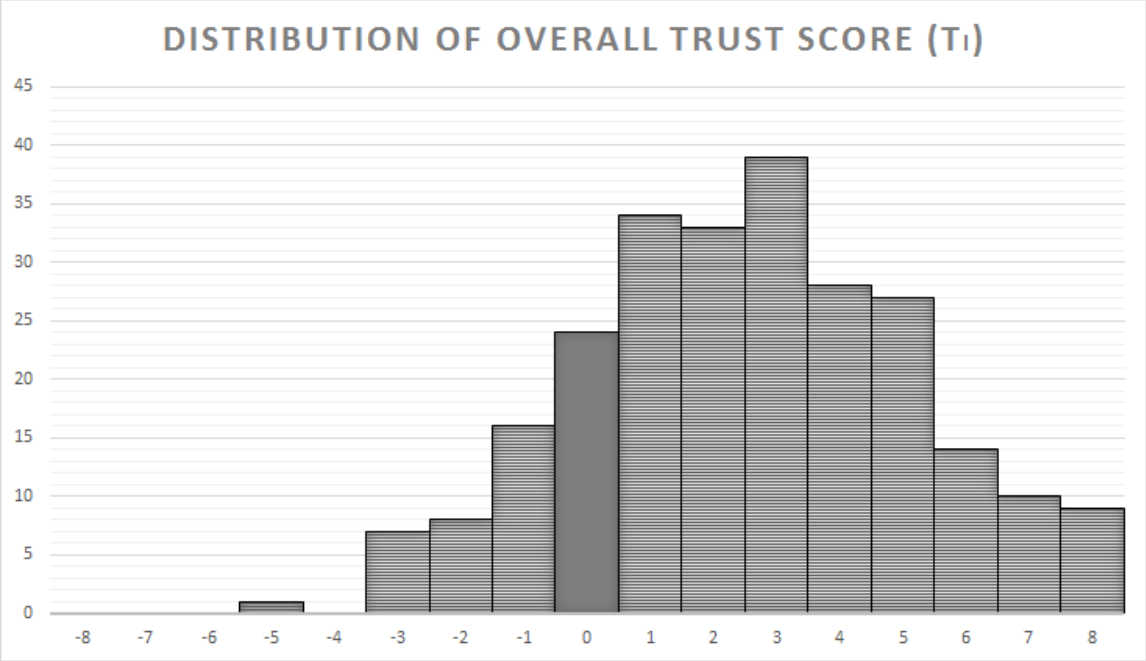


Figure 12. Distribution of the overall trust scores considering eq. I. The highlighted bar has equal values for agreeing with trust-adding sentences and trust-subtracting sentences. Showing a neutral level of trust.

5.4.2.2 Interruptions

Analyzing the overall response to each interruption statement (Table 4), even though the majority of participants agreed that they do not like to be interrupted when focused (Interruptions #1, 70.80%), there was no clear consensus as to shutting off the notifications whenever possible (Interruptions #2).

Table 4. Distribution of agreement with each of the two interruption-related statements

Agreement	**Interruptions #1**		**Interruptions #2**	
N = 250	**N**	**%**	**N**	**%**
Strongly disagree	-	-	23	9.20
Disagree	7	2.80	70	28.00
Neutral	66	26.40	49	19.60
Agree	108	43.20	73	29.20
Strongly agree	69	27.60	35	14.00

Furthermore, by analyzing individual responses and comparing the agreement between both statements, there was not a clear direct connection to be found between not wanting to be interrupted and removing sources of possible interruptions whenever possible. For example, it would be expected that a person who does not like to be interrupted when focused would act to remove notifications whenever possible to avoid this from happening. Yet there were 34 participants who agreed to not liking being interrupted when focused, but disagreed to removing notifications whenever possible.

The expected behavior would be represented on the diagonal of Figure 13 (where the attitude towards interruptions would match the behavior towards them). The pair-wise responses found beneath the diagonal represent situations where there was a higher disliking attitude towards being interrupted when focused than an active behavior towards minimizing sources of disruptions (i.e. notifications). The pair-wise responses found above the diagonal represent situations where the participant more actively removed notifications even though s/he was not necessarily bothered by them.

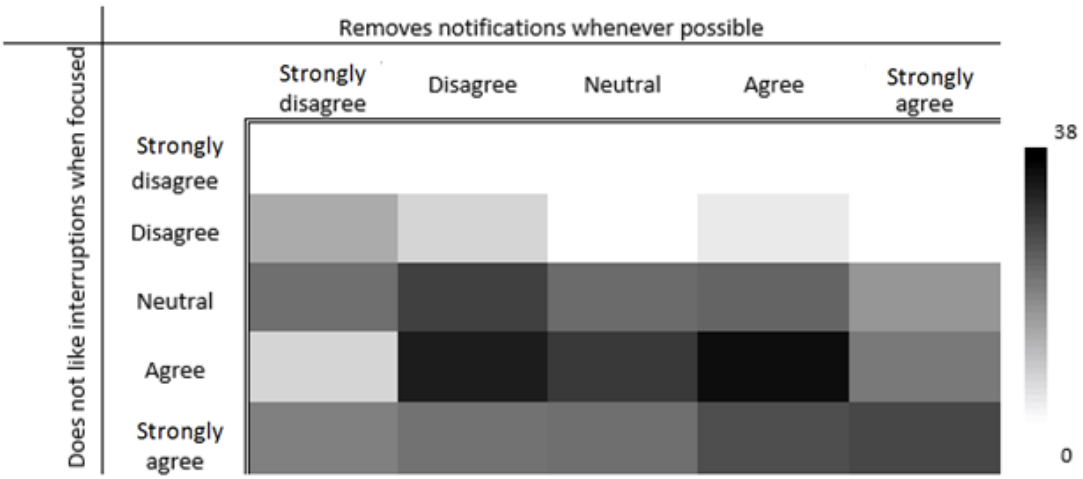


Figure 13. Heat map of the agreement with the interruption-related sentences. The darker the color the higher was the number of participants with that combination (MAX: 38, MIN: 0)

5.4.2.3 *Privacy Behavior and Privacy Concern*

The overall distribution of privacy behaviors (Table 5) shows that passive behaviors, i.e. does not require the user to go out of their way or an extra effort to enact it, had an overall higher engagement than active behaviors. The passive behaviors of refusing to share information and not using a service because of privacy concerns had 84.00% and 86.00% engagement, respectively. The active behaviors of reading privacy policies and turning on the “Do not Track” option in the browser had 48.80% and 46.80% engagement respectively.

The exception was the active behavior of clearing cookies which had a total of 84.00% engagement.

Table 5. Engagement distribution between the five listed privacy protective behaviors. The behaviors are divided as passive and active behaviors.

	N = 250	%
Passive Behavior		
Refused to Share Information	210	84.00
Did Not Use App/Website/…	215	86.00
Active Behavior		
Read Privacy Policy	122	48.80
Cleared Cookies	210	84.00
Turned on “Do Not Track’	117	46.80

Considering the total number of stated behaviors per participant, for the passive behaviors the majority of participants (76.80%) had previously enacted both. This is plausible since they are behaviors that do not require any extra effort. Active behaviors had a more distributed proportion, with one, two, and three active behaviors having an almost equal amount of participants each (29.20%, 32.00% and 28.80%, respectively). Finally, as expected, total number of state behavior behaviors was well distributed for five, four, and three, with the remaining two, one and zero totaling only 19.20% of the participants.

Table 6. Proportion of previously enacted privacy protective behaviors grouped as passive behaviors, active behaviors, and total amount of behaviors.

Passive Behaviors	**N = 250**	**%**
0	17	6.80
1	41	16.40
2	192	76.80
Active Behaviors	**N = 250**	**%**
0	25	10.00
1	73	29.20
2	80	32.00
3	72	28.80

Total Behaviors	**N = 250**	**%**
0	3	1.20
1	14	5.60
2	31	12.40
3	69	27.60
4	74	29.60
5	59	23.60

For the population that participated in the study, 34% were classified as fundamentalists, 7.2% unconcerned, and 58.8% pragmatists. Comparing to the results of Westin’s 2001 survey with U.S. citizens there is a difference of +9% of participants classified as fundamentalists and a -12.8% difference of participants classified as unconcerned. This could be a population, cultural, or temporal difference. It is important to note that from 2001

to 2016 there's been an increase in privacy related news (especially after the Snowden revelations), which could be responsible for this change.

Table 7. Privacy concern comparative table between this work and the results reported in (KUMARAGURU; CRANOR, 2005)

	Westin 2001 (U.S. Citizens)	**This work (Brazilian Citizens)**	
Fundamentalists	25%	34.00%	85
Unconcerned	20%	7.20%	18
Pragmatists	55%	58.80%	147

5.4.2.4 *Desirability for Control*

Analyzing the overall response to each desirability for control statement (Figure 14), with the necessary inversions accounted, for the group that participated in the online survey there is a trend to desire more control, i.e. all average values were above the neutral line (3). When considering desirability for control as a whole, that is, by adding up all of the individual responses with the necessary inversions already made[41] (Eq. II), this trend is also visible (M: 38.43, SD: 4.66).

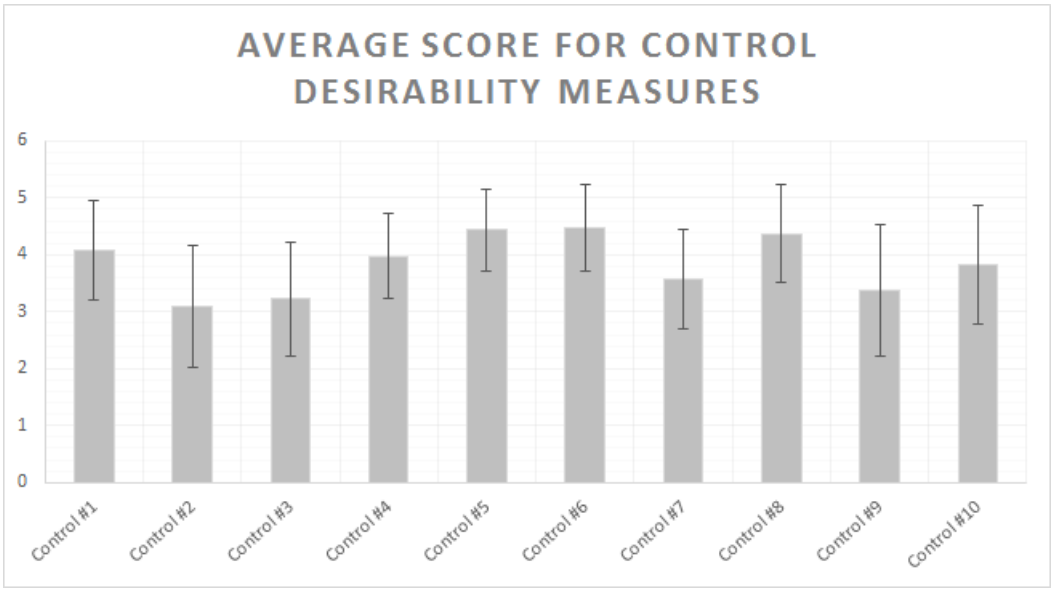


Figure 14. Average scores and standard deviations for individual desirability for control measures

However, the standard deviation for the individual responses and the difference between the maximum value obtained (48 out of 50) and the minimum (20 out of 50) show

[41] The inversions are done based on statements that had negative influence on desirability for control. As such, if a value of 5 (Completely agree) was selected for a negative statement, the inversion would give it a value of 1.

that the answers can be scattered. To understand how the distribution of the desirability of control looks like, the distribution of responses considering their overall value is shown in Figure 15 demonstrating that this group had a medium to high need for control.

$$DC_i = \sum_{1}^{10} Control_{ki} \quad (Eq.\ II)$$

where,

DC_i = overall desirability of control for the i^{th} participant, i ∈ [1, 250]

$Control_{ki}$ = Answer of the i^{th} participant, i ∈ [1, 250], for the Control #k statement, k ∈ [1, 10].

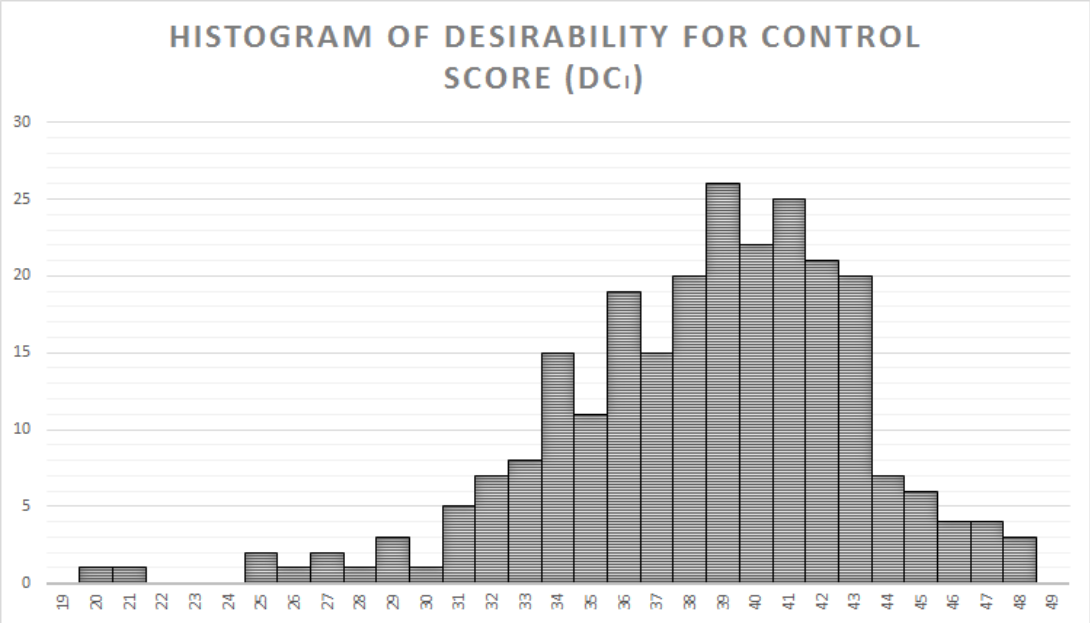


Figure 15. Distribution of the scores for desirability for control

5.4.3 Preferences

For the variables relevance characterization, the user could say each would influence (I), not influence (NI) his/her preference to accept the interruption or prefer to delegate, or that s/he was unsure (NS) of the effect it would have. Considering the overall number of possibilities (2500, 250 participants * 10 variables), the results contained 176 marked as “not sure”, 533 marked as “no influence”, and 1791 marked as “influence”. For the individual variables, the results from this analysis can be seen in Table 8.

On the high end of the overall agreement that a variable would influence the participant’s decision, there was a tie between Sharing Sensitivity and Frequency (of

Interruptions). On the low end the variable Social Expectation had the least percentage of agreement that it would influence the participant's decision (44.00%). Interestingly it also had the highest for "no influence" (12.80%) and an almost equal split between the "influence" (I, 44.00%) and the "not sure" (NS, 43.20%) options.

Table 8. Values for each variable (Activity Engagement was divided in Social Engagement and Workload). Variables in grey represent the ones related to the question "Can I be interrupted" (interruptibility variables). Variables in white represent the ones related to the question "Do I want to be interrupted" (receptivity variables).

VARIABLE	I		NI		NS	
	N=250	%	N=250	%	N=250	%
Sharing Sensitivity	212	84.80	10	4.00	28	11.20
Frequency	212	84.80	13	5.20	25	10.00
Trust	198	79.20	16	6.40	36	14.40
Workload	197	78.80	10	4.00	43	17.20
Privacy Concern	193	77.20	16	6.40	41	16.40
Mood	185	74.00	11	4.40	54	21.60
Certainty	175	70.00	28	11.20	47	18.80
Need for Control	171	68.40	16	6.40	63	25.20
Social Engagement	170	68.00	16	6.40	64	25.60
Social Expectation	110	44.00	32	12.80	108	43.20

Another variable that had a surprising result was System Certainty. Because it is the variable currently being used by privacy agents as seen in Chapter 3, it was expected that it would have a high frequency of agreement and a low frequency of disagreement of its influence. However, it was the second highest variable for "no influence" (11.20%) and the fourth lowest variable for "influence" (70.00%). This puts it behind Mood, a variable that we expected to have a lower agreement. With the exception of Social Expectation, all other variables had an overall agreement that the literature extracted variables would influence their decision to prefer to be interrupted or to delegate the privacy decision making to an intelligent agent.

When analyzing the answers individually by participants we categorized them into 6 groups. These groups do not take into consideration answers that were marked as "not sure" with the exception of the group that marked everything as unsure.

(I) did not know if it would be influenced by any of the variables (2, 0.80%);

(II) no variable would influence (5, 2.00%);

$$\#WantVariable = \#CanVariables = 0$$

(III) all variables would influence (44, 17.60%);

$$\#WantVariable = \#CanVariables = 5$$

(IV) receptivity variables were more relevant (98, 39.20%)

$$\#WantVariables > \#CanVariables$$

(V) interruptibility variables were more relevant (69, 27.60%).

$$\#WantVariables < \#CanVariables$$

(VI) mixed variables (32, 12.80%).

$$0 < \#WantVariables = \#CanVariables < 5$$

Inside groups (IV) and (V) the distribution of people per difference between the receptivity variables and the interruptibility variables show that the majority in both groups were for the situations where there is only one variable more for each group (Group IV: 63, 64.29%; Group V: 36, 52.17%). Also, there were no cases where the only variables marked as relevant were those related to wanting the interruption and only two cases where this happened for variables related to being able to receive the interruption.

Table 9. Distribution of participants for group IV and group V considering the difference in the amount of variables marked as relevant.

	Group IV		**Group V**	
	N = 98	**%**	**N = 69**	**%**
$\lvert\#WantVariable - \#CanVariables\rvert = 1$	63	64.29	36	52.17
$\lvert\#WantVariable - \#CanVariables\rvert = 2$	20	20.41	25	36.23
$\lvert\#WantVariable - \#CanVariables\rvert = 3$	5	5.10	5	7.25
$\lvert\#WantVariable - \#CanVariables\rvert = 4$	10	10.20	1	1.45
$\lvert\#WantVariable - \#CanVariables\rvert = 5$	0	0.00	2	2.90

5.4.4 Secondary Findings

On top of the results and analysis show above, which limit themselves to the examination of each data type in isolation, in this section some explorations are presented based on the collected data. These are secondary findings that arose during the development of the research and are not the focus of it, for this reason this section will be limited to the presentation and discussion of three of them. They are all related to the issue of characterizing privacy concern.

5.4.4.1 #1 Computers Knowledge Influences the Level of Overall Privacy Concern Over Data Sharing

It was expected that users with a higher level of computer literacy would be significantly more concerned over data sharing and usage (the focus of PSI) because they would be more aware of the issues and difficulties involved.

Table 10. Table comparing the privacy concern characterization obtained from PSI with the classification of computer literacy.

	Fundamentalist		Pragmatist		Unconcerned	
Expert	52	36.9%	80	56.7%	9	6.4%
High	20	28.2%	46	64.8%	5	7%
Medium	13	34.2%	21	55.3%	4	10.5%

However, independently of the level of computer literacy the participant had, the distribution of privacy concern within each computer literacy level tends to be similar (Table 10). There is only a slight variation in these distributions that could indicate a possible relationship between computer literacy and overall privacy concern.

By running a Fisher Exact test run on privacy concern as reported by PSI and self-reported computer literacy, it was not possible to refute the null hypothesis that these two variables are unrelated in this population (p-value = 0.6334).

5.4.4.2 #2 Computer literacy Influences the Number of Privacy Protective Behaviors Taken

It was expected that the participant's knowledge of computer would be related to the number of protective privacy behaviors taken. This is because the privacy behaviors listed vary from being completely independent of computer literacy (e.g. not sharing information or not using a particular app) to being more and more related to it (e.g. deleting cookies and turning on the "Do not track" option in the browser).

On this aspect, a trend seems to be clear: the more a person knows about computers the bigger is the variety of actions that s/he can take to protect his or her privacy. Users who had an expert level of knowledge reported more frequently to have taken 4 and 5 privacy protective actions than those who had a high or medium level of computer literacy. A one-way analysis of variance (ANOVA) compared the number of privacy behaviors for different levels of computer literacy. This test was found to be statistically significant, $F(2) = 18.533$, $p = 3.167e\text{-}8$. However, when measuring the strength of this relationship (eta-squared) the results show that only 13.04% of the variability in number of privacy behavior is associated with computer literacy.

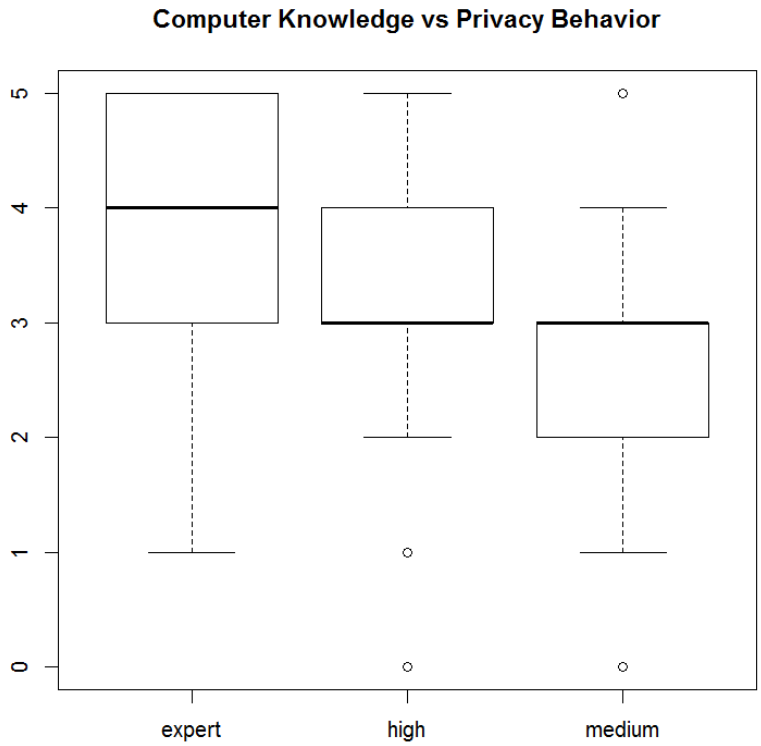


Figure 16. Comparison of computer literacy and number of privacy behaviors reported.

5.4.4.3 #3 The Level of Concern Over Privacy as Measured by Westin's Index Is Not a Good Indicator for Actual Privacy Protecting Behavior

Finally, the last secondary hypothesis stems from the attitude behavior dichotomy (ACQUISTI; GROSSKLAGS, 2005). Because the PSI is based on attitude towards privacy, it is expected that it will not be a good indicator for privacy behavior[42].

If the privacy behaviors were to match the participant's privacy concern it would be expected that Fundamentalists would have a higher number of privacy behaviors i.e. we should find the majority of fundamentalists with 4 and 5 privacy behaviors; Pragmatists should have a medium number of privacy behaviors, i.e. the majority of pragmatists should have from 2 to 3 privacy behaviors; and, Unconcerned should have the lowest number of privacy behaviors, i.e. the majority of unconcerned should have fewer than 2 reported privacy behaviors.

[42] In the survey privacy behavior was collected as a self-report on previous actions taken. This was done to minimize having the user predict future behaviors.

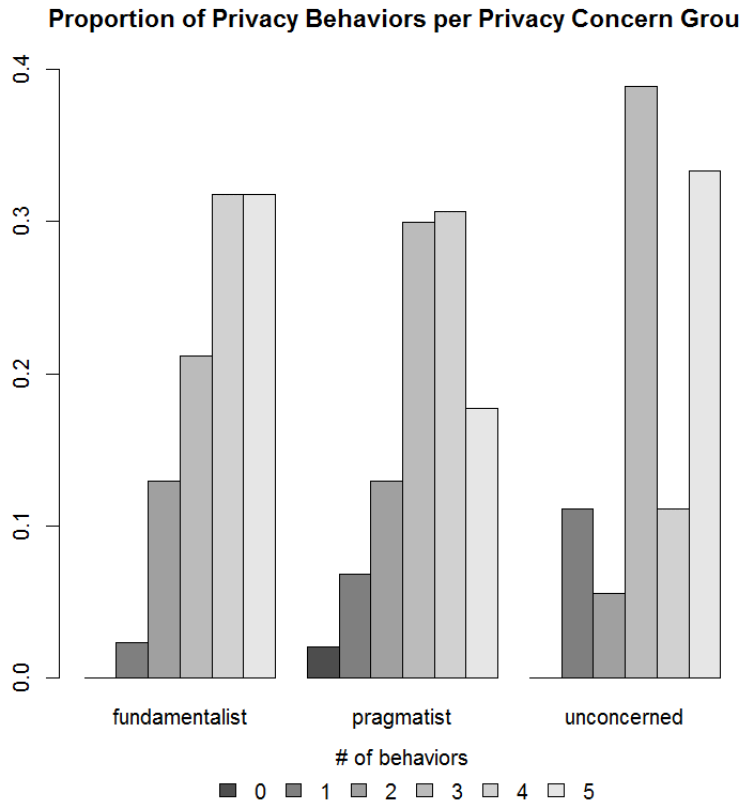


Figure 17. Graph showing the proportion of the number of privacy behaviors per group as defined by Westin's Privacy Segmentation Index.

By analyzing the proportion of each behavior per privacy concern group (Figure 17), although privacy concern as measured by Westin's PSI seems to be within expectations for Fundamentalist and just a bit more concerned than expected for Pragmatist, when it comes to Unconcerned the index classification and reported previous behaviors differ significantly.

When the level of concern is analyzed in relation to the types of privacy behavior the use of PSI as an indicator for behavior becomes even more distant from expectation. It would be expected to see Fundamentalists taking active behavior to protect their privacy, and pragmatists focusing on passive behavior. However, there seems to be no distinction in the distribution amongst these two groups.

Table 11. Contingency table for PSI categories and different types of privacy behaviors

	PASSIVE BEHAVIOR		ACTIVE BEHAVIOR		
PSI	**No Info**	**No Use**	**Policy**	**Cookies**	**DNT**
Fundamentalist	76	80	48	73	44
Pragmatist	123	122	60	122	63
Unconcerned	11	13	14	15	10

5.5 Discussion

The population that participated in the study is not a true representation of the Brazilian population. For example, by analyzing the projected distribution of age in the country[43], the age distribution would have had to be more equally distributed, in particular to the selected brackets it would be: 18-25, 18%; 26-35, 23%; 36-50, 29%; and, 50+ 30%. However, this is neither a necessarily negative nor unexpected aspect. Given the method, places of distribution of the survey link, as well as the format of the survey (online), a younger, more computer active and computer literate group was expected. This group is most likely a representation of the group that was later invited to participate in the user study, as well as the group that will, likely, serve as early adopters of Internet of Things technology.

Within this group it was possible to notice that there is a tendency of being slightly more trusting of technology than not, which is in accordance with the expectation of a younger group that grew up using technology. Even online banking, which is seen as a risky activity for many, was said to be part of the computer usage by 77.20% of the participants.

There was also a tendency of viewing interruptions that happen when the user was focused as more negative than positive. Nevertheless, this did not translate as behavior that would avoid having this type of interruption. This can be related to “fear of missing out” (or FOMO). The Oxford dictionaries added an informal definition for this acronym in 2013 as, “Anxiety that an exciting or interesting event may currently be happening elsewhere, often aroused by posts seen on a social media website”. FOMO in combination to the fact that 94.00% of the participants reported using technology for social media, 96.00% for news, and 98.80% for e-mail becomes a possible explanation for this discrepancy in attitude and behavior related to interruptions.

Considering the discrepancy between attitude and behavior in privacy, it was shown that while PSI can serve as an overall privacy concern index, it is not a good indicator of behavior. There were no significant differences between proportion of participants considering the behaviors for privacy pragmatists and fundamentalists (Table 11). Also, when considering the number of behaviors taken per group type, those classified as unconcerned did not match their behavioral expectation (Figure 17). On the other hand,

[43] http://www.ibge.gov.br/home/estatistica/populacao/projecao_da_populacao/2013/default_tab.shtm

computer literacy seemed to be somewhat related to the results of both the PSI (Table 10) and with the number of privacy behaviors taken (Figure 16).

For the first case, it is possible that as users become more aware of the technology behind the services collecting and storing their data, they also tend to become more aware of the possibilities for errors and attacks. This in turn could influence their concern over privacy. However, there was no significant trend to corroborate this hypothesis. For the case of computer literacy and privacy behaviors, the relationship could be derived from the fact that some of the behaviors listed required an additional knowledge of computers in order to be enacted (e.g. turning on the “do-not-track” option in your browser). The process of educating the users about what is collected, for what purpose, how his/her data is being protected, and what are the mechanisms available for protection, is as important as developing the technology for protecting user privacy. When a user is more informed, s/he will be aware of a wider range of protection mechanisms as well as which is better suited for each situation. In fact, the only active privacy protective behavior that was broadly performed was “clearing cookies”, which has been incentivized and taught even by news websites[44].

Still related to the use of the Privacy Segmentation Index, it is interesting to note that it may not be sufficient in representing people’s concern when dealing with a privacy agent in the Internet of Things. Firstly, the statements are too broad to be used in this context. While the first two are somewhat related to the Internet of Things - refer to control over collection and use of personal information, and handling of that data by the companies - they do not treat this case. In the Internet of Things, the collection could be done (semi-) automatically as well as the security level of the data collected could range from belonging to huge companies with plenty of security layers to a home automation system with local storage that does not have the funds to invest on a high level of data security. Second, as seen in chapter 2 and in previously presented results, there is a dichotomy between people’s attitude towards privacy and their actual behavior. The PSI relies too heavily on attitude. It would be better to have a more specific index that merged both attitudes towards privacy, as well as privacy behavior. Another scale that has been proposed that suffers less from the issue of broad focus is Internet users' information privacy concerns (IUIPC) (MALHOTRA; KIM; AGARWAL, 2004). However, its 10-item scale (control, awareness and collection) is longer than desired considering that it must be applied in combination with other scales for

[44] Alize Oliveira. 2012. “Como limpar cookies do Firefox”. Techtudo. Available at: www.techtudo.com.br/dicas-e-tutoriais/noticia/2011/05/como-limpar-cookies-do-firefox.html. Accessed on April, 2016.

the need for control and trust variables and it is also reliant on privacy attitude and not on privacy behaviors.

Considering the data for desirability of control there was a tendency amongst the participants for having a higher desire for control. When analyzing the distribution of overall scores based on the desirability for control scale, this tendency is made clear since the majority of participants fall between the scores of 33 and 43. This would indicate that this particular group might not incorporate the use of an intelligent privacy agent to make decisions for them without them being consulted about what the decision should be. Signifying that using just the system's certainty, as current systems do, in order to decide to add the user to the decision loop might not be the best idea.

By analyzing the survey data about the participants' preferences related to the proposed variables some interesting results arise. First and foremost, it is possible to see that the variable that current choreographed solutions, presented in Chapter 3, used as their basis to interrupt the user for further input (certainty), was the fourth variable with the least agreement that it would influence, and the second one with the most agreement that it would not. This shows that the current technique used is not on par with people's expectations when considering the participants of the online survey. Making it clear that it is necessary to revisit the decision of using just the agent's certainty. Another interesting result is that the social expectation of whether or not a person should be interrupted in that situation had an extremely high "not sure" rate. Meaning that, even though previous literature has pointed to this variable as relevant, it needs to be further explored before we can confidently consider it together with the rest of the set. Finally, it is important to note that the variable defined in this work as "Activity Engagement" was divided here in two: workload and social engagement. Because of this division it was possible to see that people favor the workload aspect (78.80%) over the social engagement aspect (68.00%) of this variable, being a possible simplification to be made if this continues to hold true.

The results confirm the expectation and argument of this thesis that there is a need for a broad set of variables, instead of just focusing on interruptibility or privacy and control related variables. By considering the overall agreement that the variables would influence, we can see that there was a tie to the most relevant one. They were, Sharing Sensitivity (influences the user's desire to have control) and Frequency of Interruptions (influences the user's desire to not be interrupted). After this tie, the variables from both groups are mostly interposed showing that neither group of variables can be dismissed.

The need for a broad and varied set of variables was further reinforced when we analyzed the different groups that we could consider. When analyzing considering the groupings from I to VI, it is possible to think of considering only four groups: group III, where all variables influence (44, 17.60%); group IV, where the receptivity variables were more relevant (98, 39.20%); group V, where the interruptibility variables were more relevant (69, 27.60%); and, group VI, where the number of variables marked as relevant were the same considering both groups but not on the extremes of no variables or all variables (32, 12.80%). This would lead to a lesser need for focus on the mixed group, since it was the one with the lowest frequency of the four. However, when groups IV and V are divided considering how big of a difference in relevance there was, it becomes clear that mixed preferences between the receptivity and interruptibility variables are the overwhelming majority. This shows that so far it is not possible to neatly characterize users into majority groups considering their self-reported preference towards variables. Further research is necessary if this is desired.

5.6 Conclusion

The results and discussions presented in this chapter show that the expectation of having all variables be significantly accepted by a larger population was correct, with the exception of Social Acceptance that needs to be further investigated. It is important to note, however, that this is only an indication based on a quasi-binary classification and the order found on the survey from the frequency of “influence” selection should not be taken as one variable being more relevant than another. Also, the expectation that it would be possible to identify three major groups – **can** is more important, **want** is more important, and mixed - with approximate relevance was not correct. There is too much diversity amongst opinions, which reinforces the fact that the ordering of variables found should not be generalized.

Also, possible simplifications to the group of variables could be noted, considering that activity engagement’s workload aspect had a higher perceived relevance than its social engagement counterpart. Social acceptance also did not have a high “relevance” rate, but had an almost equal “not sure” rate. This shows that, perhaps, the social aspects of context are not as relevant as the interruption’s, the user’s, and the system’s characteristics.

Through this initial intervention it was possible to better understand the group of people that participated, given demographic and personal characteristics data collected. This knowledge will be useful when analyzing the data of the next interventions. It is possible to have a baseline value to which other groups of participants can be compared to.

Finally, it was possible to notice the need for valid and related tools in order to collect data regarding preferences of control and trust in the context of a privacy decision-making agent in the Internet of Things. Such tools are needed as well as an extension or modification of the Privacy Segmentation Index that considers this particular context and privacy behavior instead of just privacy attitude.

These results and discussion are thought to be relevant and necessary for the community researching the use of privacy agents. However, it is important to note that they were obtained and based on a self-report tool (survey), for a particular culture (Brazilian), and for a specific group of users. It is necessary to verify their validity for other groups as well as check if they hold when they are collected using a more realistic and observation-based tool. Also, it is important to note that the Internet of Things as described to the participants is not, yet, our reality. For this reason, the described expected behavior and real behavior most likely will differ.

Chapter 6

User Study and Interviews

As seen in the previous chapter, the variables selected were generally well accepted. Except for Social Acceptance, there was at least a 68% agreement for all other variables that they would influence the preference to take or delegate control. However, surveys and questionnaires rely deeply on self-report and imagined behavior, both characteristics that lead the results to have a lower ecological validity. On top of this, the results obtained from the survey considered the variables individually, disregarding possible influences when considering them.

In this sense, we have performed a user study to explore the variables more deeply and obtain results closer to real-world behaviors and expectations. This chapter presents the objectives, methodology, results, limitations and ensuing discussion of this user study. Also, the results of the follow-up interviews conducted with a subset of the user study's participants are reported. The work reported in this chapter was performed in partnership with Gabriela Mattos, an undergraduate student in Computer Science. For this reason, throughout this chapter the pronoun 'we' will be used whenever the work was done as a group. The study was approved by our institution's Internal Review Board.

6.1 Objectives

As mentioned before, the overall objective of this user study was to explore the variables more deeply and obtain results closer to real-world behaviors and expectations. In particular, this deeper exploration was in order to identify if the variables were relevant and see if it is possible to identify groups of users considering these variables.

6.2 User Study Design

For this study the Experience Sampling Method (ESM) was chosen. ESM is defined by Larson and Csikszentmihalyi (2014) as “a research procedure for studying what people do, feel, and think during their daily lives. It consists of asking individuals to provide systematic self-reports at random occasions during the waking hours of a normal week.” Because participants are reporting their behaviors in a more natural environment (vs in a lab study) and at random occasions (vs at pre-defined moments), the results from ESM tend to have a higher ecological validity than other more controlled user studies. Similar studies such as SampleMe (PEJOVIC; MUSOLESI, 2014) have been successfully performed in similar settings. We based our design on the work of Pejovic and Musolesi (2014) and on the description provided by Larson and Csikszentmihalyi (2014).

However, at the same time it provides more ecologically valid data, it is also a more intense, tiresome, and intrusive method than lab studies. It requires dedication for longer periods of time than most methods, as well as that participants reflect and communicate aspects of their lives, their decision-making process, and preferences. Because of this a *research alliance* is necessary between participants and researchers, i.e. there is an understanding of the procedures and motives for the studies, and cooperation depends on the participants’ belief that the research is important (LARSON; CSIKSZENTMIHALYI, 2014). Given this necessary higher level of commitment and trust, participants were invited from within the research group communities.

They interacted with a total of 90 interruptions distributed in 10 days (From Monday to the next Wednesday) - 9 interruptions per day - and within each day the participants had a 10-hour window (from 9am until 7pm) during which the interruptions would happen. Because one of the considered variables is *Frequency of Interruptions*, these 9 interruptions per day were randomly distributed by the research group with the following considerations:

- low frequency interruptions were stand-alone interruptions with 40 minutes or more of ‘silence’ before and after it;
- medium frequency interruptions were paired with 20-minute intervals between them and 40 minutes or more of ‘silence’ before and after it;

- high frequency interruptions were blocks of three interruptions every 20 minutes within one hour that had 40 minutes or more of ‘silence’ before and after it.

Every study day had one high frequency interruption block, up to two medium frequency interruption blocks, and the necessary amount of low frequency interruptions to complete 9 interruptions. Each type of interruption frequency had a total of 30 interruptions. The full distribution can be seen on Figure 18.

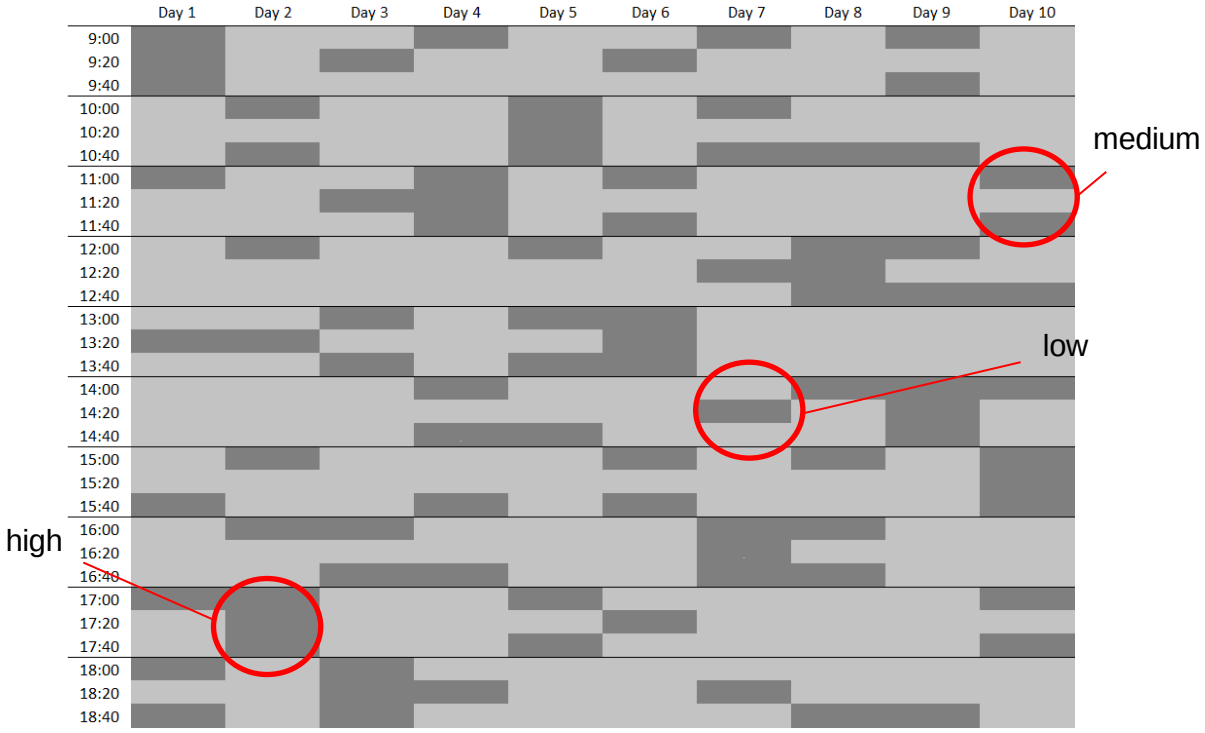


Figure 18. User study interruption frequency distribution

The study was done in 21 days given the following schedule:

- 1st day: Application link and support documents were provided. The documents covered installation steps and usage guide.
- 2nd to 5th day: Time reserved for participants to install the application and request assistance with the study. During this period, it was also possible to answer the initial questionnaire from within the application (Appendix D)
- 6th and 7th day: Classification of predefined data collection scenarios regarding its sensitivity and initial thoughts as to delegating or not.
- 8th to 17th day: ESM period

- 18th and 19th day: Re-classification of predefined data collection scenarios regarding its sensitivity and initial thoughts as to delegating or not.
- 18th to 21st day: Time reserved for participants to answer the exit questionnaire from within the application (Appendix D)

6.2.1 Initial Stage: Questionnaire and Scenarios

The initial stage of the study consisted in the participants filling out an initial questionnaire and classifying a set of 35 scenarios. These scenarios were developed by the research group by deciding on relevant examples for the factors of interest (the data type being collected, the collector, and the reason behind it). A larger subset of scenarios was originally created and reduced to 35 since participants would have to classify them in the initial stage. The initial questionnaire was used to collect demographics and personal characteristics from the participants[45]. The (semi-)static variables considered were collected in this moment: *Need for Control, Privacy Concern, Perceived Trust.*

The classification of scenarios was done so that the application could present users with pre-established types of scenarios (varying *Sharing Sensitivity*) in accordance to their own definitions of what was a sensitive situation. Participants did not have to characterize the sensitivity level in every interaction. The participants classified the scenarios in both their sensitivity level as well as their initial preference to withhold control or delegate the decision to the agent. During a pilot study, it was noticed that this initial and static classification could pose a validity problem, leading to the addition of the re-classification stage at the end of the study.

6.2.2 Main Stage: ESM

For each interruption, participants were notified via an Android notification telling them it was time to participate[46]. They could choose one of three actions: ignore/cancel the notification,

[45] These were the same questions posed to the participants of the online survey presented in the previous chapter, with the exception of the personality section, which was removed. For a description of each individual section we forward the readers to Section 5.2.

[46] Application can be found in https://github.com/jcolnago/UserStudy-Master

delegate the decision to the agent without seeing further information, or see further information before deciding whether to choose or delegate Figure 19.

During the study explanation, the participants were requested to avoid ignoring or canceling the notification unless it was a situation that they could not (e.g. very important meeting, in the shower, …), or should not answer the interruption (e.g. driving a car). To give participants some leeway, a time window of 15 minutes was added to each interruption. After this time the interruption would be removed and a count of interruptions missed would be incremented. This allowed some extra time while still maintaining the time sensitive characteristic of privacy interruptions in the Internet of Things.

Whenever the participant chose to delegate without having any further information, s/he was prompted with options to help him/her explain why. The options were related to the "Can I be interrupted?" variables: *Social Expectation* ('I shouldn't have been interrupted now)*, Activity Engagement* (I'm busy), *Mood* ('I don't have the patience to answer this now') and *Frequency of Interruptions* (I've been interrupted too much'). An option of 'Others' was also provided. With it the participant could choose and later explain why this was selected using the application. The goal was to make this interaction simple and quick, since it was expected that if the person decided to delegate control without any awareness s/he probably should not have been interrupted.

On the other hand, this concern did not exist if the person decided to see more information before deciding. In this situation, the length and somewhat complexity of the questions were considered a good way to simulate the time and effort necessary to make privacy related decisions. In this situation, the participant was presented with a scenario that s/he had initially classified and a level of system certainty. The *Sharing Sensitivity* and *Prediction Certainty* values for every interruption was the same for all participants. The first was adapted to each individual user considering the initial classification of scenarios, but the second were static values. The certainty values were low (70-85%), medium (85-95%) and high (95-100%). Both values were statically defined to avoid having to have the user classify the same certainty level or the same scenario multiple times.

After reading both the certainty and scenario, the participant chose whether they would prefer to choose or to delegate in this case. This was followed by a contextualization of the user's situation and state of mind based on the remaining variables. *Mood* was represented by

a direct representation of the participant's current mood; *Activity Engagement* was divided into its two components: workload and social engagement[47]; *Social Expectation* was represented by the participant's perspective of the rudeness of the interruption; and, *Frequency of Interruption,* while internally controlled, was also directly answered. The latter was the only variable which was both internally and directly controlled because in previous discussions inside the research group we realized that the definition of what is a high, medium, or low frequency varies immensely between people.

Finally, the last thing the participants were inquired about was why they had made that decision. Here we offered a shortcut to what we believed were the variables that would consciously affect the decision, namely the certainty level and the three components considered for the sensitivity – who, what and why. These variables were selected because they were the ones being displayed when participants made the decision. However, participants had the choice of an open answer to either list other reasons or explain their reasoning, if desired.

6.2.3 Final Stage: Questionnaire and Scenarios

The final stage of the study consisted of the participants filling out an exit questionnaire and re-classifying the set of 35 scenarios. The exit questionnaire was used to collect information as to what they perceived as being the most relevant influencers of their decision making process, their preference as to the agent's behavior for the interruptions that they missed, and questions about the user study and its format in general. The questionnaire can be found in Appendix D.

The re-classification of scenarios was done to verify an impression that the *Sharing Sensitivity* and preference for control for the same scenario varied with time. As such, the participants re-classified the scenarios in both their sensitivity level as well as their initial preference to withhold control or delegate the decision to the agent.

[47] As in the online survey.

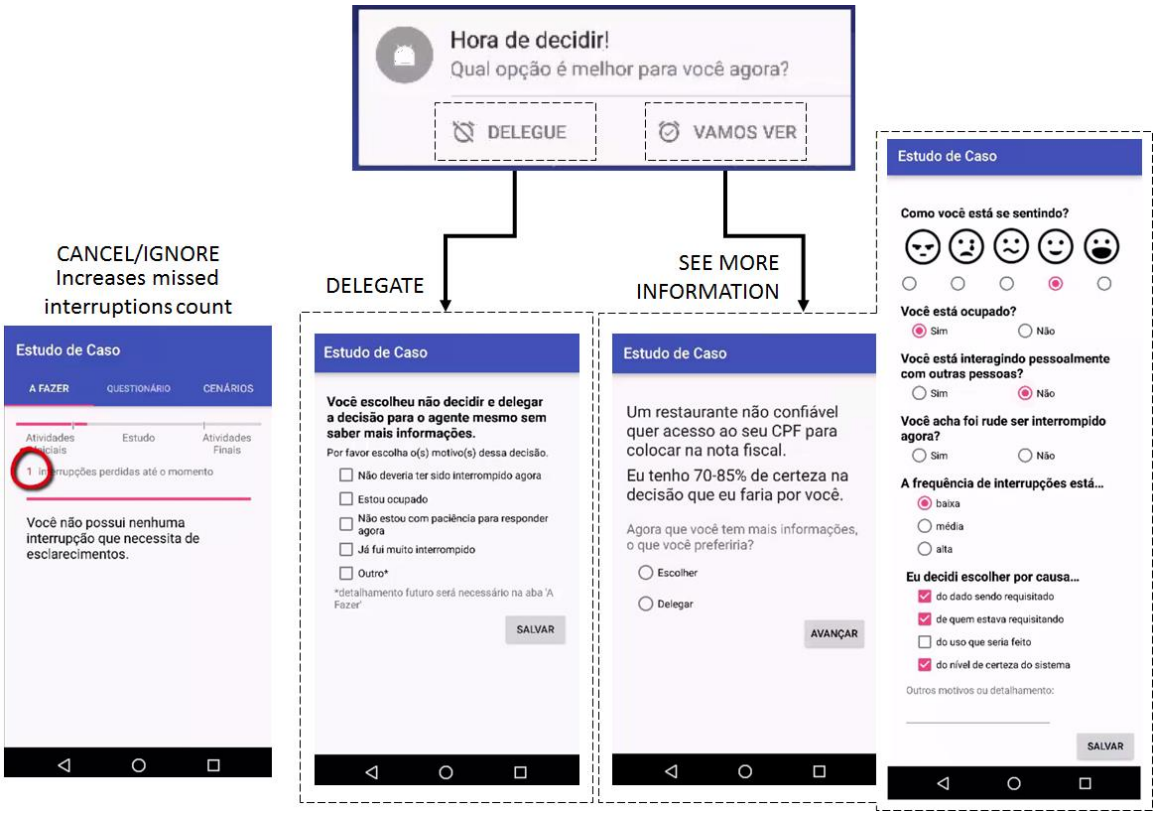


Figure 19. Depiction of the workflow and screens (in Portuguese) with which the participant would interact.

6.3 Results

As mentioned, the goal of this user study was to explore the variables more deeply and obtain results closer to real-world behaviors and expectations. The results presented here were obtained from 21 participants of the ESM study previously described. Some post-hoc filtering had to be done with the results for situations where there was a misbehavior when writing the results to file.

6.3.1 Demographics

As can be seen on Table 12, gender was well distributed within the participants (9 female and 12 male) and was very close to the distribution obtained with the online survey (OS). Age, however, was even more biased to a younger population than it was on the online survey, with the majority of participants (12 out of 21) being in the 18-25 bracket.

Similarly, expert computer literacy and more than 8 hours of daily computer use were the most frequently reported values for each category. Nevertheless, in the user study there was one report of low computer literacy. This did not occur on the online survey. Finally, related to computer use, ‘work’ and ‘other’ had an increase in frequency, but all others were less frequently reported than on the online survey. In particular, social networking, online banking and study had the highest decreases from the listed activities.

Table 12. Demographic values from participants of the user study in comparison with the values obtained from participants of the online survey (OS).

	N=21	%	OS %
Gender			
Female	9	42.86	42.00
Male	12	57.14	58.00
Age			
18 - 25 years	12	57.14	44.40
26 - 35 years	5	23.81	35.20
36 - 50 years	3	14.29	9.60
50+ years	1	4.76	10.80
Computer literacy			
Expert	15	71.43	56.40
High	4	19.05	28.40
Medium	1	4.76	15.20
Low	1	4.76	-
Daily Computer Use			
Less than 2 hours	1	4.76	2.80
Between 2 and 6 hours	3	14.29	19.60
Between 6 and 8 hours	3	14.29	21.20
More than 8 hours	14	66.67	56.40
Computer Use			
E-mails	20	95.24	98.80
News	20	95.24	96.00
Study	18	85.71	96.40
Entertainment	18	85.71	93.20
Work	18	85.71	85.60
Shopping	17	81.95	90.80
Social Networking	16	76.19	94.00
Online Banking	14	66.67	77.20
Others	6	28.57	4.80

6.3.2 *Personal Characteristics*

The personal characteristics results were divided into smaller groups to facilitate data representation.

6.3.2.1 Trust

Differently from the results from the online survey, the participants of the user study had an overall higher agreement with the statement that they had important documents without back-up on technological devices (Table 3, Trust #1, 3 disagreed, 14 agreed), but had a slightly higher disagreement over agreement with the statement that they relied on technological devices to serve them reminders of important events (Trust #2, 10 disagreed, 8 agreed). The trend that they don't worry more when something is more technological (Trust #3, 13 disagreed, 3 agreed) and that they don't distrust technology in general (Trust #4, 13 disagreed, 4 agreed) held from the online survey.

Table 13. Distribution of agreement with each of the four trust-related statements

	Trust #1			**Trust #2**			**Trust #3**			**Trust #4**		
N = 21	N	%	OS%	N	%	OS%	N	%	OS%	N	%	OS%
Strongly disagree	2	9.52	19.60	6	28.57	7.20	4	19.05	24.40	7	33.33	40.80
Disagree	1	4.76	28.80	4	19.05	9.20	9	42.86	35.20	6	28.57	40.40
Neutral	4	19.05	7.60	3	14.29	14.80	5	23.81	24.00	4	19.05	14.40
Agree	4	19.05	23.60	6	28.57	38.80	3	14.29	13.20	4	19.05	3.60
Strongly agree	10	47.62	20.40	2	9.52	30.00	-	-	3.20	-	-	0.80

To analyze individual answers, the overall trust was calculated as presented in Chapter 5 in order to see the combination effect of each statement per person. In Figure 12 the distribution obtained from the user study (bars) is compared to the distribution obtained from the online survey (line).

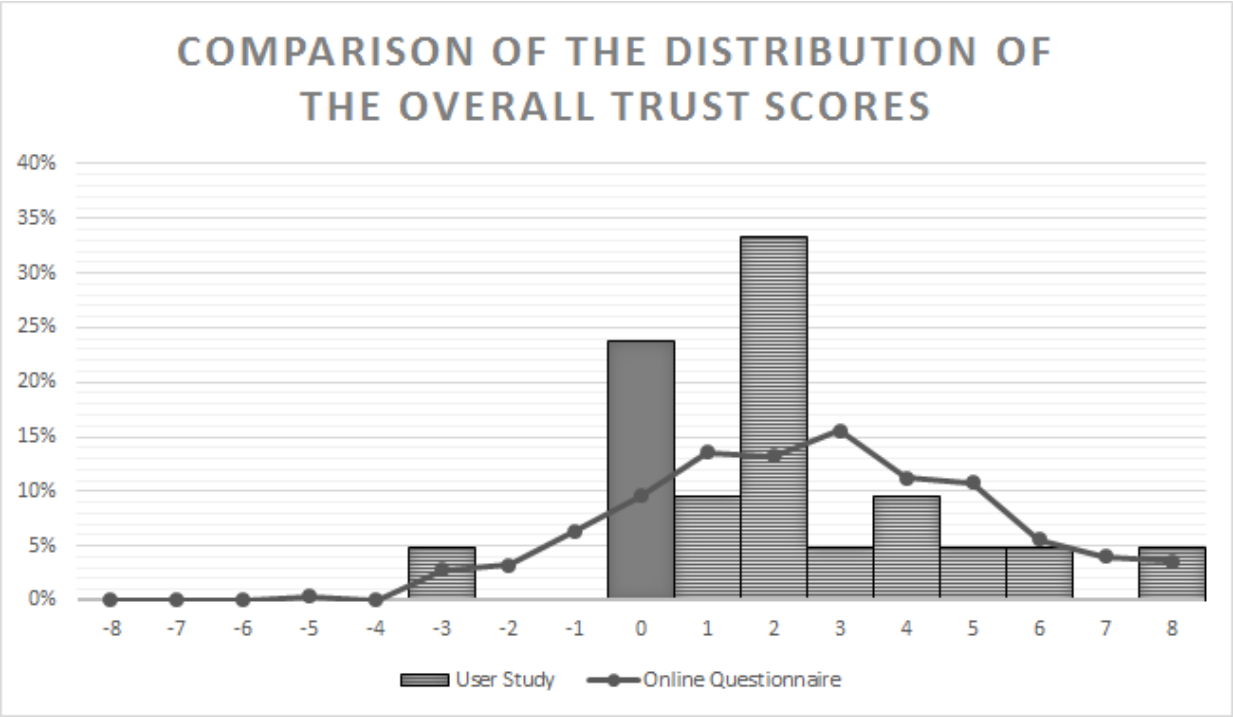


Figure 20. Distribution of the overall trust scores for the user study compared to the overall trust scores obtained from the online survey. The highlighted bar indicates the neutral score.

6.3.2.2 Interruptions

Analyzing the overall response to each interruption statement (Table 4), related to not liking to be interrupted when focused (Interruptions #1), there was no total agreement either way. However, there was only one person that strongly disagreed, indicating that while it may not be a general trend, the participants are not totally opened to being interrupted when focused. On the other hand, the participants seem to generally agree with the statement that they try to shut off notifications whenever possible (Interruption #2, 15 out of 21).

Differently from the results obtained with the online survey, by analyzing individual responses and comparing the agreement between both statements it is possible to see that, for this group, there is a connection between not liking to be interrupted when focused and removing notifications whenever possible. Furthermore, the majority of participants can be found in the lower right corner, where they were neutral or agreed that they do not like to be interrupted when focused and remove notifications whenever possible.

Table 14. Distribution of agreement with each of the two interruption-related statements

	Interruptions #1			Interruptions #2		
N = 250	N	%	OS %	N	%	OS %
Strongly disagree	1	4.76	-	2	9.52	9.20
Disagree	4	19.05	2.80	1	4.76	28.00
Neutral	6	28.57	26.40	3	14.29	19.60
Agree	5	23.81	43.20	7	33.33	29.20
Strongly agree	5	23.81	27.60	8	38.10	14.00

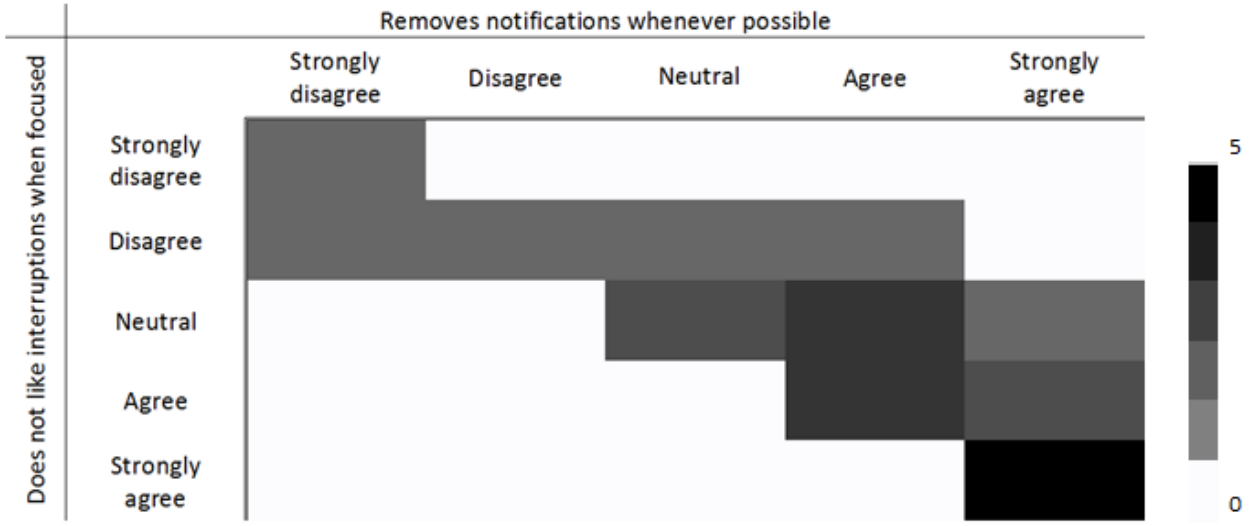


Figure 21. Heat map of the agreement with the interruption-related sentences. The darker the color the higher was the number of participants with that combination (MAX: 5, MIN: 0)

6.3.2.3 *Privacy Behavior and Privacy Concern*

As in the online survey, the overall distribution of privacy behaviors (Table 15) shows that passive behaviors, i.e. does not require the user to go out of their way or an extra effort to enact it, had an overall higher engagement than active behaviors. The passive behaviors of refusing to share information and not using a service because of privacy concerns had 20 and 17 participants (out of 21), respective, stating that they engaged in these behaviors. The active behaviors of reading privacy policies and turning on the “Do not Track” option in the browser had 5 and 12 participants (out of 21), respectively, with privacy policies being less than half (percent-wise) than what was reported on the online survey. The exception was, again, the active behavior of clearing cookies which had a total of 19 out of 21 participants who had previously engage in it.

Table 15. Engagement distribution between the listed privacy protective behaviors. The behaviors are divided as passive and active behaviors.

	N = 21	%	OS %
Passive Behavior			
Refused to Share Information	20	95.24	84.00
Did Not Use App/Website/…	17	80.95	86.00
Active Behavior			
Read Privacy Policy	5	23.81	48.80
Cleared Cookies	19	90.48	84.00
Turned on “Do Not Track’	12	57.14	46.80

Considering the total number of stated behaviors per participant (Table 16), as expected, for the passive behaviors most participants (17 out of 21) had previously enacted both. Active behaviors had a more distributed proportion, with two and one active behaviors being the most frequent number of active behaviors (10 and 7 out of 21, respectively). Finally, three and four total behaviors were the most predominant number of behaviors, with an almost equal number of participants (9 and 7 out of 21, respectively).

For the population that participated in the study, more than half were classified as fundamentalists (11 out of 21), 2 as unconcerned, and 8 as pragmatists. Comparing to the results of Westin’s 2001 survey with U.S. citizens, as with the results obtained from the online survey, the expected number of fundamentalist and pragmatists do not match (Table 17).

Table 16. Proportion of previously enacted privacy protective behaviors grouped as passive behaviors, active behaviors, and total amount of behaviors.

Passive Behaviors	**N = 21**	**%**	**OS %**
0	1	4.76	6.80
1	3	14.29	16.40
2	17	80.95	76.80
Active Behaviors	**N = 21**	**%**	**OS %**
0	1	4.76	10.00
1	7	33.33	29.20
2	10	47.62	32.00
3	3	14.29	28.80
Total Behaviors	**N = 21**	**%**	**OS %**

0	-	-	1.20
1	1	4.76	5.60
2	1	4.76	12.40
3	9	42.86	27.60
4	7	33.33	29.60
5	3	14.29	23.60

Table 17. Privacy concern comparative table between this work and the results reported in (KUMARAGURU; CRANOR, 2005)

	Westin 2001 (U.S. Citizens)	**Online survey (Brazilian Citizens)**	**User Study (Brazilian Citizens)**	
Fundamentalists	25%	34.00%	11	52.38%
Unconcerned	20%	7.20%	2	9.52%
Pragmatists	55%	58.80%	8	38.10%

6.3.2.4 *Desirability for Control*

Finally, analyzing the overall response to each desirability for control statement (Figure 14) with the necessary inversions accounted for, similarly to the group that participated in the online survey, for the group that participated in the user study there is a trend to desire more control. In the user study group, only the second measure had an average below the neutral line. When considering desirability for control as a whole this trend is also visible (M: 39.29, SD: 4.15).

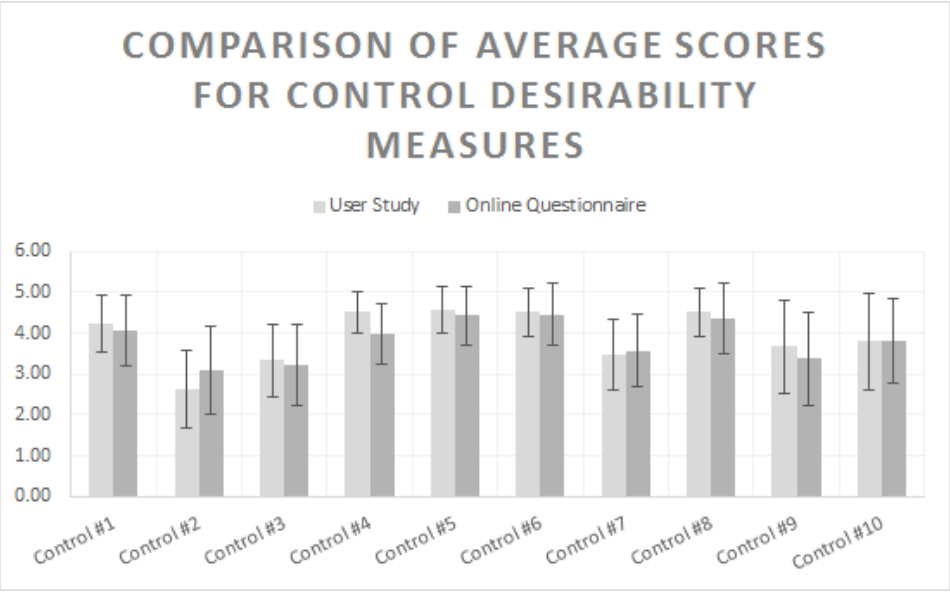


Figure 22. Average scores and standard deviations for individual desirability for control measures

Average-wise the groups that participated in the user study and in the online survey are very similar. To understand how the distribution of the desirability of control looks like the distribution of responses considering their overall value is shown in Figure 23. The percentage of participants for each of the obtained desirability for scores are presented for both the user study (bars) and online survey (line).

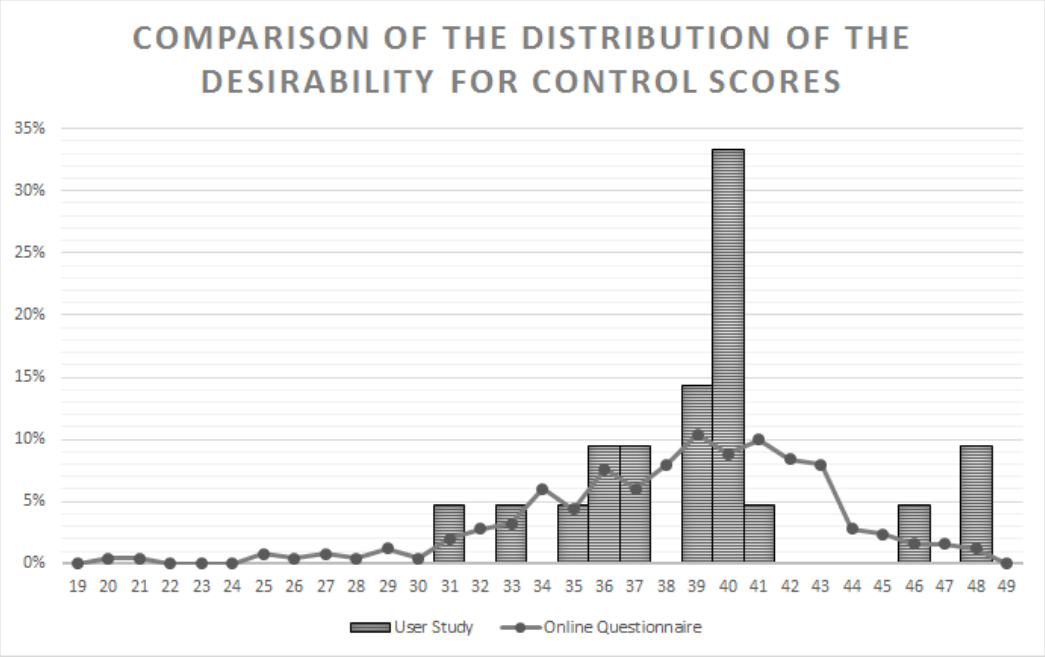


Figure 23. Distribution of the scores for desirability for control. Presented as percentages to allow side-by-side comparison.

6.3.3 Variable Analysis

To analyze the effect of the different variables on the preference to delegate or not control, the results are divided between an analysis of results obtained from the participants answer during the study and those obtained on the exit questionnaire, where participants had to rate what they thought influenced their preferences (as in the online survey). For the behavioral analyses there was a total of 1890 possible data collection moments, 90 per participant. From these 16 had to be removed because there was a problem saving the data

(15) or because it was mistakenly selected (1)[48], and 760 were missed/dismissed by the participant. This totals 776 interruptions (41.06%) that did not directly yield data for the user study.

6.3.3.1 Behavioral Analysis

As previously described in this chapter, when prompted with an interruption the participants could decide to delegate the decision directly to the agent, without even seeing the scenario; see it and decide to delegate it to the agent; or, see it and decide to make the decision themselves. Figure 24 shows there was a significant number of missed interruptions and that they were not evenly distributed. It also shows that there was a smaller number of situations in which the participant decided to delegate directly, with some participants not engaging in this behavior at all.

In fact, there were 122 interactions in which the participants decided to delegate control without even seeing the scenario, representing 6.46% of total possible interruptions and 10.95% of noticed interruptions. In 439 interactions the participants saw the scenario and then decided to choose themselves, 23.23% of total possible interruptions and 39.41% of noticed interruptions. In 553 interactions participants saw the scenario and then decided to delegate the decision to the agent, which corresponds to 29.26% of total possible interruptions and 49.64% of noticed interruptions.

Before the user study was performed, three groups were conceptualized based on the possible specific behaviors.

- **Delegators:** would delegate directly more than select to see more information.
- **Controllers:** would select to see more information more frequently than delegate directly AND want to choose the outcome themselves, actively exerting their control.
- **Watchers:** would select to see more information more frequently than delegate directly AND want to delegate the decision, passively exerting their control through awareness.

[48] The participant used one of the open text answers to explicitly say that they selected to answer the interruption like that by mistake.

As such, classification into these groups would follow the following logic:

```
if (delegated/(seen&chosen+seen&delegated) > 1)
   group = 'delegator'
else
    if (seen&chosen/seen&delegated > 1)
      group = 'chooser'
    else
         group = 'watchers'
```

However, by analyzing Figure 24 it is possible to see that only participant, 4B02, demonstrated a behavior closer to that expected from a delegator (Delegated/Seen = 0.71). Since no participant fitted into the "delegator" group, the ratio of seen&delegated/seen&chosen was analyzed against personal and behavior characteristics to identify if there are inference relationships. Different methods were selected considering the characteristic of the data and this selection and results are described below.

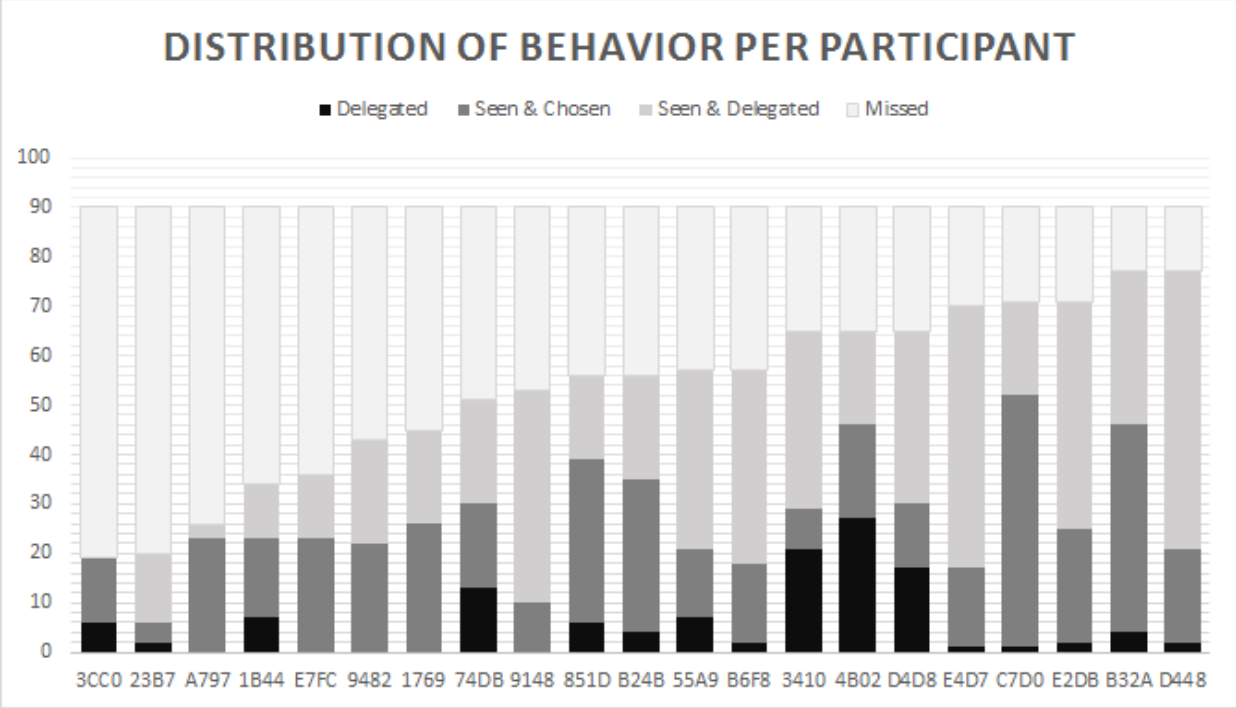


Figure 24. Distribution of behavior per participant considering the 4 possible situations: delegate the choice directly (Delegated), see the scenario and decide to choose (Seen & Chosen), see the scenario and decide to delegate the choice to the agent (Seen & Delegated), and missed interruptions (Missed).

Given the qualitative independent variables, Shapiro-Wilk test was used to check for normality and define whether to use a parametric or a non-parametric test. As see in Table 18, privacy concern, computer literacy, age and gender were not normally distributed (for $p < 0.05$).

Table 18. Shapiro-Wilk Normality Test (H_0: Data is normally distributed) and Levene's Test for Homogeneity of Variance (H_0: Data is homogeneous)

	Shapiro-Wilk Test		**Levene's Test**		
Variable	W	p-value	DF	F-value	Pr(>F)
Privacy Concern	0.7774	**0.0003017**	2	4.3719	**0.02834**
Computer literacy	0.6033	**2.136e-06**	3	0.7678	0.5277
Age Group	0.7447	**0.0001051**	3	2.0088	0.1509
Gender	0.6332	**4.509e-06**	1	0.2521	0.6214

However, since ANOVA is reportedly robust against skews in normality (SCHMIDER et al., 2010) the assumption of homogeneity was checked. Next, Levene's test was used to verify if the null hypothesis that the variances are the same (homogeneous). Only privacy concern refuted the null hypothesis considering $p < 0.05$($p=0.02834$) and so ANOVA with Welsh correction was used in this case.

Table 19. F-test values using ANOVA for gender, age group, computer literacy and privacy concern (with Welsh correction)

Variable	**Df**	**F-value**	**Pr (>F)**
Privacy Concern	**2**	**12.664**	**0.009961**
Computer literacy	3	0.732	0.547
Age Group	3	1.664	0.212
Gender	1	0.119	0.734

By analyzing the output from the tests (Table 19), we can conclude that there is a relation between privacy concern and the ratio between chosen and delegated after seen. Computer literacy, age group, and gender do not have statistically relevant relations.

The Pearson correlation was used between the delegate/seen ratio and the quantitative variables, need for control and trust. Neither were highly correlated with this ratio. However, trust (0.062) showed positive relations and need for control (-0.066) showed negative relations. The nature of these relationships match expectations:

- The higher the level of trust, the more a person will delegate, and
- The lower the need for control, the more a person will delegate.

6.3.3.1.1 Delegated

For the first case, delegating directly, we believed it would represent situations in which the participant had a lower desire/concern over the data sharing activity than the preference of not having that interruption occur at that moment. For this reason, the participants were shown with the variables related to being able to be interrupted at that moment. However, in order to account for the possibility of external variables having an influence, the participants had the option to select the "other" option and later explain it. The participants could select any combination of the presented statements.

Not surprisingly, the most frequently selected statement was the one related to Activity Engagement (72.13%). The Frequency statement, however, had a surprisingly low occurrence, only 10.66%. The variables, their statements, and frequency of selection can be seen on Table 20.

Table 20. Frequency of selection for each variable considering their associated statements when the participant selected to delegate directly.

	Statement	**N = 122**	**%**
Activity Engagement	I am busy	88	72.12
Social Acceptance	I shouldn't have been interrupted now	43	35.25
Other	Other	23	18.85
Mood	I don't have the patience to answer right now	22	18.03
Frequency	I have been interrupted too many times	12	10.66

For the selections of "Other", only 6 answers had additional explanations. Driving was the main reason why "Other" was selected, 4 out of 6, with 2 of these selections happening in combination with other statements (1, Other and Activity Engagement; and 1, Other, Activity Engagement and Social Acceptance), and 2 where that selection was the only selected option. The other 2 explanations were "at the supermarket" in combination with Activity Engagement and Social Acceptance, and "I don't remember" by itself.

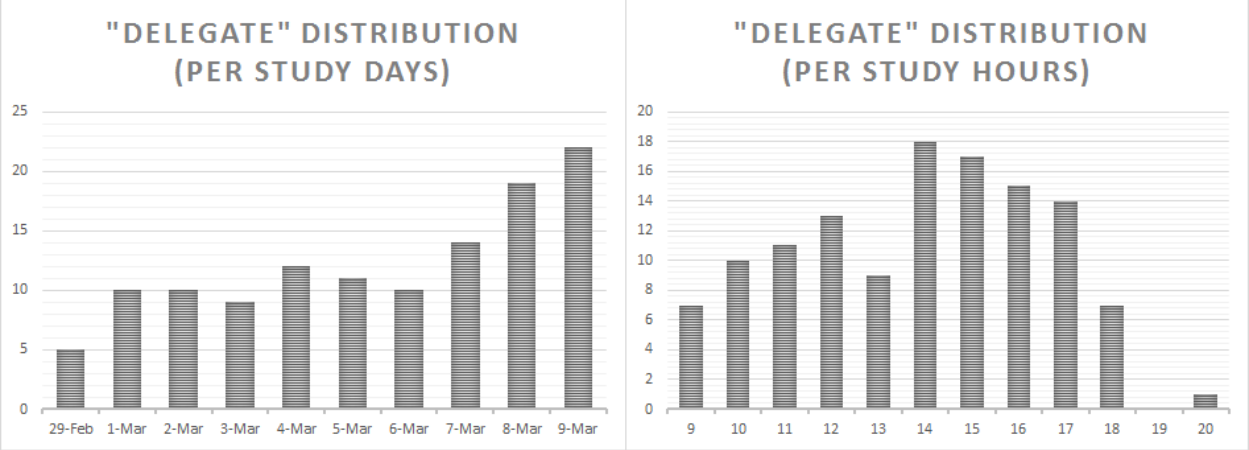


Figure 25. Distribution of the immediately delegated interruptions by study days (left) and study hours (right)

As can be seen on Figure 25 the number of immediately delegated interruptions increased during the study, and within a day the lowest numbers of delegated interruptions were for the first hour, during lunch, and for the last hour of the study. There was one interruption that was answered at 8pm that occurred as the result from a bug in the application logic. Lastly, by analyzing the distribution of selection throughout the user study, it is possible to note that “Mood” and “Frequency” related statements were more frequently selected on the second half of the study (Table 21).

Table 21. Distribution of explanation of why it was decided to delegate directly over the course of the user study

	29-Feb	1-Mar	2-Mar	3-Mar	4-Mar	5-Mar	6-Mar	7-Mar	8-Mar	9-Mar
Social Acceptance	4	4	7	2	4	3	5	4	4	6
Activity Engagement	3	4	4	3	8	5	2	8	13	11
Mood	1	0	0	1	0	3	2	3	2	3
Frequency	0	0	0	0	0	3	2	2	2	3

6.3.3.1.2 Seen

For the second and third cases it is taken into consideration the interruptions with which the participant decided to see more information before making a decision. In this case, the participant was shown a scenario composed of a data type, a requester, and an intended use associated with a level of certainty that the agent had about the participant’s desire to share or not that information. Based on this context and on the participant’s current context, s/he was

asked to decide if s/he would prefer to delegate this decision to the agent or if s/he wanted to make the decision by him/herself.

Because in this situation the participant had at least some desire to be interrupted to become aware of what was happening, following this decision it was requested that s/he classified his/her context based on the variables related to if s/he could be interrupted. Variables related to if s/he wanted to be interrupted, *sharing sensitivity* and *prediction certainty*, were internally controlled, but were also directly asked if they had an influence in his/her decision.

The scenarios and certainty seen by the users were distributed as seen on Table 22. Differences for different levels of the variables were expected given that not every interruption would be seen by everyone. However, sensitivity and certainty were not as well balanced as frequency because of an error in the planned distribution of interruptions[49]. As such, the interruptions shown were internally biased to be with more medium sensitivity than high sensitivity, and with a low/medium level of certainty. While this inherent bias is a strong limitation to the analysis of results by themselves, we believe that by analyzing them in comparison this overall distribution, the effects of it can be mitigated.

Table 22. Distribution of scenarios and certainty characteristics on the interruptions seen by the participants

	All Seen		**Seen & Chosen**		**Seen & Delegated**	
	N=992	**%**	**N=439**	**%**	**N=553**	**%**
Sensitivity						
Low	317	31.96	63	14.35	254	45.93
Medium	448	45.16	233	53.08	215	38.88
High	227	22.88	143	32.57	84	15.19
Certainty						
Low (70-85%)	551	55.54	266	60.59	285	51.54
Medium (85-95%)	327	32.96	115	26.20	212	38.34
High (95-100%)	114	11.49	58	13.21	56	10.13

Considering the pre-established variables by themselves, despite the difference in distribution of sensitivity, it is possible to notice that scenarios that had a low level of sensitivity had a 4:1 ratio of being delegated instead of chosen. For certainty, a medium level certainty displayed a ratio of almost 2:1 of being delegated instead of chosen. Performing the same

[49] This is responsible for the empty values in Table 24 and Table 25

analysis on the results for the “seen” interruptions, i.e. resulted in the participants choosing to make the decision themselves, it is possible to note that for the pre-established variables by themselves, only scenarios with high sensitivity levels presented a ratio favorable to being chosen instead of delegated (approx. 2:1). Chi-square tests between the decision made and sensitivity ($\chi^2(2, N = 992) = 110.62$, $p = 2.2e\text{-}16$) corroborate the statement that there is a more-than-random relation between these variables when considering data from all participants. The same was observed for certainty ($\chi^2(2, N = 992) = 16.58$, $p = 0.00025$).

Interruption frequency was also internally established in the user study. However, participants were directly asked about how they perceived the frequency for each interruption because we wanted to account for differences in preferences. The pre-established frequency levels were all equally distributed (30 for low, medium and high). However, not all interruptions were seen by all participants. Table 23 shows the distribution of both the pre-established observed frequency levels and the perceived ones.

Table 23. Distribution of pre-established and perceived frequency levels for the interruptions seen by the participants

	All Seen		**Seen & Chosen**		**Seen & Delegated**	
	N=992	**%**	**N=439**	**%**	**N=553**	**%**
Frequency						
Low	350	35.28	160	36.45	190	34.36
Medium	314	31.65	139	31.66	175	31.65
High	328	33.06	140	31.89	188	34.00
Perceived Frequency						
Low frequency	314	31.65	126	28.70	188	34.00
Medium frequency	534	53.83	240	54.67	294	53.16
High frequency	144	14.52	73	16.63	71	12.84

As can be seen, pre-established frequencies and perceived frequencies do not show much difference between chosen and delegated. This was verified for pre-established frequencies ($\chi^2(2, N = 992) = 0.63$, $p = 0.73$) and perceived frequencies were significant only at $p<0.1$ ($\chi^2(2, N = 992) = 4.69$, $p = 0.096$).

Table 24. Comparison of effect of the variables Perceived Frequency (PF), Certainty (Ce) and Sensitivity (S) together on the decision to Choose (C) or to Delegate (D)

PF	Ce	S	C	D	C/D	D/C
L	L	L	20	70	---	3.50
L	L	M	44	34	1.29	---
L	L	H	25	6	4.17	---
L	M	L	4	21	---	5.25
L	M	M	17	40	---	2.35
L	M	H	---	---	---	---
L	H	L	---	---	---	---
L	H	M	---	---	---	---
L	H	H	16	17	---	1.06
M	L	L	19	79	---	4.16
M	L	M	70	49	1.43	---
M	L	H	44	19	2.32	---
M	M	L	10	52	---	5.20
M	M	M	61	70	---	1.15
M	M	H	---	---	---	---
M	H	L	---	---	---	---
M	H	M	---	---	---	---
M	H	H	36	25	1.44	---
H	L	L	7	18	---	2.57
H	L	M	21	7	3.00	---
H	L	H	16	3	5.33	---
H	M	L	3	14	---	4.67
H	M	M	20	15	1.33	---
H	M	H	---	---	---	---
H	H	L	---	---	---	---
H	H	M	---	---	---	---
H	H	H	6	14	---	2.33

Table 25. Comparison of effect of the variables Frequency (F), Certainty (Ce) and Sensitivity (S) together on the decision to Choose (C) or to Delegate (D) .

F	Ce	S	C	D	C/D	D/C
L	L	L	20	81	---	4.05
L	L	M	36	22	1.64	---
L	L	H	31	3	10.33	---
L	M	L	2	10	---	5.00
L	M	M	50	56	---	1.12
L	M	H	---	---	---	---
L	H	L	---	---	---	---
L	H	M	---	---	---	---
L	H	H	21	18	1.17	---
M	L	L	14	37	---	2.64
M	L	M	44	29	1.52	---
M	L	H	22	11	2.00	---
M	M	L	10	46	---	4.60
M	M	M	33	38	---	1.15
M	M	H	---	---	---	---
M	H	L	---	---	---	---
M	H	M	---	---	---	---
M	H	H	16	14	1.14	---
H	L	L	12	49	---	4.08
H	L	M	55	39	1.41	---
H	L	H	32	14	2.29	---
H	M	L	5	31	---	6.20
H	M	M	15	31	---	2.07
H	M	H	---	---	---	---
H	H	L	---	---	---	---
H	H	M	---	---	---	---
H	H	H	21	24	---	1.14

Analyzing these variables in combination and comparing the results obtained from using perceived frequency (Table 24) and pre-established frequency (Table 25), it is possible to notice a significant difference on the ratios of chosen and delegated decisions. Given the observational nature of this study, the results reported by the users are of a higher interested to us. For this reason, the following analysis and discussions will focus on the values of perceived frequency instead of pre-established frequency.

The results of a logistic regression model with these three variables (**Error! Not a valid bookmark self-reference.**) yield that sensitivity and certainty are the statistically relevant factors. However, so was the intercept. High sensitivity and medium sensitivity positively affect the odds of choosing. Medium and high certainty negatively affects the odds of choosing. This can be observed on Table 24

*Table 26. Coefficients for logistic regression with the decision made as dependent variable and perceived frequency, sensitivity and certainty as independent variables. Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1*

	Estimate	**Std.-Error**	**Pr(>|z|)**	
(Intercept)	-1.36	0.17	6.81e-15	***
Perceived Frequency				
Medium	0.16	0.16	0.29	
High	0.42	0.22	0.056	.
Sensitivity				
Medium	1.59	0.18	<2e-16	***
High	2.31	0.26	<2e-16	***
Certainty				
Medium	-0.60	0.17	0.00031	***
High	-1.08	0.29	0.00018	***

Finally, there seems to be a relation between choosing or delegating when considering *who* ($\chi^2(1, N = 992) = 30.84$, $p = 2.8e\text{-}08$), *why* ($\chi^2(1, N = 992) = 40.80$, $p = 1.7e\text{-}10$), and *certainty* ($\chi^2(1, N = 992) = 77.03$, $p = 2.2e\text{-}18$), but not *what* ($\chi^2(1, N = 992) = 1.47$, $p = 0.226$).

Comparing the results of reported influence for the different aspects of the scenario and the certainty presented, it is possible to note that the type of data (*what*) was relevant in both the situations in which the participant decided to choose (79.04%) or decided to delegate (75.59%) thus not being an influence in either. The requester (*who*) was reported to have influenced more frequently the situations where the participant decided to choose, while the reason for the request (*why*) and the agent's *certainty* were reported to have influenced more frequently the situations where the participant decided to delegate (62.93%

and 57.50%, respectively. See Table 27 for the other values). This is corroborated by the coefficients of the logistic regression modeled using these variables (Table 28).

Table 27. Self-report of motivators for the decision to choose or delegate

	All Seen		**Seen & Chosen**		**Seen & Delegated**	
	N=992	**%**	**N=439**	**%**	**N=553**	**%**
What						
Influence	765	77.12	347	79.04	418	75.59
No Influence	227	22.88	92	20.96	135	24.41
Who						
Influence	477	48.08	255	58.09	222	40.14
No Influence	515	51.92	184	41.91	331	59.86
Why						
Influence	534	53.83	186	42.37	348	62.93
No Influence	458	46.17	253	57.63	205	37.07
Certainty						
Influence	447	45.06	129	29.38	318	57.50
No Influence	545	54.94	310	70.62	235	42.50

*Table 28. Coefficients for logistic regression with the decision made as dependent variable and the selection for what, why, who and certainty as independent variables. Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1*

	Estimate	**Std.-Error**	**Pr(>|z|)**	
(Intercept)	0.44	0.18	0.016	*
What (TRUE)	-0.062	0.17	0.72	
Why (TRUE)	-1.08	0.15	1.60e-13	***
Who (TRUE)	0.94	0.15	2.09e-10	***
Certainty (TRUE)	-1.177	0.14	2.43e-16	***

Considering the data collected for the characterization of the participants' context, it is possible to note that for the majority of interruptions, participants had a positive mood (573, 57.76%), were busy at the moment of interaction (653, 65.83%), were not interacting with other people (536, 54.03%), and did not perceive them as being rude (822, 82.86%).

As can be seen on Table 29, the more significant differences between the context for interruptions that were *seen and chosen* and *seen and delegated*, happened in:

- Mood ($\chi^2(4, N = 992) = 27.87$, $p = 1.3e\text{-}05$): participants reported being more anxious when deciding to choose to share or not for the presented scenario themselves than when deciding to delegate, and gladder when deciding to delegate;
- Workload ($\chi^2(1, N = 992) = 10.05$, $p = 0.0015$): participants reported being busier when deciding to choose, than when deciding to delegate; and,

- Social Interaction ($\chi^2(1, N = 992) = 4.923, p = 0.0265$): participants reported interacting more when deciding to delegate.

Social acceptance ($\chi^2(1, N = 992) = 0.80, p = 0.37$) did not have a significant difference between both cases, but there were not that many interruptions perceived as rude. However, by inputting these variables into a logistic regression model (Table 30), only workload and social interaction were relevant. The first having a positive effect on deciding to choose and the later a negative effect

Table 29. Characterization of context for all seen interruptions, interruptions that were seen followed by a decision to choose themselves, and interruptions that were seen followed by a decision to delegate it to the agent.

	All Seen		**Seen & Chosen**		**Seen & Delegated**	
	N=992	**%**	**N=439**	**%**	**N=553**	**%**
Mood						
Angry	25	2.52	13	2.96	12	2.17
Sad	18	1.81	14	3.19	4	0.72
Anxious	306	30.85	162	36.90	144	26.04
Glad	573	57.76	217	49.43	356	64.38
Happy	70	7.06	33	7.52	37	6.69
Workload						
Busy	653	65.83	313	71.30	340	61.48
Not busy	339	34.17	126	28.70	213	38.52
Social Interaction						
Interacting	456	45.97	184	41.91	272	49.19
Not interacting	536	54.03	255	58.09	281	50.81
Social Acceptance						
Rude	170	17.14	81	18.45	89	16.09
Not rude	822	82.86	358	81.55	464	83.91

*Table 30. Coefficients for logistic regression with the decision made as dependent variable and the selection for mood, workload, social engagement and social expectation as independent variables. Significance codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1*

	Estimate	**Std.-Error**	**Pr(>|z|)**	
(Intercept)	-0.01	0.43	0.98	
Mood				
Sad	1.12	0.70	0.11	
Anxious	-0.011	0.42	0.98	
Glad	-0.57	0.42	0.17	
Happy	-0.22	0.47	0.64	
Busy (TRUE)	0.42	0.15	0.0041	**
Interacting (TRUE)	-0.39	0.14	0.0043	**
Rude (TRUE)	0.0064	0.19	0.97	

6.3.3.2 Self-Report Analysis

The self-report analysis performed at the end of the study allowed participants to select how much they thought certain aspects influenced their decisions throughout the study – influenced, kind of influenced/I don't know, and did not influence. In the results it is interesting to note that *Trust*, *Need for Control* and *Social Engagement* were the only ones that had similar values for all three levels in comparison to the results obtained from the online survey, with the latter having a higher discrepancy than the first two. *Sharing Sensitivity*, *Frequency*, *Social Engagement* and *Mood* were considered as an influencing factor by less than half of the participants in the user study than it occurred in the online survey, with *Mood* not being reported as influencing at all. *Workload* and *Certainty* were also more frequently considered less relevant. Finally, *Privacy Concern* was the only variable reported by more participants as influencing the decision in the user study than in the online survey. Table 31 shows the specific values.

For the exit questionnaire, *Sharing Sensitivity* and *Trust* were further divided considering finer-grained aspects that were deemed important. For the *Sharing Sensitivity* these aspects were "who", "what" and "why", and for *Trust* it was related to the desire to make sure that the decision was the right one. These finer-grained aspects all were deemed more relevant to the behaviors enacted than their more abstract counterpart.

Table 31. Reported influence of the different aspects considered on the exit questionnaire in comparison to the results obtained on the online survey. Some aspects were represented with a finer-grained that do not have corresponding values on the online survey.

VARIABLE	I			NI			NS		
	N=21	%	OS %	N=21	%	OS %	N=21	%	OS %
Sharing Sensitivity	8	38.10	84.80	1	4.76	4.00	12	57.14	11.20
Who (requester)	17	80.95	-	0	0.00	-	4	19.05	-
What (data type)	20	95.24	-	0	0.00	-	1	4.76	-
Why (usage)	16	76.19	-	0	0.00	-	5	23.81	-
Frequency	6	28.57	84.80	6	28.57	5.20	9	42.86	10.00
Trust	16	76.19	79.20	1	4.76	6.40	4	19.05	14.40
Right Choice	18	85.71	-	0	0.00	-	3	14.29	-
Workload	10	47.62	78.80	5	23.81	4.00	6	28.57	17.20
Privacy Concern	19	90.48	77.20	0	0.00	6.40	2	9.52	16.40
Mood	0	0.00	74.00	6	28.57	4.40	15	71.43	21.60
Certainty	10	47.62	70.00	4	19.05	11.20	7	33.33	18.80
Need for Control	15	71.43	68.40	1	4.76	6.40	5	23.81	25.20
Social Engagement	4	19.05	68.00	6	28.57	6.40	11	52.38	25.60
Social Expectation	7	33.33	44.00	4	19.05	12.80	10	47.62	43.20

6.3.4 Scenario and Preference Classification

As mentioned, the participants classified the scenarios based on two aspects at the beginning and at the end of the user study: sharing sensitivity and their preference for control. No participants held constant preferences for the sharing sensitivity for all 35 scenarios at the beginning and at the end of the study. Nevertheless, there were significant variations between participants. For control changes, constant preferences happened for three participants: 9148, 3CC0, 851D (Figure 26).

For participants 3CC0 and 851D this meant keeping their preference of choosing for all presented scenarios, so the lack of variability is not that impressive. However, it does show that these two participants would really never want to give up control to an intelligent privacy agent. For participant 9148 the lack of variation is truly surprising, because there was no absolute preference – i.e. the classification of control preference was a combination of “delegate” and “choose” scenarios.

Table 32. Minimum, average, standard deviation, and maximum values of changes in the sensitivity and control preference reported for the scenarios at the beginning and at the end of the study.

	Minimum	Average	Standard deviation	Maximum
Sensitivity changes				
Total	2	10.52	3.38	15
Increased concern	0	6.52	3.38	13
Decreased concern	0	4.00	2.56	10
Control changes				
Total	0	9.38	5.87	20
Increase control	0	5.29	4.78	18
Decreased control	0	4.10	3.93	17

Furthermore, Figure 26 shows that there is a wide range of variation when considering if the changes reflected an increase or decrease in concern and control. Nevertheless, there was a slightly higher frequency of changes that reflected an increase in concern ($M_{increase}$: 6.52, $SD_{increase}$: 3.38 vs. $M_{decrease}$: 4, $SD_{decrease}$: 2.56) and an increase in control ($M_{increase}$: 5.29, $SD_{increase}$: 4.78 vs. $M_{decrease}$: 4.10, $SD_{decrease}$: 3.93).

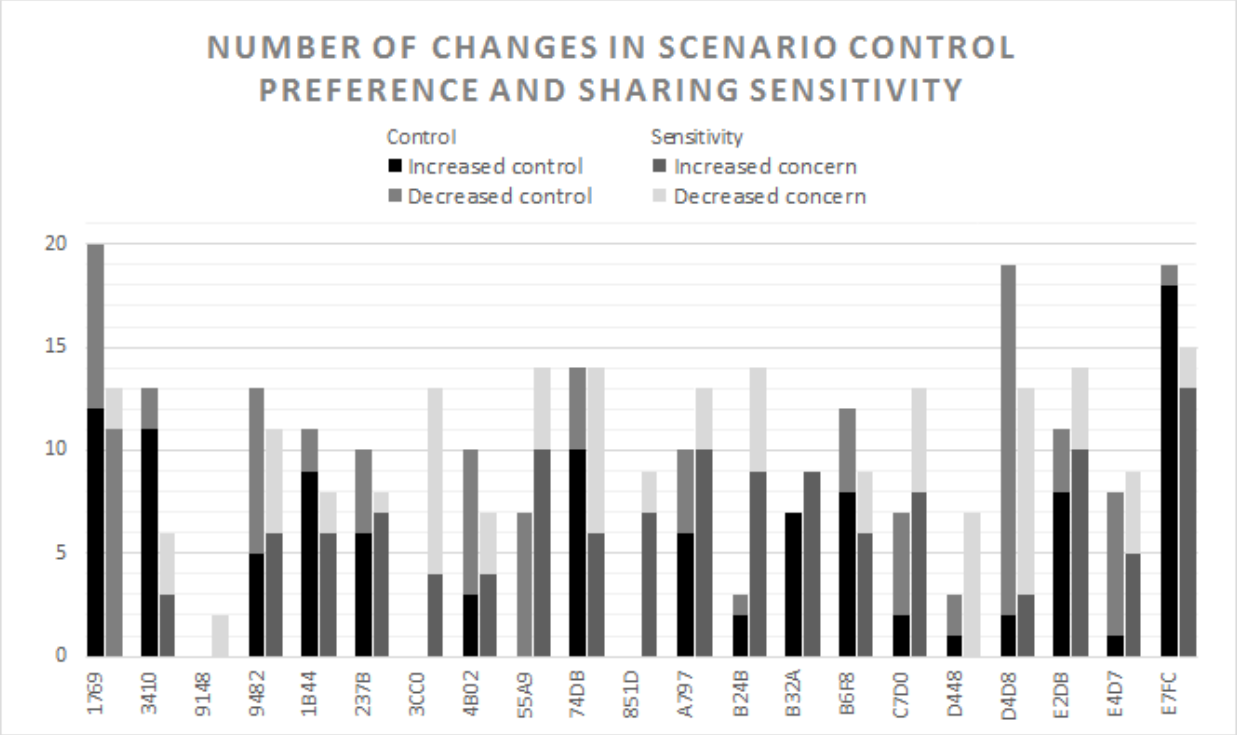


Figure 26. Number of changes in the control and sensitivity reported by each participant.

6.3.5 Exit Questionnaire

On the exit questionnaire the participants were requested to answer about the perceived relevance of the different variables as in the online survey, but also to explore aspects about the format of the user study and their preference towards agent behavior when interruptions were missed.

Some results that inform about necessary changes to the format of the user study have already been presented. In particular, the necessity of a shortcut for when the participants cannot or should not interact with the study became even more evident with comments such as “interactions while driving seem to require an agent”, “I was in a business breakfast when two interruptions occurred and I had to explain what was happening”, “notifications while driving are unpleasant”, and “many of my missed interruptions happened because I was doing daily choirs that required my attention”. Also, the need for on-demand classification of frequency of interruptions[50], which was already made clear with the difference between perceived and planned frequency, became even clearer when the participants were asked to classify their agreement with the methodology used to classify

[50] Instead of static pre-defined values.

the interruptions as low, medium or high frequency. Only high frequency yielded results that would deem our definition passable (Table 33 shows full results).

Table 33. User responses to the exit questionnaire about the used definitions of low, medium and high frequency interruptions

	1/hour (low)		2/hour (medium)		3 or more/hour (high	
	N=21	%	N=21	%	N=21	%
Completely disagree	7	33.33	9	42.86	2	9.52
Disagree	2	9.52	1	4.76	2	9.52
Neutral	5	23.81	3	14.29	1	4.76
Agree	6	28.57	5	23.81	2	9.52
Completely agree	1	4.76	3	14.29	14	66.67

Related to the duration of the study and number of interruptions per day, participants found the study to have a good duration (only one participant said it was too long and one said it was too short) and a good number of interruptions. For the latter, 8 participants said the number of interruptions per day were good, 9 said they were many but not burdensome, and 4 thought they were excessive.

Table 34. User responses to the exit questionnaire over the user study format and agent behavior

	N=21	%
Duration		
Too long	1	4.76
Long*	4	19.05
Neutral*	13	61.90
Short*	2	9.52
Too short	1	4.76
Interruptions per day		
Excessive	4	19.05
Many but OK	9	42.86
Acceptable	8	38.10
Few	0	0.00
	N=21	**%**
Agent Behavior		
Deny all	4	19.05
User defined	13	61.90
High certainty	4	19.05
Medium-High certainty	0	0.00
Autonomous agent	0	0.00
Allow all	0	0.00

Finally, related to how the participants would want the agent to behave for the interruptions they missed, 4 said that all requests should have been denied, 13 said that the agent should act based only on user pre-defined preferences, and 4 said that they would allow the agent to act if it had a high level of certainty. In fact, as a final observation one participant said “I want agents that learn but do not act alone”.

6.4 Interview Results and Discussion

As a final stage in the user study 19 out of 21 participants were interviewed - two did not have the time availability to participate. The goals of performing the interviews were to identify threats to validity and to better understand the mental process of deciding when to delegate and when to choose. Other observations and suggestions for a better user study and agent design were also drawn from the interviews.

One fact that became abundantly clear throughout the interviews was that the characteristics collected in the initial questionnaire matched well the participants’ profiles. Issues related to the need for control, privacy concern and trust came up frequently. Some selected excerpts are:

> *“You want to give me suggestions, that’s fine. But don’t take away my autonomy.” (P8)*
>
> *“(about using a smart coffee maker) only if I knew how it would work. So that I could be sure that there was no way that it could be sending meta-data to some spy […]. I think that everything new that is developed, the last thing people are concern with is security.” (P15)*
>
> *“If this were a real agent making decisions like in the study, what would mean a missed interruption… it would be a decision made without my knowledge. With the level of control I had to visualize information and what it did or did not do, I wouldn’t sign up for a system like that.” (P17)*
>
> *“I rather it wouldn’t act than that it acts without me knowing what it would do.” (P20)*

6.4.1 Threats to Validity

One of the focus of performing the interviews were to identify threats to the validity of the data. These threats could come from different interpretations of the application and requests, superficiality of response in particular situations, interdependency of variables, and other miscellaneous aspects.

6.4.1.1 Different interpretations of the user study application

During the initial phase of the user study all participants were instructed on the context of an intelligent privacy agent capable of making decisions for them in the Internet of Things. They were also told about the goal of the user study: to better understand how they would prefer to behave in such context, when would they prefer to take control and when would they want to delegate it. The overall goal and context was well understood by the participants in general. However, some saw the application not as a tool to collect behavior, but as a representation of how the agent would behave. For this reason, some people rarely delegated decisions to the agent no matter external influences (e.g. workload or frequency of interruptions). One participant put it as "*if the system, even with a high level of certainty, is still asking me… then it is because it wants my opinion" (P20).* This could bias the results towards wanting more control, even though that was not the most important factor. Another issue that stemmed from seeing the application as the real agent was an annoyance with the lack of learning skills of the agent.

> *"I think (the frequency) was high because my days follow a routine. I do the same things almost every day, almost in the same order. So the impression was that a real agent should have learned already. He should have added the rules. There shouldn't be so many new things for it to bother me." (P20)*

6.4.1.2 Different interpretations of requests

Another threat to the validity of the research is that some participants, though not a majority, had different interpretations about certain information requests than it was originally intended.

In particular, the 'mood' request led to different interpretations in two different aspects. First, not all participants understood the request as being related to their current mood. Some answered it in relation to the effect that the interruption had on them.

> *"I didn't know how to answer my mood. The notification wasn't making me happier or sadder. So I always answered it with a happy face." (P17)*

> *"My mood was related to the interruption. The interruption didn't matter to me." (P15)*

> *"Once or twice I used the face right before (the smiley) one because I had just answered an interruption. Or if I was talking to someone and my phone rang. Than my 'mood face' changed" (P21)*

Another source of different interpretations was the emotions represented by the images. A couple of participants interpreted the options as a scale, not necessarily associating with the middle image (anxious).

> *"My mood was always the same. I am a bit indifferent to things. So I always picked the one in the middle, so I wouldn't be too happy nor too sad." (P15)*

> *"I feel weird telling a device that I'm happy. So most of the time I picked the on in the middle. Neither happy, nor sad. I was there… just fine. But sometimes I said I was angry when the notification was annoying me." (P8)*

This last exert shows an extra threat that was caused by the lack of comfort in reporting such a personal detail to an outsider.

All in all, it seems that mood could be used for two different purposes: to predict if the user should be interrupted and to predict if that user should have been interrupted. The first, which was the focus of this study, cannot rely on self-report after the fact because the interruption can affect the participant mood. It should be measured via sensors. On the other hand, the second can rely on self-report after the fact.

Another request that led to different interpretation was the one that asked if the interruption was rude. The intended interpretation was related to social acceptance, i.e. if the interruption disrupted an on-going interaction and if that was perceived poorly. While it was already expected that the response to this request would vary because not everyone perceive the same interruptions as being rude, the feedback showed that the interpretation of rudeness was also associated with the fact that this was a non-sentient device and part of a user study that they agreed to participate. This could be an explanation as to why there were so few interruptions marked as rude.

> *"How could the app be rude if it didn't know my current situation? Most of the time I said It wasn't rude. When I did it coincided with the angry face." (P8)*

"I think that an interruption is rude if you say you don't want to be interrupted and you are. But if you accept that you are going to be interrupted, then it can't be rude. I don't remember if I said any [interruption] was rude, maybe when I was annoyed, or busy, or maybe during class." (P15)

"(Rude) would be if it were interrupting me all the time. But if you are participating on a study, then you made yourself available." (P7)

"In general I didn't see it as rude, because when I agreed to participate I was already expecting this. [...] Maybe in some situations I said it was, because I was talking with my manager. […] (If it wasn't the study) I would probably find it ruder." (P10)

Also, as could be seen in the previous examples some participants associated rudeness with different factors during the study, such as being occupied or interacting. This was expected because they are factors that dictate when it is socially acceptable to receive interruptions. However, a few participants associated with other factors such as mood and the scenario being presented.

"If it was bugging me somehow, or if it was disrupting me. […] The chair was rude, because it is rude to want to know my weight. […] My criteria for rude was if it were being annoying, in this case it was rude because I was in a bad mood." (P9)

"The busier I was, the worst was my mood and I found interruptions rude" (P18)

Another type of comment that could explain why there were so few interruptions seen as rude is that if the participant was in a situation s/he should not be interrupted, s/he usually silenced their phones.

"(If I was in the movie theater) it would probably be missed unless the system could somehow override my 'do not disturb' policy." (P1)

"For me (rude) means inappropriate. If I were in a meeting and the interruption disrupted it. But since when I was in those moments I didn't check the interruptions, I missed them, I don't think I answered that any of them were rude." (P12)

"(If I were in a presentation) then my phone would be on 'none' and I wouldn't even see it interrupted me" (P21)

This shows us a couple of things. The first being that when interruptions are expected they tend to not be considered as rude. It becomes harder to examine this variable in a study situation.

Another factor is that 'rudeness' and social acceptance seem to have too many confounding variables already being considered. So it may be best to remove it, especially because users reported performing their own filtering of notifications in inappropriate situations. Instead of considering if it would be rude to interrupt the user, the agent could try to do it (if other variables indicate it) and, if it is not urgent, it could give up and use the user's default behavior instead.

6.4.1.3 Recall and Rules of Thumb

Whenever the participant decided to see more information and decided to delegate or choose, s/he was later requested to explain what motivated that decision. However, a great number of participants reported relying or gut reactions or pre-conceived rules of thumb to make the decision. Some participants saw this as a positive thing:

> *"I think it was way more out of instinct. There's a research that shows that when you follow your gut feeling you are usually right. […] My answers were fairly automated. But I always remembered what they were." (P17)*

While others saw it as a deterrent, especially because the explanation was so far removed from the decision point, and changed their approach.

> *"This is something that was too much at the end. […] You know how you make a decision and go: 'Yup, that's it.' And then you have to explain exactly why and you have to think about what you just did. […] As I was using the app I started thinking as soon as I read the question, so that I could answer the questionnaire." (P20)*

Also, to avoid missing interruptions or because the scenarios were repeating themselves. participants started making decisions based on rules of thumb.

> *"(For me) it was a rational decision, but sort of mechanical. Like, SSN and store, pick. I wasn't that concerned about the percentage, the certainty, more about the data and what was being done with it. But because the questions were similar at one point it was just mechanical." (P5)*

"If I was in my car waiting for my son and there's someone waiting for my parking space, sometimes what I did was that I would see the scenario and pick something, but my answers weren't thought out. I did it, just so I wouldn't miss the interruption." (P8)

"At the beginning of the study, when the 4 variables were still novelty, I would stop and think about it. Later the process became more automatic and instinctive." (P1)

While neither gut reactions nor rules of thumb invalidate their answers, when the decisions were made without careful consideration it was sometimes harder to remember why they made that particular decision. They had not absorbed the facts presented in the scenario fully. One way to mitigate this in future studies, without giving up the fact that we did not want to allow the participants to go back and rethink their choice, is to move the requests that require some sort of recall closer to the point of the decision. Contextual factors, such as busy and interacting, could be moved further down.

Another point that should be considered is to have a higher variability of scenarios in order to keep participants interested and focused on their answers. Finally, the last comment highlights the need to make clear that it is not a problem to miss interruptions to avoid situations such as the one described, in which the study seems to have caused unnecessary anxiety. In fact, one participant stated: *'… I knew this was to help you. So after I missed the first one I ran to get all the others.'* (P7)

6.4.1.4 Not Real

Another issue that was mentioned by some of the participants was that the lack of realism made them behave differently from how they normally would. The majority stated this as something that they only stopped to think about during the interview, that is, they did not consciously let it affect their decision during the user study, but it could have subconsciously affected them. However, some said that at certain points or in certain situations, their awareness that their data would not be really compromised led them to behave differently than they believe they would.

For some, this meant that they were less concerned than they would normally be.

"Maybe if they were the actual scenarios I would have been a bit more conservative. I know how programs work, so I know that 80% certainty isn't really 80% certainty in an autonomous program." (P20)

> *"Maybe, but when I was answering I didn't take that into consideration, I tried to see it as a real situation. But maybe, somehow, unconsciously, I did consider it. Maybe because it wasn't something real we end up less concerned." (P9)*

> *"If I had the time I would consider as something busy, But, if I was busy my brain would say: 'Forget about it, it's just a study'". (P18)*

For others, this meant that they behaved more concerned than they think they would be.

> *"Some situations I don't know if they were real, so I thought they were weird […] and maybe it did (change my behavior), because I didn't know how it would work. […] I was more protective because I didn't know how it would work." (P8)*

But some reported that even though they had this awareness of safety, for some situations that was not an influence.

> *"(About delegating) I believe that deep, deep, deep down it has to do with the fact that it wasn't something that was really happening. […] But (scenarios) that requested personal information, like SSN or bank information, those I said: no, no, no! So my trust in the system wasn't higher because of that, even knowing it was a simulation, I wanted to have control." (P4)*

Another aspect that relates to the situations not being real, but outside of the content of the scenarios or awareness that it was a study is the fact that the scenarios did not match the participants' current situation. This was reported to have made it more difficult to interpret and think about how they would behave or what they should consider to make that decision.

> *"It was out of context […] For example, if any restaurant asks for my bank information now (and I'm not at a restaurant), it doesn't matter if it is trustworthy or not." (P17)*

One participant suggested that the application could do a better job matching the presented scenarios to the current situation.

> *"It would have been cooler if the study could propose more appropriate scenarios to my current moment. ("Even if that meant that we would have to be tracking you somehow?") For the study to feel more real? Yes." (P2)*

However, even though another participant saw this mismatch as something that made it difficult to see the interruptions as real, this participant was not comfortable with the idea of the application knowing enough to do that.

> *"Sometimes it was something that didn't match the moment. But the perspective of my phone stalking me enough to know what I'm doing and suggest a scenario is a little bit creepy." (P18)*

6.4.1.5 Interdependence of Variables (considered static)

As mentioned before, there were three variables that we varied internally: frequency, certainty, and sensitivity. For all of these variables we believed they would neither be static nor constant throughout participants. For this reason, the scenarios were classified right before the start of the study; certainty was represented as broad ranges; and frequency was asked per interruption.

However, during the user study several participants approached the research team with comments about the study. Given these comments we noticed that it was necessary to approach the matter of what people considered appropriate for the different levels of frequency and certainty during the interviews.[51] With hindsight it does not come as a surprise that there are no "magic numbers" for these variables and that they are extremely dependent of other factors, such as context and content.

While some participants were able to very specifically state their preference for low, medium and high levels of certainty and frequency, they quickly realized that it was not so direct when prodded for further information.

> *"70% for me is low. 80% medium and from 90% up is high. […] I think it is static… but maybe the sensitivity of the situation would make a difference as to how I perceived it. Like I said, if it is a scenario for something silly that wouldn't make a difference in my life, 90% is a high enough value. But if it is something important, like bank information, 90% isn't that high" (P9)*
>
> *"Depending on the information 90% is still frightening, but if it is something like weight, 80% is enough." (P12)*
>
> *"High would be 95%, medium and low I don't know. Medium… maybe 70% and low below that? But If it is something that I don't want to be shared then even*

[51] Because sensitivity is too much of a complex matter to be analyzed in one interview we decided to not approach it.

100% (would not be enough). But it it's something that I don't care, it would be lower. Maybe even what is medium and low would change." (P16)

"I would say 1 or 2 an hour is low, 2 or 3 medium and more than 3 is high. […] If I'm not busy, if it is a day I'm not doing anything […] then I wouldn't mind to spend all day (answering notifications)" (P4)

"Low is one every 4 hours. Medium one per hour, and high two or three per hour. […] I think it is not static. If I don't have anything to do I would like to answer… I even thought it was interesting to read (the scenarios)" (P11)

This shows that the effort put into the distribution of interruptions in regard to frequency, sensitivity and certainty would have been better used in designing a system that generated randomly distributed interruptions, with random levels of certainty, and in creating a broader number of scenarios, which would also avoid the feeling of repetition. The added effort for the participant would be to classify sensitivity and certainty, something that they were already doing implicitly. By doing this, we believe the results would have a higher validity than what was achieved.

6.4.1.6 Miscellaneous

Other aspects that were mentioned but given their very low frequency[52] did not warrant their own subsections were:

- **external factors** during the study that made them become more or less concerned about privacy (one participant (P17) mentioned the FBI vs Apple case)
- **inherent biases** against the concept of IoT or against the concept of an intelligent agent
    - *"I was not surprised the chair wanted to know my weight, because the internet of things exists and that by itself is an absurd" (P20)*
    - *"I understand (the possibility of this type of system), but I don't want a personal assistant." (P20)*
- **Inability to change decisions** after pressing send hindered the participants' ability to give better answers that they thought after the fact.
    - *"Sometimes I would answer and press send, and a couple of minutes later I would think: 'Oh, I should have selected or deselected that box'*

[52] Usually reported by just one participant.

And there was no return mechanism. […] I don't think there were any unrelated answers, but I could have answered some better." (P20)

- **Issues using the app** led one participant to be redirected to the scenario option even when s/he wanted to delegate it directly after pressing send hindered the participants' ability to give better answers that they thought after the fact.[53]

6.4.2 Mental Process for Delegating or Choosing

The majority of participants, as could be noticed from the previously presented data, had a similar mental process to make their decision. From the interviews the process was as shown in Figure 27. The first step was to examine the current situation. If there was something extreme about the participant's mood, situation (either focus or interaction), or the patience towards the user study the interruption would be delegated directly or ignored. The choice between these two varied too much between participants. One possible reason for this variability could be related to the semi-static variables: need for control, trust and privacy concern.

"Not even (when I couldn't answer) did I delegate it directly to the agent. Because I didn't know what it was." (P8)

"I think I did (delegate directly) sometimes. I think I was back in São Carlos during class and I couldn't have my phone out for long." (P15)

"I'm not going to let it decide if I wasn't me who told it what to do" (P3)

The majority of participants actually avoided delegating directly and preferred to ignore the interruption because the first translated as a loss of control, while the latter was interpreted as a "do nothing" option.

"To delegate directly meant that I was giving the machine power to decide over something that might have been serious and that I wouldn't see. […] When I ignored it meant that it wouldn't do anything." (P9)

Others pointed out the fact that even when they were delegating directly they would have an extra step to go through. So they would rather ignore it completely.

[53] Both the button and the message would redirect to the scenario. But only the button would redirect to delegate.

> *"Many times (I ignored it) because I couldn't answer at the moment and even when I delegated directly I had to answer other things. If I could just delegate (without answering anything) I would." (P18)*
> *"Actually, I think that that's another reason why I wouldn't delegate directly. Because even when I did I would have to answer things. So I knew it would still take time. So when I was extremely busy I would do nothing." (P17)*

If the context was within normal expectations, the participants verified how much they cared about the situation being presented or as some put it: the risk associated. For some that meant the trustworthiness of the requester ("If said 'not trustworthy' I never allowed it." (P8)), for others the type of data or a combination of factors. If they did care about the data, they wanted to choose. If not, the system certainty and the perceived gain or benefit seemed to be weighted in.

> *"When it was something really private, 'Something wants your bank information', advertisement, or that chair… then I would choose. When I thought that the data would be put to good use, then I would delegate." (P9)*

It seems that the context was only considered at the end of the thought process as a way to balance how many interruptions would actually be desired. In a way it did not influence the decision directly, but served as "effect multipliers". For example, if it were something that the participant did not care about, the use was reasonable but the confidence was only okay, then the workload level or interaction level would come into consideration.

The described process was extracted from common behavior that was mentioned and organized in such a way that matched different situations described. However, no participant reported all of the steps in this exact order. Some never mentioned the certainty or the benefits, some gave context a higher focus then others. This process is an overall view that has to be personalized for each user.

Another important caveat is that this process was extracted from this particular group of participants and, as such, relates to people with a high privacy concern, medium-low trust in technology, and high need for control. However, even as the user study progressed, participants reported slight changes to their own mental process. Some user reported becoming increasingly annoyed *("I tried to be consistent, but as I was getting more annoyed by the end of it I started delegating directly more interruptions." (P9))*, others said it might be that they understood better or got more comfortable with the idea *("By the end I started delegating more. I don't know if I started to understand better the proposal or if I just got used to the idea of delegating. But I think I changed a bit in the end" (P5))*, and others saw

it as a decrease in concern *("I was delegating less at the start, but later I started to delegate more because I started to 'calm down'") (P4))*. This shows that this process, as privacy, is individual and dynamic. One particular actually reported all three aspects:

> *"I started to delegate more at the end because I started to get tired of answering. At first I answered everything, or ignore the ones I couldn't answer […] By the end of the study I realized what type of questions it was asking me and I realized I could delegate more without knowing. It wasn't life or death." (P18)*

6.4.3 Agent Design Recommendations

While the focus of the user study was not to extract requirements and recommendations for the design of the intelligent agent, during the interview several participants made comments that have led to a small compilation of such observations. Some of these suggestions could also be applied to the design of the user study which could lead to a better experience and data collection.

6.4.3.1 Smartphones may not be the best tool

For a user study using ESM, a smartphone is a fairly powerful and adequate tool. Nevertheless, during the interviews it was possible to note that it may not be the best interface for an agent, or at least not the only one.

While some of the missed interruptions were caused by a lack of desire to delegate the decision to the agent or a lack of time to dedicate to the study, when asked to think about why there were so many missed interruptions, the majority of participants said it was because they do not constantly pay attention to their phones.

This behavior was explained in different ways. One was because the participants do not keep the phone physically close to them at all times. Another was because they do not pay attention to it during work hours. And some participants pointed out the fact that they would sometime silence their phones for different reasons and forget it like that, causing them to miss interruptions[54].

[54] See comments when discussing rudeness for more examples.

"Sometimes I was in a different place and I received an interruption and I didn't even know it was happening." (P15)

"Sometimes I would leave my phone in one place and go do some other thing. I really don't pay that much attention to what I'm doing on my phone." (P5)

"Usually when I am busy and focused at work and my phone vibrates I don't even notice it. Sometimes I'll say: 'I'll check it later'. And then I forget." (P20)

"Another reason was that I would put it on vibrate to not be bothered. But what happened was that I forgot it like that and it stayed like that for a while." (P8)

"I always leave my phone on vibrate. So it doesn't make any noise and if I'm not really paying attention I don't notice it vibrated." (P19)

"I'm not a person who is with their phone all the time. Business hours was a bit complicated. Clothes with no pockets (meant) the phone wasn't with me. It would stay in the office." (P18)

"During work my phone isn't with me." (P16)

And in fact, more than one participant reported paying more attention to their phones during the study than they normally do.

"In most cases it was because I forgot the phone somewhere. […] During the study I was trying to keep the phone with me way more than after it ended. And I still missed a bunch of interruptions." (P4)

"I tried to answer them all, but some I missed. I tried to keep my phone with me at all times." (P7)

Lastly, one participant noticed that there are already many notifications on their phones. So the study notifications got mixed up with those.

"It was the same sound as Whatsapp and two groups. But I couldn't leave those groups. So sometimes I would run to check the notification and it was from the groups." (P7)

However, when questioned about the possibility of having the notification being delivered from different devices there was some agreement that it might increase their chances of seeing it. With only one (P17) participant saying that it would not matter, because at times he prefers to be completely unplugged and some stating that for the devices they own the smartphone would still be the best choice.

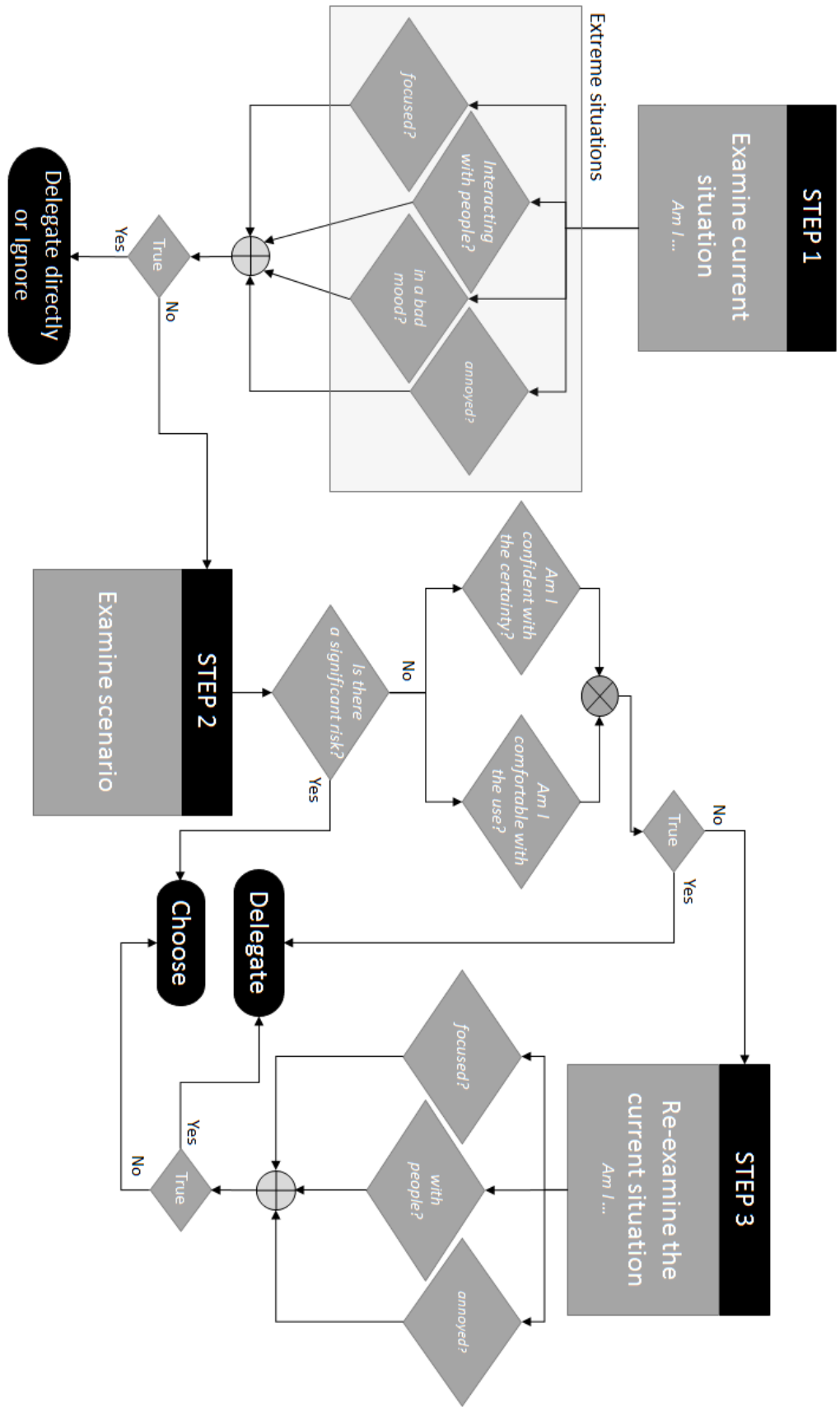


Figure 27. Mental process extracted from the interview

6.4.3.2 Dashboard

To try and understand why participants lost interruptions and what could be done to reduce them, one of the questions was if being notified that they were missing interruptions would make the participants pay more attention to their phone. A few agreed with this, saying that it would be nice to know when they missed interruptions *("I think it would be cool to know when I'm missing them so I can be more attentive" (P12))***,** a few said it would have no effect on their level of attention *("I don't think it would matter, I would be like 'Oh, ok. Great.'" (P5))*, but most said that it would make them anxious *("Since I wouldn't be able to go back and answer things to tell me I missed things would only make me anxious" (P9))***.** It was suggested by participants that this notification should happen once or twice a day with all missed interruptions in an aggregate form to avoid adding up the interruption count.

However, one discussion that arose from this was related to how an agent should deal with informing its user of missed, dismissed and delegated interruptions. In par with the characteristics of this group, participants generally agreed that they would like to have some sort of dashboard or notification that aggregated information about these interruptions and the decisions made for them, even if they would not check it frequently.

> *"I think I would want some sort of report. If something went wrong, why it did. Or maybe if I'm bored one day. But I don't think I would check it." (P15)*
>
> *"I think I would like a log so I could revise it." (P11)*
>
> *"What it did and didn't do, like a history. I could even see if I need to change something in the agent that I don't agree with" (P16)*
>
> *"I would like a history, a dashboard. For example, 'Today I delegated 50 things. What did you delegate? Here. Take a look'. It should be categorized and prioritized somehow. 'You lost so much money, or gave your localization to that many people'[55]" (P17)*
>
> *"For me it could decide and tell me later. Like: 'Here this happened and you didn't answer so I did this.' So that I could know what it did. […] I could say what was good and what needed to change I would change." (P21)*
>
> *"For example, let's say that for interruptions I missed [the agent] made a decision. I would want to be able to review these decisions to know if I approve*

[55] This is very close to the approach used by Almuhimedi et al. (2015) as a way to make people more aware of their privacy and data sharing.

them or not. It is a matter of checking what it is doing, basically…. Lack of trust in the technology" (P18)

6.4.3.3 Shortcut for high workload moments

As seen on the results from the data collected during the study, the interruptions were poorly perceived in some situations, e.g. while driving or doing daily chores. During the interviews some participants said that they ignored and/or dismissed interruptions because they were busy attending to other things:

"I think lack of time. You think: 'Oh, I'm busy. I'll check it later.' And when you went to check it, it wasn't there anymore." (P9)

"Sometimes I was in the middle of driving and even to delegate there were additional buttons to press. So I just ignored it." (P18)

This does not apply to the agent, since it should know that the user is in a high workload moment and cannot be interrupted. The agent could incorporate this knowledge by allowing 'snoozing' for situations where participants should not have interrupted, but since they did the user is now aware and concerned.

These comments show that if there were a shortcut for the participants to state these moments in the user study, more data could be extracted from the missed interruptions. This shortcut could work as the "Others" on the delegate option. That is, the participants could select it in a way to state "I cannot answer this now" and later on they could revise the moments they did this and offer further information.

One important thing to note about this approach of shortcut-then-more-information is that the participants should be reminded to add more information and that there should options for the user to choose from. The latter was noticed when a participant stated:

"If there was an option to check I would check it." (P9)

6.4.3.4 Policies and End-User Programming

One of the approaches suggested by the participants was the use of user pre-defined policies to inform the agents decision to share or not information, as well as the decision to interrupt or not the user. Based on this the system could continue learning and inferring decisions and the user would be able to modify and adapt them whenever s/he desired. As discussed in Chapter 2, this approach has been explored. In fact, the variables defined for

the Intelligent Privacy Interruptions could be used to inform on which aspects are necessary for these policies and which aspects should be made available for configuration for the end-user programming. However, it is not a trivial approach and when one participant was asked to specify a bit more about this rules he soon realized the complexity.

> *"I would create a rule, for example, to never share my SSN. There. That's a rule. There's no need for a scenario. (And in situations that weren't approached by rules) then it can ask, because it doesn't know. (So you would only like the system to ask you if it didn't know) Yes. If based on the rules I established he couldn't do it… okay, this is an intelligent system and not just a rule follower. So if he could make an inference with a high degree of certainty, well… then certainty could be part of the rules. Yes, then for example, … well… I don't know." (P20)*

From the comments throughout the interviews one possible approach is to use rules and end-user programming for absolute situations. For example, one approach could be to have different types of rules.

- **Dogmas** would be absolute truths that the agent should not diverge from no matter the value of other indicators. They could be characterized by the presence of "always" and "never".

  "Never share my SSN without asking me first" (P20)
- **Rules** would indicate strong preferences that would lead to corrective behavior if not followed. They would be similar to dogmas, only they would allow for exceptions.

  "Do not interrupt me if I'm sleeping (unless for phone calls)" (P20)
- **Guidelines** would indicate preferred behavior, but would allow the agent to analyzed previous behavior and current factors to decide whether to follow it or not.

In this case, the user would be only one able to define dogmas. While the agent could use observed behavior to create further guidelines, which could go up the hierarchy if frequently observed and/or if confirmed by the user *("Even if it learned, it has to confirm it with me before adding this rule to the database" (P3))*

Lastly, one interesting observation is that the majority of participants reported starting to wonder and pay more attention about their sharing habits online. It is not known if this effect could be lasting or not, but it does indicate that education and creating awareness is an important method to improve privacy practices. This could be approached separately

from the technology perspective, but when brought to it, it reinforces the notion that it is particularly important to keep the user in the loop when in the context of privacy decisions.

6.5 Discussion

As there were many different aspects to explore in this user study the discussion will try to follow the same structure of the results to ease the understanding. The first aspects that will be discussed are the demographical and personal characteristics of the user study group, how they match-up against that of the online survey and what it meant for the study. This will be followed by a discussion about what affected the three different groups of users that were considered: delegators, watchers and choosers. In the sequence a discussion of the variables that influenced the decision to delegate directly, see and choose and see and delegate is presented. Observations and possible patterns are indicated, discussing how they can be used to inform privacy agents in choreographed solutions. Lastly, results from the two self-report moments will be discussed: the self-report of the influence of variables and the self-report on sharing and control preferences. During the whole discussion, aspects learned from the interviews will be used to reinforce or contradict the data collected. However, the results from the interviews will not be individually treated in this section because threats to validity and improvements on user study will be treated in the limitations section; mental process is associated with the analysis what affected the participants' decisions; and agent design is not the focus of this work, so their presentation and brief discussion should suffice.

The first thing that is important to discuss are the characteristics of the group that participated in the user study. Throughout the presentation of results for the demographics and personal characteristics, the data obtained from the user study was compared to that obtained from the online survey. The demographics of the group that participated in the user study were similar to the demographics of the group that participated in the online survey. However, this group is younger, more tech savvy, and a bigger consumer of technology. Yet they have a lower use, or different perspective[56], of traditional technology assisted applications.

[56] There was an increase in others, which means that they either perform activities outside of the ones listed or that they view them as being outside of the ones listed.

Considering aspects of trust, this group also showed to be slightly more trusting of technology then not. But since the higher frequency of scores were found for values at or closer to neutral it does not imply that they would necessarily rely on technology too much. As confirmed by the interviews, this was one of the reasons why the participants did not want to delegate information directly to the agent and wanted to at least know what was the scenario before feeling comfortable to do so.

This group was also biased against interruptions but unlike the participants of the online survey, they acted to avoid them. While being biased against interruptions could be a positive aspect for such an agent-based approach, for ESM studies this can lead to annoyance with the number of interruptions. This was indeed observed on this user study since the “mood” variable and “frequency” variable started to be reported as reasons to delegate directly only/more on the second half of the study, as well as agrees to some of the comments from the interviews. Another issue for ESM studies is because this group reported acting to avoid interruptions. As reported in the interviews, one of the reasons why some of the participants missed interruptions was because they had silenced their phones. This was particularly true during “non-appropriate” moments, which could be responsible for the fact that so few interruptions were perceived as rude.

Related to privacy, this group tended towards fundamentalists levels of concern over privacy. As shown from the results on the online survey, this did not necessarily reflect on the stated engagement of privacy behaviors. Finally, related to their need for control, user study participants also had a higher desire for control. However, there was a considerable difference between those that scored 40 and 48 out of 50 points in the user study and in the online survey, showing the presence of extremes within the group. Both facts are in line with the comments made during the interviews that the participants wanted to at least know what was happening, be that before an action is taken or through a report-like dashboard in the application. This is also in line with the fact that no participant was categorized as a “delegator”.

Even though no participants were delegators, it was possible to examine if they would be “watchers” or “choosers”. By using ANOVA and Pearson Correlation for the qualitative and quantitative variables, respectively, it was possible to note that *privacy concern* was a significant variable. *Trust* and *need for control* were not highly correlated, but the nature of their relationship matches our expectations. Trust was positively correlated with being a watcher and need for control was negatively correlated. While these relations were to be

expected, it was interesting to note that no significant relations were found for the demographic variables: gender, age group and computer literacy.

After understanding a bit more as to what makes a person be a “watcher” instead of a “chooser”, the issue of understanding what influenced the decision to delegate directly was approached. Given the reported frequencies of *activity engagement*, *social acceptance*, *mood* and *frequency* it became clear that high activity engagement was the biggest reason why people preferred to delegate directly, followed by a distant social acceptance. However, it is interesting to note that in extreme workload situations some participants chose to ignore the interruption instead of delegating because of the extra step necessary when delegating. It is possible that if there were a shortcut for these situations, there would have been more directly delegated interruptions, maybe even leading to participants becoming “delegators”.

It is also interesting to note that participants became tired from the number of interruptions and started delegating more after the second half of the study. While this was reported in the interview, it is possible that an external reason had an effect. Because there was a delay with the start of classes, they only started on the last three days of the user study and about a quarter of participants were involved with classes either in a teaching or attending capacity. However, it was also after the second half that mood and frequency variables started being reported as reasons to delegate directly, which reinforces the comments obtained in the interviews.

All in all, these results show that solutions that reduce the number of required interruptions over time will most likely be beneficial to its users, since a high frequency of interruptions starts to become an issue when the exposure becomes too long. It also shows what interruptibility research has long explored: that people should not and do not want to be interrupted during high workload moments. This works adds to this knowledge by noting that this appears to be true even in situations where privacy is on the line.

The last aspect to discuss about the interruptions that were delegated directly is that they seem to be normally distributed during a day apart from lunch hour. That is, we observed that the number of directly delegated interruptions increased up until lunch time and then decreased until the end of business hours. This could be because the workload tends to lower at the very start and end of the business day. However, if this trend is observed in other and broader studies it could serve as a temporal indicator to the privacy agent of when its user is less likely to want to be interrupted, without having to measure workload and interaction levels.

Moving on to the situations where the participants saw the interruption and then decided to delegate or to choose, it was observed that not all variables were relevant. Considering the internally controlled variables, frequency, certainty and sensitivity, we observed that frequency did not have a significant relation with making the decision to choose or to delegate. This is different from what was observed from directly delegated, where as time went on and the participants started to get tired of the interruptions, frequency started being reported as more significant. Nevertheless, this matched what was reported in the interviews, where no participant mentioned deciding to delegate because they were receiving too many interruptions. On the other hand, medium and high certainty seem to influence participants towards delegating more, but with a lower impact than medium and high sensitivity had towards choosing more. This also matches participants report that they first checked the scenario, then the certainty.

Considering the report made by the users about the importance of the composing aspects of the scenario (*what*, *who* and *why*) and certainty on their decision, *who* was the only factor that positively impacted the decision of choosing. *Certainty* and *why* had a negative impact, while *what* was not considered relevant for informing this decision as it was frequently reported in both situations. This shows us that while knowing the sensitivity of the scenario should be important to inform the agent's decision to give back control or not, it is also important to know the individual aspects of the sensitivity, as they can indicate different behaviors. Nevertheless, it is important to note that for these aspects we had no information about how users perceived them, just that they were perceived as important. From the interviews and knowledge obtained from previous literature we can extrapolate some relations.

Because the type of data was frequently considered relevant by the participants and because it was what many participants reported as being the first thing they checked, it is possible to infer that only high levels of certainty would warrant being reported as relevant. That is, if the certainty was low, the concern over the data type would be more predominant and overpower the relevance of certainty on the decision.

Also, motives that did not yield benefits or did not seem reasonable were the situations that influenced participants to report them as being relevant. Acceptable motives were not as impactful. This is based on the comments that participants could remember more strongly the negative situations (e.g. the chair) than the positive ones. Similarly, not trustworthy requesters would be responsible for the higher frequency of being reported as relevant when deciding to choose, because they meant for these participants an increase in

risk. On the other hand, trustworthy requesters were not reported in the interviews as possible reduction in risks.

Lastly, considering the variables associated with if the user “can” be interrupted, while *mood* and *social engagement* (workload and social interaction, in this study) were reported as having more-than-random significance, only the social engagement aspects were considered relevant when informing the decision to choose or the delegate. However, it is important to take these particular results with a grain of salt since the statements for *mood* and *social acceptance* were the two variables that reported the most variability in interpretation.

It is interesting to note that the results obtained from the data and the mental process created from what was reported in the interviews seem to be significantly consistent. This shows that participants had a high ability to report on past behavior. When comparing the self-reported influence of variables at the end of the study with those of the online survey it was possible to note that participants of the user study were able to report with more accuracy which were the aspects that influenced them and by how much (NS meant a medium level of influence and “not sure”). Even though there were significant differences between the groups and the format for the self-report, this is highlights the issue of performing research that explores behavior and preferences for a context that does not exist. While self-report should never be the only method used, hindsight offers valuable information for participants. If the participants have no previous behaviors to rely on, their reported attitudes will most likely be significantly different from future observed behavior.

Another result that could highlight the effect of participating in the situation that is being required to be reported was the number of changes in the level of concern and sensitivity. Overall there were significant changes in preferences reported at the beginning of the study and at the end for individual scenarios. This could be due to the influence the study had on participants or it could simply be because of time. To verify this, we ran a follow-up experiment with a control group that went through no intervention. The results of this study will be analyzed by the undergraduate student Gabriela Mattos as her own research project.

6.6 Limitations

In this study there following limitations were identified. They have been discussed throughout this chapter. For this reason, this section will list and briefly discuss them:

- Sample size: this study was conducted with a limited number of participants.
    - Reason: the amount of effort required by participants
    - Effect: the findings of this study are ***only indications*** of possible behaviors.
    - Possible approach: re-conduct this study with a much larger population.
- Sample characteristics: this study was conducted with a very specific type of participants.
    - Reason: possibly because of how the participants were selected. A majority were participants that have privileged knowledge of computers.
    - Effect: the findings of this study are ***not generalizable*** for users with different characteristics.
    - Possible approach: re-conduct this study with a more diverse population.
- Different interpretations: participants had different views of what the study application was representing, as well as from some of the variables.
    - Reason: because participants and research group were not co-located, the tools to explain the user study were made available through video and texts.[57]
    - Effect: results may ***not reflect reality***.
    - Possible approach: on future studies, reserve additional time to clarify with each participant individually the different aspects of the study.
- Perception of controlled variables was not consistent throughout participants or scenarios: participants showed a great diversity of opinions as to what the different levels of certainty, frequency and sensitivity meant.
    - Reason: opinions vary given previous knowledge and personal characteristics. Also, different aspects on the scenario lead to changes in perception.
    - Effect: results may ***not reflect reality***.
    - Possible approach: on future studies, have participant classify each presented scenario individually on frequency, certainty and sensitivity.

[57] Participants had the opportunity to contact the research group to clarify issues, but that mostly did not happened or only happened during the user study.

- Issues with the study design: not all combinations of sensitivity and certainty were available throughout the study.
    - Reason: when moving from the format of the pilot study to the user study, there was a problem updating the file that stored these combinations.
    - Effect: results may ***be skewed***.
    - Possible approach: on future studies, have multiple researchers verify the code distribution. However, given the previous listed limitation, it would be best to avoid predefined combinations all together.
- Not real: for some participants the study and some scenarios were consciously not perceived as real.
    - Reason: for the scenarios it was a matter of not matching expectations of existing technologies and not matching their current situation. For the study it was a matter of knowing it was a study.
    - Effect: results may ***not reflect reality***.
    - Possible approach: on future studies, try to match the presented scenarios with the participants' context (in the least invasive manner as possible). The perception that it was just a study could only be removed if some sort of deception was used.
- Not individualized analysis: the analyses made in this chapter were related to the results obtained from all participants.
    - Reason: there was both a time constraint to analyze each participant's results individually and for some participants there were not enough data points to extract statistically meaningful data.
    - Effect: results may ***not reflect individual differences***.
    - Possible approach: analyze the data collected for everyone, when possible. If this can be done prior to the defense, participants dossiers will be added as appendix.

Other identified limitations were reported by a very low number of participants, usually just one for each, and can be considered part of the inherent noise of user studies.

6.7 Conclusion

This study explored the effects of the different variables in the preference to delegate or withhold control in a more realistic situation than the online survey. Using experience sampling we exposed participants to possible scenarios that could be part of the Internet of Things and requested them to define the preferred behavior expected from an agent. The participants would also characterize their context based on the variables identified in the literature.

While it would be desirable to say that certain combination of variables lead to this behavior or that one, given the limitations of this study it is not possible to generalize nor to confidently state that. However, this study does show that for this particular group there seems to be a significantly consistent mental process that guides the participants' decision making. This process was consistent with reported behaviors on the interviews as well as collected data. However, it needs to be adapted for each participant individually to account for individual preferences. Nevertheless, this mental process is a stepping stone towards informing privacy agents on how to balance their own autonomy and user control based on user preferences.

Chapter 7

Conclusion and Future Work

In the Internet of Things everyday devices and appliances (“things”) are imbued with networking and processing capabilities; even those that are traditionally standalone. The goal is to allow these different and heterogeneous “things” to communicate and exchange data to provide new and better services to its users. With the level of data communication that will come from billions of devices exchanging data, privacy becomes an important concern. While automated solutions suffer from a lack of user awareness of what is happening, orchestrated solutions (based on “notice and consent”) suffer from an excess of it. Considering the scale of the Internet of Things it becomes infeasible to have users consent for every interaction. Because of this, an approach that is being used is that of choreographed solutions. These solutions are found between orchestrated and automated solutions in their balance of system autonomy and control. In general, choreographed solutions are agent-based solutions that have some sort of intelligence imbued.

In this work an important gap in the design of these privacy agents was addressed. Broadly speaking, this gap refers to usability and its dimension of user satisfaction. More specifically it deals with the issue of balancing the system’s autonomy over the decision-making process and the level of user control desired and appropriate.

Previous work on choreographed solutions have heavily focused on developing agents that could make correct decisions based on privacy preferences, which is, by no means, an easy task. Nevertheless, this left the issue of usability and user satisfaction on the sidelines, usually mentioned as future and necessary work, or not at all.

A well-known fact from Human-Computer Interaction is that for users to be comfortable and to adopt new technologies they must feel empowered and in control. This thesis identified aspects that can aid in achieving this in privacy agents by informing them as to when to add the user to the loop not only because it is necessary, but also if that is desired by the user.

These aspects were identified through literature review and cover aspects of interruptibility (mood, social acceptance, frequency of interruptions and social expectation), as well as aspects related to receptivity and privacy that may increase users' desire to be interrupted to decide themselves (privacy concern, trust, need for control, sharing sensitivity and system certainty). The identification, discussion, and grouping of these variables led to the creation of what was called **Intelligent Privacy Interruptions**.

Since these variables were identified in diverse literature, mostly with a different focus, we have performed two user interventions to validate if they would apply to the context of this thesis. The first one was an online survey that had two goals. The first was to obtain more information about the demographics and characteristics for a sample of the Brazilian population. This was important because there were no scales and questionnaires that were designed for the purposed we intended, nor that were validated for the Brazilian culture. *This is an avenue of future work that was identified as necessary and that should be explored*. As such, we have adopted and adapted previously used measurements and established a baseline for comparison in the subsequent study. The second goal was to perform an initial validation, a sanity check, that the variables identified in the literature would be in general agreement to the users' expectations.

From this survey, it was possible to note an overall general agreement with the variables extracted from the literature. Some were reported as relevant more frequently than others. In fact, certainty, which is currently the most commonly used variable to decide to interrupt a user for further information, was not as frequently reported as expected. Furthermore, social expectation was less frequently reported as an influencer than most.

This survey, however, was a very simple verification, using quasi-binary options and not requiring participants to classify the variables in their order of preference. This was done because, within the research group, we witnessed difficulties in predicting influence for a non-real situation. However, it needed further verification before conclusions could be drawn.

This was tackled in our experience sampling-based user study. While this study has its own limitations that could lead to skewed results and hinders its generality, it yielded significant contributions. One of them was the identification of the possibility that users can be grouped as **delegators, watchers,** and **choosers** and that identified variables had statistically significant relations with this groups – namely privacy concern, trust and need for control. Thus, a*nother line for future work lies with using better designed tools and scales for user characterization (trust, privacy concern and need for control) to further verify the*

nature of these relations. If this can be done, it would make it easier for privacy agents to select appropriate behavior.

Another contribution that stemmed from this study was the indication that the set of **Intelligent Privacy Interruptions can be simplified and refined**. Simplification, for instance, can be achieved by removing the social acceptance variable. This aspect showed not to be a significant variable and was correlated by the participants with activity engagement. Other variables that could be removed if further investigations reinforce their lack of influence are mood and frequency. On the other hand, it was noticed that the definition of sharing sensitivity could be refined to account for the different aspects that compose it (in this work, who, what and why). This could help inform the behavior to be taken when dealing with users classified as watchers or choosers. An associated contribution was **the identification of the nature of the relations** between sharing sensitivity (and its subparts), certainty, user workload and social interactions, with the decision of this sample of users to delegate or to choose after seeing the data request scenario.

As secondary contributions, it was also possible to identify and reinforce some of the **design recommendations for privacy agents.** For instance, a dashboard could allow users to keep tabs on what is being done and alter it if necessary. Another example is the use of end-user programming and promotion of observed behaviors from suggestions, to rules and dogmas. It was also possible to note that the use of a privacy agent on a smartphone can lead to many missed interruptions given the established behaviors of silencing phones and not paying it much attention since it is a source of (constant) interruptions.

Finally, the last contribution this thesis makes is the identification of a **mental process** that was used by the participants to inform their decision to delegate interruptions directly, or to see them and choose/delegate it. The identified mental process is restricted to the specific sample of the population that participated in the user study and *a broader study is necessary to verify if it is applicable to users in general, or if there are significant differences*. It is important to note, that this mental process still needs to go through *personalization steps to truly match the expectations of individual users* and that users reported **slight changes in the emphasis put into the different variables in this mental process as the interaction went on**.

With this we conclude that this research must be continued for the refinement of a decision model for the behavior of privacy agents based on the indications and insights

discussed in this thesis. As identified, an important step would be the development of more appropriate questionnaire and scales which could be used to categorize participants as delegators, choosers or watchers. This could be a first level of abstraction to inform the behavior of privacy agents. Another important step would be to improve the user study application and design to account for the identified limitations and run a broader and more longitudinal study. This way the indications and observations found in this thesis can be verified or refuted with increased validity.

Bibliography

ACKERMAN, M. S. Privacy in pervasive environments: Next generation labeling protocols. **Personal and Ubiquitous Computing**, v. 8, n. 6, p. 430–439, nov. 2004.

ACQUISTI, A. Complementary Perspectives on Privacy and Security: Economics. **IEEE Security and Privacy**, v. 11, n. 2, p. 93–95, mar. 2013.

ACQUISTI, A.; ADJERID, I.; BRANDIMARTE, L. Gone in 15 Seconds: The Limits of Privacy Transparency and Control. **IEEE Security and Privacy**, v. 11, n. 4, p. 72–74, 2013.

ACQUISTI, A.; GROSSKLAGS, J. Privacy and Rationality in Individual Decision Making. **IEEE Security and Privacy**, v. 3, n. 1, p. 26–33, jan. 2005.

AGIR, B.; CALBIMONTE, J.-P.; ABERER, K. **Semantic and Sensitivity Aware Location Privacy Protection for the Internet of Things**. (S. Decker et al., Eds.)Proceedings of the 2nd International Conference on Society, Privacy and the Semantic Web - Policy and Technology - Volume 1316 (PrivOn'14). **Anais**...Aachen, Germany: CEUR-WS.org, 2014

ALMUHIMEDI, H. et al. **Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging**. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). **Anais**...New York, NY, USA: ACM, 2015

AN, X.; JUTLA, D.; CERCONE, N. **Reasoning about obfuscated private information: who have lied and how to lie**. Proceedings of the 5th ACM workshop on Privacy in Electronic Society (WPES '06). **Anais**...New York, NY, USA: ACM, 2006

ANDERSEN, M. S.; KJARGAARD, M. B.; GRONBAEK, K. **The SITA principle for location privacy — Conceptual model and architecture**. Proceedings of the 2013 International Conference on Privacy and Security in Mobile Systems (PRISMS '13). **Anais**...Washington, DC, USA: IEEE, 2013

BAINBRIDGE, L. Brief paper: Ironies of automation. **Automatica**, v. 19, n. 6, p. 775–779, 1983.

BARKHUUS, L. **The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI**. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’12). **Anais**...New York, NY, USA: ACM, 2012

BARKHUUS, L.; DEY, A. **Location-Based Services for Mobile Telephony: a Study of Users ’ Privacy Concerns**. Proceedings of the 2003 IFIP TC13 International Conference on Human-Computer Interaction. **Anais**...2003

BELCHER, J. et al. **NotiFly: Enhancing Design Through Claims-based Personas and Knowledge Reuse**. (M. Guimarães, Ed.)Proceedings of the 43rd annual Southeast regional conference - Volume 2 (ACM-SE 43). **Anais**...ACM, 2005

BELLOTTI, V.; SELLEN, A. **Design for privacy in ubiquitous computing environments**. (G. de Michelis, C. Simone, K. Schmidt, Eds.)Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work (ECSCW’93). **Anais**...Norwell, MA, USA: Kluwer Academic Publishers, 1993

BILOGREVIC, I. et al. **Adaptive information-sharing for privacy-aware mobile social networks**. Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing (UbiComp ’13). **Anais**...New York, NY, USA: ACM, 2013

BORGESIUS, F. Informed Consent: We Can Do Better to Defend Privacy. **IEEE Security & Privacy**, v. 13, n. 2, p. 103–107, 2015.

BORST, J. P.; TAATGEN, N. A.; VAN RIJN, H. **What Makes Interruptions Disruptive?: A Process-Model Account of the Effects of the Problem State Bottleneck on Task Interruption and Resumption.** Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI ’15). **Anais**...New York, NY, USA: ACM, 2015

BOYLE, M.; GREENBERG, S. The Language of Privacy: Learning from Video Media Space Analysis and Design. **ACM Transactions on Computer-Human Interaction**, v. 12, n. 2, p. 328–370, jun. 2005.

BRADSHAW, J. M. et al. **Kaa: policy-based explorations of a richer model for adjustable autonomy**. Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems (AAMAS ’05). **Anais**...New York, NY, USA: ACM, 2005

BROENINK, G. et al. The Privacy Coach: Supporting customer privacy in the Internet of

Things. **CoRR**, v. abs/1001.4, 2010.

BUNNIG, C.; CAP, C. H. **Ad Hoc Privacy Management in Ubiquitous Computing Environments**. Proceedings of the 2009 Second International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC '09). **Anais**...Washington, DC, USA: IEEE, 2009

BURGER, J. M.; COOPER, H. M. The Desirability of Control. **Motivation and Emotion**, v. 3, n. 4, p. 381–393, 1979.

BUSCH, M.; HOCHLEITNER, C.; TSCHELIGI, M. **Is This Information Too Personal? The Relationship between General Information Privacy Concerns and Personality**. Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS '14). **Anais**...Menlo Park, CA: USENIX Association, 2014

CALO, R. Tiny Salespeople: Mediated Transactions and the Internet of Things. **IEEE Security & Privacy**, v. 11, n. 5, p. 70–72, set. 2013.

CAVOUKIAN, A. **Privacy by Design**Toronto, 2011. Disponível em: <www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>

COLNAGO, J.; GUARDIA, H. **How to Inform Privacy Agents on Preferred Level of User Control ?** Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16). **Anais**...ACM, 2016

CONSOLVO, S. et al. **Location Disclosure to Social Relations: Why, When & What People Want to Share**. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05). **Anais**...New York, NY, USA: ACM, 2005

COPIGNEAUX, B. **Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the Internet of Things**. Proceedings of the 2014 World Forum on Internet of Things (WF-IoT). **Anais**...Washington, DC, USA: IEEE, 2014

COUGHLAN, T. et al. **Tailored scenarios: a low-cost online method to elicit perceptions on designs using real relationships**. CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13). **Anais**...New York, NY, USA: ACM, 2013

DABBISH, L. A.; BAKER, R. S. **Administrative assistants as interruption mediators**. CHI '03 Extended Abstracts on Human Factors in Computing Systems (CHI EA '03).

Anais...New York, NY, USA: ACM, 2003

DAVIS, F. D.; BAGOZZI, R. P.; WARSHAW, P. R. User acceptance of computer technology: a comparison of two theoretical models. **Management Science**, v. 35, n. 8, p. 982–1003, 1989.

ELKHODR, M.; SHAHRESTANI, S.; CHEUNG, H. **A contextual-adaptive Location Disclosure Agent for general devices in the Internet of Things**. Proceedings of the 2013 IEEE 38th Conference on Local Computer Networks Workshops (LCN Workshops '13). **Anais**...Washington, DC, USA: IEEE, 2013

ERCOLINI, D. A. G.; KOKAR, M. M. Desktop Agent Manager (DAM): Decision Mechanism. **International Journal of Human-Computer Interaction**, v. 9, n. 2, p. 133–149, jun. 1997.

EUROPEAN COMISSION. **Factsheet on the "Right to be Forgotten" ruling (c-131/12)**. [s.l: s.n.].

EVANS, D. **The Internet of Things - How the Next Evolution of the Internet is Changing Everything**CISCO, , 2011.

EVANS, K. Where in the World Is My Information? Giving People Access. **IEEE Security & Privacy**, v. 12, n. 5, p. 78–81, 2014.

FALCONE, R.; CASTELFRANCHI, C. The human in the loop of a delegated agent: The theory of adjustable social autonomy. **IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans**, v. 31, n. 5, p. 406–418, set. 2001.

FEREIDUNIAN, A. et al. **Adaptive autonomy: Smart cooperative cybernetic systems for more humane automation solutions**. 2007 IEEE International Conference on Systems, Man and Cybernetics. **Anais**...2007

FISCHER, J. E. et al. **Effects of content and time of delivery on receptivity to mobile interruptions**. Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI '10). **Anais**...New York, NY, USA: ACM, 2010

FISHER, R.; SIMMONS, R. **Smartphone Interruptibility Using Density-Weighted Uncertainty Sampling with Reinforcement Learning**. Proceedings of the 2011 10th International Conference on Machine Learning and Applications and Workshops (ICMLA '11). **Anais**...Washington, DC, USA: IEEE, 2011

FLEMISCH, F. et al. Towards a dynamic balance between humans and automation: Authority, ability, responsibility and control in shared and cooperative control situations. **Cognition, Technology and Work**, v. 14, n. 1, p. 3–18, 2012.

FTC STAFF REPORT. **IoT Privacy & Security in a Connected World**. [s.l: s.n.].

GAUD, N.; DEEN, A.; SILAKARI, S. **Architecture for discovery of context-aware web services based on privacy preferences**. Proceedings of the 2012 Fourth International Conference on Computational Intelligence and Communication Networks (CICN ’12). **Anais**...Washington, DC, USA: IEEE, 2012

GELLMAN, R. Willis Ware’s Lasting Contribution to Privacy: Fair Information Practices. **IEEE Security & Privacy**, v. 12, n. 4, p. 51–54, 2014.

GOMER, R.; SCHRAEFEL, M. C.; GERDING, E. **Consenting Agents: Semi-Autonomous Interactions for Ubiquitous Consent**. Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp ’14 Adjunct). **Anais**...New York, NY, USA: ACM, 2014

GOODRICH, M. A. et al. **Managing Autonomy in Robot Teams: Observations from Four Experiments**. 2007 2nd ACM/IEEE International Conference on Human-Robot Interaction. **Anais**...2007

GRANDHI, S.; JONES, Q. Technology-mediated interruption management. **International Journal of Human Computer Studies**, v. 68, n. 5, p. 288–306, maio 2010.

GÜRSES, S. Can you engineer privacy? **Communications of the ACM**, v. 57, n. 8, p. 20–23, ago. 2014.

HÄKKILÄ, J.; KÄNSÄLÄ, I. **Role based privacy applied to context-aware mobile applications**. Proceedings of the 2004 IEEE International Conference on Systems, Man and Cybernetics. **Anais**...IEEE, 2004

HARDIAN, B.; INDULSKA, J.; HENRICKSEN, K. **Balancing autonomy and user control in context-aware systems - A survey**. Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2006. **Anais**...IEEE, 2006

HARDIN, B.; GOODRICH, M. A. **On using mixed-initiative control: a perspective for managing large-scale robotic teams**. Proceedings of the 4th ACM/IEEE international

conference on Human robot interaction (HRI ’09). **Anais**...New York, NY, USA: ACM, 2009

HARR, R.; KAPTELININ, V. **Interrupting or not: Exploring the effect of social context on interrupters’ decision making**. Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design (NordiCHI ’12). **Anais**...New York, NY, USA: ACM, 2012

HEIJDEN, H. VAN DER. **Ubiquitous computing, user control, and user performance: conceptual model and preliminary experimental design**. Proceedings of the Research Symposium on Emerging Electronic Markets. **Anais**...Bremen, Germany: 2003

HENNE, B.; HARBACH, M.; SMITH, M. **Location privacy revisited: factors of privacy decisions**. CHI ’13 Extended Abstracts on Human Factors in Computing Systems (CHI EA ’13). **Anais**...New York, NY, USA: ACM, 2013

HENZE, M. et al. **User-Driven Privacy Enforcement for Cloud-Based Services in the Internet of Things**. Proceedings of the 2014 International Conference on Future Internet of Things and Cloud (FICLOUD ’14). **Anais**...Washington, DC, USA: IEEE, 2014

HO, J.; INTILLE, S. S. **Using context-aware computing to reduce the perceived burden of interruptions from mobile devices**. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’05). **Anais**...New York, NY, USA: ACM, 2005

HOFF, K.; BASHIR, M. **A Theoretical Model for Trust in Automated Systems**. CHI ’13 Extended Abstracts on Human Factors in Computing Systems (CHI EA ’13). **Anais**...New York, NY, USA: ACM, 2013

HOLVAST, J. History of Privacy. In: MATYÁŠ, V. et al. (Eds.). . **The Future of Identity in the Information Society**. [s.l.] Springer Berlin Heidelberg, 2009. v. 298p. 13–42.

HONG, J. I. et al. **Privacy Risk Models For Designing Privacy-Sensitive Ubiquitous Computing Systems**. Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques (DIS ’04). **Anais**...New York, NY, USA: ACM, 2004

HONG, J. I.; LANDAY, J. A. **An architecture for privacy-sensitive ubiquitous computing**. Proceedings of the 2nd international conference on Mobile systems,

applications, and services (MobiSys '04). **Anais**...New York, NY, USA: ACM, 2004

HUGHES-ROBERTS, T. **Privacy and social networks: Is concern a valid indicator of intention and behaviour?** Proceedings of the 2013 International Conference on Social Computing (SocialCom '13). **Anais**...Washington, DC, USA: IEEE, 2013

HUHNS, M.; SINGH, M. P. Service-oriented computing: Key concepts and principles. **IEEE Internet Computing**, v. 9, n. 1, p. 75–81, 2005.

HULL, R. et al. **Enabling Context-Aware and Privacy-Conscious User Data Sharing**. Proceedings of the 2004 IEEE International Conference Mobile Data Management. **Anais**...Washington, DC, USA: IEEE, 2004

ITU. **The Internet of ThingsITU Internet Reports - Executive Summary**. [s.l: s.n.].

JIN, H. et al. **Recommendations-based Location Privacy Control**. Proceedings of the 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '13). **Anais**...Washington, DC, USA: IEEE, 2013

KERN, N. et al. **A Model for Human Interruptability: Experimental Evaluation and Automatic Estimation from Wearable Sensors**. Proceedings of the Eighth International Symposium on Wearable Computers (ISWC '04). **Anais**...Washington, DC, USA: IEEE, 2004

KIM, J. et al. **Dynamic Privacy Management in Ubiquitous Computing Environments**. Proceedings of the 2010 Second International Conference on Communication Software and Networks (ICCSN '10). **Anais**...Washington, DC, USA: IEEE, 2010

KIM, J.-D.; SON, J.; BAIK, D.-K. CA5W1HOnto: Ontological Context-Aware Model Based on 5W1H. **International Journal of Distributed Sensor Networks**, p. Article ID 247346, 11 pages, 2012.

KIM, S.; CHUN, J.; DEY, A. K. **Sensors Know When to Interrupt You in the Car : Detecting Driver Interruptibility Through Monitoring of Peripheral Interactions**. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). **Anais**...New York, NY, USA: ACM, 2015

KORFF, S.; BÖHME, R. **Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation**. Proceedings of the Tenth Symposium On Usable Privacy and Security (SOUPS '14). **Anais**...Menlo Park, CA: USENIX Association, 2014

KORTENKAMP, D.; KEIRN-SCHRECKENGHOST, D.; BONASSO, R. P. **Adjustable control autonomy for manned space flight**. Proceedings of the 2000 IEEE Aerospace Conference. **Anais**...Big Sky, MT: IEEE, 2000

KUMARAGURU, P.; CRANOR, L. **Privacy indexes: A survey of westin's studies**. Pittsburg, PA: [s.n.].

LANGHEINRICH, M. A Privacy Awareness System for Ubiquitous Computing Environments. In: BORRIELLO, G.; HOLMQUIST, L. E. (Eds.). . **UbiComp 2002: Ubiquitous Computing: 4th International Conference Göteborg, Sweden, September 29 - October 1, 2002 Proceedings**. 2498. ed. [s.l.] Springer Berlin Heidelberg, 2002. p. 237–245.

LARSON, R.; CSIKSZENTMIHALYI, M. Flow and the Foundations of Positive Psychology. p. 21–35, 2014.

LEDERER, S. et al. Personal privacy through understanding and action: five pitfalls for designers. **Personal and Ubiquitous Computing**, v. 8, n. 6, p. 440–454, nov. 2004.

LEDERER, S.; MANKOFF, J.; DEY, A. K. **Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing**. CHI '03 Extended Abstracts on Human Factors in Computing Systems (CHI EA '03). **Anais**...New York, NY, USA: ACM, 2003a

LEDERER, S.; MANKOFF, J.; DEY, A. K. **Towards a Deconstruction of the Privacy Space**. Proceedings of the Workshop on Ubicomp Communities: Privacy as Boundary Negotiation. **Anais**...2003b

LEON, P. G. et al. **What matters to users?: factors that affect users' willingness to share information with online advertisers**. Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13). **Anais**...New York, NY, USA: ACM, 2013

LOPEZ-TOVAR, H.; CHARALAMBOUS, A.; DOWELL, J. **Managing Smartphone Interruptions through Adaptive Modes and Modulation of Notifications**. Proceedings of the 20th International Conference on Intelligent User Interfaces (IUI '15). **Anais**...New York, NY, USA: ACM, 2015

LUGER, E.; RODDEN, T. **An informed view on consent for UbiComp**. Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing (UbiComp '13). **Anais**...New York, NY, USA: ACM, 2013

LUGER, E.; RODDEN, T. **Sustaining consent through agency: a framework for future development**. Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct). **Anais**...New York, NY, USA: ACM, 2014

MALHOTRA, N. K.; KIM, S. S.; AGARWAL, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. **Information Systems Research**, v. 15, n. 4, p. 336–355, 2004.

MCCRAE, R. R.; JOHN, O. P. An introduction to the five-factor model and its applications. **Journal of Personality**, v. 60, n. 2, p. 175–215, 1992.

MCCRICKARD, D. S.; CHEWAR, C. M. Attuning notification design to user goals and attention costs. **Communications of the ACM**, v. 46, n. 3, p. 67–72, mar. 2003.

MCDONALD, A. M.; CRANOR, L. F. The Cost of Reading Privacy Policies. **I/S - A Journal of Law and Policy for the Information Society**, v. 4, n. 3, p. 1–22, 2008.

MEHROTRA, A. et al. **Designing content-driven intelligent notification mechanisms for mobile applications**. Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15). **Anais**...New York, NY, USA: ACM, 2015a

MEHROTRA, A. et al. **Ask, but don't interrupt: the case for interruptibility-aware mobile experience sampling.** Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (UbiComp/ISWC'15 Adjunct). **Anais**...New York, NY, USA: ACM, 2015b

MILBERG, S. J. et al. Values, personal information privacy, and regulatory approaches. **Communications of the ACM**, v. 38, n. 12, p. 65–74, 1995.

MONIRUZZAMAN, M.; FERDOUS, M. S.; HOSSAIN, R. **A Study of Privacy Policy Enforcement in Access Control Models**. Proceedings of the 2010 13th International Conference on Computer and Information Technology (ICCIT '10). **Anais**...Washington, DC, USA: IEEE, 2010

MORTON, A.; SASSE, M. A. **Privacy is a process, not a PET**. Proceedings of the 2012 workshop on New security paradigms (NSPW '12). **Anais**...New York, NY, USA: ACM, 2012

MYERS, K. L.; MORLEY, D. N. **Human directability of agents**. Proceedings of the 1st international conference on Knowledge capture (K-CAP '01). **Anais**...New York, NY, USA: ACM, 2001

NORMAN, D. **The design of everyday things**. [s.l.] Basic Books, 2013.

O'HARA, K. The Fridge's Brain Sure Ain't the Icebox. **IEEE Internet Computing**, v. 18, n. 6, p. 81–84, 2014.

ORTMANN, S.; LANGENDÖRFER, P.; MAASER, M. **A self-configuring privacy management architecture for pervasive systems**. Proceedings of the 5th ACM international workshop on Mobility management and wireless access (MobiWac '07). **Anais**...New York, NY, USA: ACM, 2007

OULASVIRTA, A.; SALOVAARA, A. **A cognitive meta-analysis of design approaches to interruptions in intelligent environments**. CHI '04 Extended Abstracts on Human Factors in Computing Systems (CHI EA '04). **Anais**...New York, NY, USA: ACM, 2004

PALLAPA, G.; KUMAR, M.; DAS, S. K. **Privacy infusion in ubiquitous computing**. Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous '07). **Anais**...Washington, DC, USA: IEEE, 2007

PAPAZOGLOU, M. et al. Service-Oriented Computing: a Research Roadmap. **International Journal of Cooperative Information Systems**, v. 17, n. 2, p. 223, 2008.

PARASURAMAN, R.; SHERIDAN, T. B.; WICKENS, C. D. A model for types and levels of human interaction with automation. **IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans**, v. 30, n. 3, p. 286–297, maio 2000.

PATIL, S. et al. **Interrupt Now or Inform Later ?: Comparing Immediate and Delayed Privacy Feedback**. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). **Anais**...New York, NY, USA: ACM, 2015

PEJOVIC, V.; MUSOLESI, M. **InterruptMe: designing intelligent prompting mechanisms for pervasive applications.** Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14). **Anais**...New York, NY, USA: ACM, 2014

PEJOVIC, V.; MUSOLESI, M.; MEHROTRA, A. **Investigating The Role of Task Engagement in Mobile Interruptibility**. Proceedings of the 17th International

Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI ’15). **Anais**...New York, NY, USA: ACM, 2015

PELTZ, C. Web Services Orchestration and Composition. **Computer**, v. 36, n. 10, p. 46–52, 2003.

PERZANOWSKI, D. et al. **Goal tracking in a natural language interface: towards achieving adjustable autonomy**. Proceedings of the 1999 IEEE International Symposium on Computational Intelligence in Robotics and Automation (CIRA’99). **Anais**...Monterey, CA: IEEE, 1999

PIELOT, M.; RELLO, L. **The Do Not Disturb Challenge - A Day Without Notifications**. Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA ’15). **Anais**...New York, NY, USA: ACM, 2015

RÖCKER, C. Information Privacy in Smart Environments: A Cross-Cultural Study Analyzing the Willingness of Users to Share Context Information. In: TANIAR, D. et al. (Eds.). . **Computational Science and Its Applications – ICCSA 2010**. Lecture Notes in Computer Science. [s.l.] Springer Berlin Heidelberg, 2010. p. 93–106.

SADEH, N. et al. Understanding and Capturing People’s Privacy Policies in a Mobile Social Networking Application. **Personal and Ubiquitous Computing**, v. 13, n. 6, p. 401–412, 2009.

SARKER, H. et al. **Assessing the Availability of Users to Engage in Just-In-Time Intervention in the Natural Environment**. Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp ’14). **Anais**...New York, NY, USA: ACM, 2014

SCERRI, P. et al. **A prototype infrastructure for distributed robot-agent-person teams**. Proceedings of the second international joint conference on Autonomous agents and multiagent systems. **Anais**...New York, NY, USA: ACM, 2003

SCERRI, P.; PYNADATH, D.; TAMBE, M. **Adjustable Autonomy in Real-World Multi-Agent Environments**. Proceedings of the fifth international conference on Autonomous agents (AGENTS ’01). **Anais**...New York, NY, USA: ACM, 2001

SCHAUB, F. et al. **Privacy context model for dynamic privacy adaptation in ubiquitous computing**. Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp ’12). **Anais**...New York, NY, USA: ACM, 2012a

SCHAUB, F. et al. **Towards Context Adaptive Privacy Decisions in Ubiquitous Computing**. Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). **Anais**...Washington, DC, USA: IEEE, 2012b

SCHAUB, F. et al. **A Design Space for Effective Privacy Notices**. Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15). **Anais**...Ottawa: USENIX Association, 2015

SCHAUB, F.; KÖNINGS, B.; WEBER, M. Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making. **IEEE Pervasive Computing**, v. 14, n. 1, p. 34–43, 2015.

SCHIAFFINO, S.; AMANDI, A. User – interface agent interaction: personalization issues. **International Journal of Human-Computer Studies**, v. 60, n. 1, p. 129–148, jan. 2004.

SCHMIDER, E. et al. Is It Really Robust?: Reinvestigating the robustness of ANOVA against violations of the normal distribution assumption. **Methodology**, v. 6, n. 4, p. 147–151, 2010.

SCHNORF, S.; ORTLIEB, M.; SHARMA, N. **Trust, transparency & control in inferred user interest models**. CHI "14 Extended Abstracts on Human Factors in Computing Systems (CHI EA"14). **Anais**...New York, NY, USA: ACM, 2014

SELLNER, B. et al. Coordinated multiagent teams and sliding autonomy for large-scale assembly. **Proceedings of the IEEE - Special Issue on Multi-Robot Systems**, v. 94, n. 7, p. 1425–1443, 2006.

SHEIN, E. Ephemeral Data. **Communications of the ACM**, v. 56, n. 9, p. 20–22, set. 2013.

SMITH, J. et al. **Learning to recognise disruptive smartphone notifications**. Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services (MobileHCI '14). **Anais**...New York, NY, USA: ACM, 2014

SOLOVE, D. **Understanding Privacy**. [s.l.] Harvard University Press, 2008.

SVENDSEN, G. B. et al. Personality and technology acceptance: the influence of personality factors on the core constructs of the Technology Acceptance Model. **Behaviour & Information Technology**, v. 32, n. 4, p. 323–334, 2013.

TOCH, E. **Super-Ego: A Framework for Privacy-Sensitive Bounded Context-Awareness**. Proceedings of the 5th ACM International Workshop on Context-Awareness for Self-Managing Systems (CASEMANS '11). **Anais**...New York, NY, USA: ACM, 2011

TURNER, L. D.; ALLEN, S. M.; WHITAKER, R. M. **Interruptibility prediction for ubiquitous systems: conventions and new directions from a growing field**. Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15). **Anais**...New York, NY, USA: ACM, 2015

UKIL, A. et al. **Negotiation-based privacy preservation scheme in Internet of Things platform**. Proceedings of the First International Conference on Security of Internet of Things (SecurIT'12). **Anais**...New York, NY, USA: ACM, 2012

UR, B.; WANG, Y. **A Cross-Cultural Framework for Protecting User Privacy in Online Social Media**. WWW Workshop on Privacy and Security in Online Social Media (PSOSM13). **Anais**...2013

VERMESAN, O. et al. Internet of Things Strategic Research and Innovation Agenda. In: VERMESAN, O.; FRIESS, P. (Eds.). . **Internet of Things: Converging Technologies for Smart Enviroments and Integrated Ecosystems**. [s.l.] River Publishers, 2013. p. 7–152.

WAREN, S.; BRANDEIS, L. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

WEISER, M. The Computer for the 21st Century. **Mobile Computing and Communications Review**, v. 3, n. 3, p. 3–11, 1991.

WEISER, M.; BROWN, J. S. The Coming Age of Calm Technology. In: DENNING, P. J.; METCALFE, R. M. (Eds.). . **Beyond calculation**. New York, NY, USA: Copernicus, 1997. p. 75–85.

WESTIN, A. **Privacy and Freedom**. [s.l.] The Bodley Head Ltd, 1967.

WILSON, S. et al. **Privacy manipulation and acclimation in a location sharing application**. Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing (UbiComp '13). **Anais**...New York, NY, USA: ACM, 2013

YEE, G. **A privacy-preserving UBICOMP architecture**. Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST

Technologies and Business Services. **Anais**...New York, NY, USA: ACM, 2006

ZHANG, N.; TODD, C. **A privacy-respecting context-aware architecture**. Proceedings of the 2006 IET International Conference on Wireless, Mobile and Multimedia Networks. **Anais**...IET, 2006

ZÜGER, M.; FRITZ, T. **Interruptibility of Software Developers and its Prediction Using Psycho-Physiological Sensors**. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI ’15). **Anais**...New York, NY, USA: ACM, 2015

Appendixes

Appendix A

Variables that Influence Sharing Sensitivity

As previously mentioned, in this work a higher privacy concern when sharing data within a certain context indicates a higher sharing sensitivity in that context. However, there is a variety of aspects that can be considered when determining a person's privacy concern in a particular sharing situation: it is necessary to be aware of the physical, social, personal and cultural context (BARKHUUS, 2012; SCHAUB; KÖNINGS; WEBER, 2015).

In order to identify what are finer grained aspects of context used when considering privacy concern and sharing decisions, a literature review related to these topics was conducted. This literature review also helped determine the most significant variables to be considered that can sufficiently inform the user of the current privacy scope. The finer grained aspects were classified considering an extended 5W1H framework for contextual information (similar to the one presented in (KIM; SON; BAIK, 2012)) where a broad **context** variable was considered to represent both broad references to context as "the circumstance under which a device is being used." (ACKERMAN et al. 1999) and the personal, social and cultural aspects of it. The broader variables are:

- **who**: indicates that the person must have some knowledge of the recipient of the data being collected;
- **what**: indicates the type of data or information being collected;
- **where**: indicates the location, generally represented through GPS coordinates, where the person was when the data was being collected;
- **when**: indicates the day and time when the data was being collected;
- w**hy**: indicates why the application requesting data needs the data and the validity of the request); and,
- **'how':** relates the different aspects of the collection and use of data.

In Table 35 these variables and finer grained aspects are presented with the relevant references. Because **context** was added as a broad variable to represent the references that presented social, cultural or personal aspects, or that simply indicated context without further discussion, no finer grained aspects were listed to avoid misrepresentation.

Table 35. Classification of the different references for aspects that influence privacy sensitivity considering the 5W1H framework and subcategories.

WHO (ACKERMAN, 2004; BELLOTTI; SELLEN, 1993; CONSOLVO et al., 2005; HÄKKILÄ; KÄNSÄLÄ, 2004; HENNE; HARBACH; SMITH, 2013; HONG et al., 2004; HONG; LANDAY, 2004; LEDERER et al., 2004; LEDERER; MANKOFF; DEY, 2003a)		
Familiarity	Is the sender aware of the existence of the requester and how do they relate?	(ALMUHIMEDI et al., 2015; ACKERMAN, 1999 apud BARKHUUS; DEY, 2003; BILOGREVIC et al., 2013; LEDERER; MANKOFF; DEY, 2003b; SADEH et al., 2009)
Third-Party	Is the data to be used by or shared to a third-party?	(BELLOTTI; SELLEN, 1993; LEDERER et al., 2004; LEON et al., 2013)
Perception	What is the sender's perception of the requester? Is it of trust?	(CONSOLVO et al., 2005; HONG et al., 2004; MORTON; SASSE, 2012)
WHAT (ACKERMAN, 1999 apud BARKHUUS; DEY, 2003; BILOGREVIC et al., 2013; BUNNIG; CAP, 2009; COUGHLAN et al., 2013; HONG; LANDAY, 2004; HONG et al., 2004; LEDERER et al., 2004; LEON et al., 2013)		
Data Granularity	How detailed is the data being communicated?	(CONSOLVO et al., 2005; GAUD; DEEN; SILAKARI, 2012; HONG et al., 2004; HONG; LANDAY, 2004)
Data Identifiability	Is the information related directly to the sender or to a sender activity?	(LEDERER; MANKOFF; DEY, 2003b)
WHERE (BILOGREVIC et al., 2013; GAUD; DEEN; SILAKARI, 2012; HÄKKILÄ; KÄNSÄLÄ, 2004; SADEH et al., 2009)		
Semantical Location	Where and why is the sender at the current location?	(AGIR; CALBIMONTE; ABERER, 2014; BILOGREVIC et al., 2013; CONSOLVO et al., 2005; JIN et al., 2013; LEDERER et al., 2004; LEDERER; MANKOFF; DEY, 2003a)
Location Properties	What are the different characteristics of the sender's location?	(BILOGREVIC et al., 2013)

WHEN (BELLOTTI; SELLEN, 1993; BILOGREVIC et al., 2013; GAUD; DEEN; SILAKARI, 2012; HÄKKILÄ; KÄNSÄLÄ, 2004; SADEH et al., 2009)		
Time Interval	How long since the last request or consent?	(BILOGREVIC et al., 2013; MORTON; SASSE, 2012)
Frequency	How frequently has the same request been made?	(GAUD; DEEN; SILAKARI, 2012; HONG et al., 2004; HONG; LANDAY, 2004)
Situation	Is the sender in a normal or a special one situation?	(HONG; LANDAY, 2004)
WHY (ACKERMAN, 2004; ALMUHIMEDI et al., 2015; BELLOTTI; SELLEN, 1993; CONSOLVO et al., 2005; COUGHLAN et al., 2013; MORTON; SASSE, 2012)		
Usefulness	Is the requester offering a functionality the sender desires?	(ALMUHIMEDI et al., 2015; ACKERMAN, 1999 apud BARKHUUS; DEY, 2003; BARKHUUS, 2012; BILOGREVIC et al., 2013; BOYLE; GREENBERG, 2005; HENNE; HARBACH; SMITH, 2013; HONG; LANDAY, 2004; HONG et al., 2004)
Sharing risks	What are the risks and implications of sharing this information?	(ACKERMAN, 2004; BUNNIG; CAP, 2009; HONG et al., 2004; LEDERER et al., 2004)
	HOW	
Lifespan	For how long will the data be kept?	(HENNE; HARBACH; SMITH, 2013; HONG et al., 2004; HONG; LANDAY, 2004; LEDERER et al., 2004; LEON et al., 2013)
Uses	How can the requester use and manipulate the information sent?	(BELLOTTI; SELLEN, 1993; GAUD; DEEN; SILAKARI, 2012; LEDERER et al., 2004)
Type of Disclosure	How was the collection made?[58]	(HENNE; HARBACH; SMITH, 2013; HONG et al., 2004; LEDERER et al., 2004; LEDERER; MANKOFF; DEY, 2003b)
Collection method	How is the information sent?[59]	(HENNE; HARBACH; SMITH, 2013; LEDERER et al., 2004)

[58] Some examples: surveillance, transaction, inferred from other collection, third-party data.

[59] Media through which it is conveyed and tangibility of the medium (photo with location vs GPS position)

CONTEXT (GAUD; DEEN; SILAKARI, 2012; HENNE; HARBACH; SMITH, 2013; LEDERER et al., 2004; LUGER; RODDEN, 2013; MORTON; SASSE, 2012; WESTIN, 1967)

Appendix B

Online Survey

The online survey was divided into 5 sections: introduction to the research and survey, demographics, personal characteristics, “a day in the Internet of Things” scenario, and preference collection. Because this was an online survey, this appendix will only show the questions and options, and the actual survey can be accessed at https://goo.gl/Ls9NS9.

PÁGINA INTRODUTÓRIA

Olá!
Meu nome é Jessica Colnago e sou pós-graduanda em ciência da computação pela Universidade Federal de São Carlos e esse questionário será utilizado como parte da coleta de dados para uma pesquisa do meu mestrado.

As perguntas apresentadas são para conhecer suas preferências sobre:

- decidir em cada circunstância sobre o compartilhamento de dados relacionados a você

- delegar essa escolha para um agente inteligente.

O questionário engloba dados demográficos e a sua opinião, considerando certos aspectos identificados na literatura como capazes de influenciar o seu comportamento em relação ao contexto desse questionário.

É importante salientar que não existem respostas certas ou erradas; assim, é importante que você responda de acordo com as suas preferências. Será mantida privacidade absoluta das respostas.

Para as suas respostas serem salvas é necessário que você vá até o final do questionário e selecione o botão para submeter os dados.

Toda e qualquer informação necessária entre em contato com masterproject@jessicacolnago.com.

Obrigada.

Diante das considerações sobre o texto acima, você permite que suas respostas sejam usadas dentro do que foi explicado?

[ ] Sim [ ] Não[60]

[60] In case the participant did not accept they were directly redirected to the “Thank you” page.

DADOS DEMOGRÁFICOS

Para começar eu preciso coletar alguns dados sobre você:

Nacionalidade:

( ) Brasil Outros: _____

Sexo:

( ) Feminino ( ) Masculino

Em qual das faixas etárias abaixo você se encontra?

( ) abaixo de 18 anos
( ) Entre 18 e 25 anos
( ) Entre 26 e 35 anos
( ) Entre 36 e 50 anos
( ) Acima de 50 anos

Qual das frases abaixo melhor descreve seu conhecimento de computadores e outros dispositivos?

( ) Preciso de ajuda para usar computadores, celulares, etc.
( ) Consigo usar computadores para funções simples, como acessar a internet, escrever documentos, ouvir música, etc.
( ) Consigo usar computadores para funções mais complexas, como uso de programas especializados para edição de vídeos, fotos, análise estatísticas, etc.
( ) Sou capaz de programar novas funções para um computador.

Quais os principais usos que você faz de computadores e outros dispositivos?

[ ] Estudo
[ ] Redes sociais
[ ] Notícias
[ ] E-mails
[ ] Compras
[ ] Operações bancárias
[ ] Entretenimento
[ ] Trabalho
[ ] Outros: _____

Quanto tempo por dia você passa utilizando computadores e outros dispositivos?

( ) Menos que ou 2 horas por dia
( ) Entre 2 e 6 horas por dia
( ) Entre 6 e 8 horas por dia
( ) Mais do que 8 horas por dia

CARACTERÍSTICAS PESSOAIS

Por favor, indique o quanto você concorda que as frases abaixo se aplicam a você.

Possuo arquivos/documentos importantes no meu computador/tablet/celular sem cópias em outros lugares.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Conto com meu celular/tablet/computador para lembrar de eventos importantes.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Quanto mais tecnológico algo é, fico mais preocupado que algo vai dar errado.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Não confio em tecnologias em geral.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Não gosto de ser interrompido enquanto estou concentrado.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Desligo as notificações do celular/tablet/computador sempre que posso.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Por favor indique se você já fez alguma das opções abaixo:

[ ] Se recusou a dar informação online porque você achou que era muito pessoal ou desnecessária.
[ ] Decidiu não usar um site/aplicativo/programa porque você não tinha certeza como as suas informações seriam utilizadas.
[ ] Leu a política de privacidade de um site/aplicativo/programa.
[ ] Deletou os cookies do seu navegador.
[ ] Ligou a opção de “não seguir” do seu navegador.

Por favor, indique o quanto você concorda que as frases abaixo se aplicam a você.

Consumidores perderam todo o controle sobre como suas informações pessoais são coletadas e usadas pelas empresas.

( )	( )	( )	( )
Discordo fortemente	Discordo	Concordo	Concordo fortemente

A maioria dos negócios lidam com informações pessoais coletadas dos seus clientes de forma correta e confidencial.

( )	( )	( )	( )
Discordo fortemente	Discordo	Concordo	Concordo fortemente

Existem leis e práticas organizacionais que fornecem um nível razoável de proteção para a privacidade dos consumidores.

( )	( )	( )	( )
Discordo fortemente	Discordo	Concordo	Concordo fortemente

Por favor, indique com que frequência as frases abaixo se aplicam a você.

Essas questões são para identificar uma visão geral do seu desejo por controle.

Eu prefiro um emprego que eu tenha muito controle sobre o que eu faço e quando eu faço.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu gosto de participar politicamente porque eu quero ter o máximo de participação que eu posso em como as políticas públicas devem ser feitas.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu tento evitar situações que alguém me diz o que eu tenho que fazer.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Outras pessoas normalmente sabem o que é melhor para mim.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu gosto de tomar as minhas próprias decisões.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu gosto de ter controle sobre o meu próprio destino.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu geralmente me considero mais capaz em lidar com situações do que outros.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu queria poder deixar outra pessoa decidir por mim o máximo das minhas decisões de vida.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Existem muitas situações que eu preferiria só ter uma opção do que ter que tomar uma decisão.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Eu gosto de esperar e ver se outra pessoa vai resolver um problema para eu não ter que me preocupar com isso.

( )	( )	( )	( )	( )
Nunca	Quase nunca	Não tenho certeza ou se aplica na metade do tempo	Quase sempre	Sempre

Por favor, indique o quanto você concorda que as frases abaixo se aplicam a você.

Eu me sinto confortável junto com pessoas.

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo, nem discordo	Concordo	Concordo fortemente

Eu falo com muitas pessoas diferentes em festas.

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo, nem discordo	Concordo	Concordo fortemente

Eu não gosto de chamar atenção para mim.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu gosto de ficar nos bastidores.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu demonstro interesse em outras pessoas.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu gosto de fazer as pessoas se sentirem confortáveis.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu não me interesso nos problemas de outras pessoas.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu insulto pessoas

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu estou sempre preparado.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu sou preciso no meu trabalho.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu deixo meus pertences em qualquer lugar.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu frequentemente esqueço de pôr as coisas de volta no lugar.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu tenho um vocabulário rico.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu sou cheio de ideias.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu não sou interessado em ideias abstratas.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu não tenho uma boa imaginação.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu sou calmo na maior parte do tempo.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu raramente fico deprimido.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu me preocupo com as coisas.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

Eu fico estressado facilmente.

( ) Discordo fortemente	( ) Discordo	( ) Nem concordo, nem discordo	( ) Concordo	( ) Concordo fortemente

DESCRIÇÃO DE CENÁRIO

Pronto.

Nesta etapa final descreverei o contexto dessa pesquisa. Eu pesquiso sobre a "Internet das Coisas", onde os diferentes objetos do seu dia a dia são capazes de coletar dados sobre você, o ambiente ao redor deles e sobre eles mesmos (por exemplo, como são usados), e comunicar esses dados para outros objetos.

O propósito disso tudo é oferecer serviços para você que se adaptam ao seu ambiente e às suas preferências.

Eu vou descrever uma possível manhã nesse mundo da "Internet das Coisas".

Obs.: tudo descrito aqui é possível de ser criado com a tecnologia que temos hoje.

Seu despertador verificou na agenda do seu smartphone que hoje você terá uma apresentação importante pela manhã e, por isso, decidiu acordar você um pouco mais cedo para você não se atrasar. Você demora um pouco para levantar e, ao sair da cama, seu travesseiro envia para a cafeteira dados de como foi a sua noite para preparar o café de acordo. Como você não dormiu muito bem, a cafeteira está preparando um café extraforte.

Antes de descer para a cozinha você vai ao banheiro. Lá, dados sobre a sua saúde são coletados, como seu peso, nível de açúcar, pressão e nível de ansiedade, e apresentados para você no espelho do banheiro. Você percebe que seus dados estão fora do padrão e decide usar seu bracelete inteligente para acompanhar eles durante o dia. Esses dados são automaticamente enviados para o seu médico.

Ao terminar o café da manhã preparado para você considerando os dados coletados no banheiro e seu histórico, você se prepara para sair para o trabalho. Porém, seu celular identifica que se você for de ônibus chegará com pouco tempo para se preparar para a apresentação. Um táxi é chamado para você e está lhe esperando quando você termina de se arrumar.

Ao entrar no táxi, repara que é um dos novos táxis autoguiados, e seu celular disponibiliza o seu endereço do trabalho para o sistema. No caminho, você recebe várias notificações de sistemas requisitando seus dados de preferência e hábitos. Até os outdoors aderiram à "Internet das Coisas" e por isso constantemente requisitam dados para apresentar propagandas personalizadas para você.

Ao chegar no trabalho, o sistema do taxi utiliza as informações na sua carteira eletrônica para debitar o valor da corrida.

Entrando no prédio, o sistema identifica que você chegou e já inicia os aparelhos na sala de apresentações para você. Você verifica no seu relógio que está adiantado e que seu nível de ansiedade está alto. Aproveita então os momentos antes da apresentação para tentar dar uma acalmada nos nervos e tomar um chá de camomila que acabou de ser preparado na sala de apresentações.

PREFERÊNCIA EM RELAÇÃO A INTERRUPÇÕES

Como você pode perceber, essa "Internet das Coisas" pode facilitar bastante a sua vida. Porém, nós vemos dois problemas com esse cenário.

1) Toda essa troca de informações faz com que dados e informações relacionados a você sejam divulgados e trocados sem que você tenha muito controle a respeito disso.

2) Com todas essas “coisas” querendo suas informações por diferentes motivos, vão existir muitas interrupções durante o dia para que você possa escolher compartilhá-los ou não.

Para ajudar com esses dois problemas, muita pesquisa e estudos vêm sendo realizados. Em particular, uma abordagem muito comum é oferecer para vocês um “Agente pessoal”.

Esse agente sabe e aprende as suas preferências de compartilhamento de dados. Dessa forma, ao invés de interromper você ou de divulgar suas informações para qualquer um, esse agente toma essas decisões de acordo com as suas preferências.

O que nós queremos saber é o seguinte: Considerando que existe esse agente para ajudar a você nas decisões de compartilhar ou não os seus dados, o que você acha que vai influenciar a sua vontade de deixar ele tomar essas decisões automaticamente ou de lhe interromper para obter sua opinião?

Você acha que o seu humor no momento de receber a interrupção afetaria a sua preferência de tomar a decisão de privacidade ou delegá-la ao agente?

( )	( )	( )
Influenciaria	Não influenciaria	Não sei ou não tenho opinião

Você acha que a opinião das pessoas ao seu redor sobre você ter sido interrompido afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( )	( )	( )
Influenciaria	Não influenciaria	Não sei ou não tenho opinião

Você acha que o seu nível de concentração em uma tarefa afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( )	( )	( )
Influenciaria	Não influenciaria	Não sei ou não tenho opinião

Você acha que o seu nível de interação com outras pessoas no momento de receber a interrupção afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( )	( )	( )
Influenciaria	Não influenciaria	Não sei ou não tenho opinião

Você acha que a frequência das interrupções afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que a sua vontade de estar em controle afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que a sua personalidade afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que o seu nível de preocupação com privacidade afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que a sua confiança nesse agente afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que o nível de certeza que o agente tem na decisão que você tomaria afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que o tipo de compartilhamento (tipo de dado, quem está requisitando e o motivo) afetaria a sua preferência de ser interrompido para tomar a decisão de privacidade ou delegá-la ao agente?

( ) Influenciaria ( ) Não influenciaria ( ) Não sei ou não tenho opinião

Você acha que existem situações diferentes das listadas acima que poderiam influenciar a sua preferência de tomar a decisão ou de delegá-la ao agente?

Appendix C

Informed Consent Form

The following text reproduces the informed consent form signed by all participants of the user study presented in Chapter 6.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado para participar da pesquisa “Estabelecimento de um modelo de equilíbrio entre controle e autonomia no contexto de Internet das Coisas”.

1. Esta pesquisa tem como intuito identificar as variáveis que influenciam na escolha de permitir ou não que um sistema computacional inteligente tome decisões pelo usuário no que diz respeito ao compartilhamento de dados no contexto de Internet das Coisas; bem como propor um modelo visando melhorar a experiência de uso de tal sistema.
   a. Você foi selecionado para ser usuário do nosso sistema de coleta de preferências sobre interrupções para compartilhamento de dados na Internet das Coisas, mas sua participação não é obrigatória
   b. Os objetivos desse estudo são os de identificar quais variáveis afetam a concordância com uma interrupção para exercer controle em um momento de compartilhamento de dados na Internet das Coisas e as variações dentro dessas variáveis entre diferentes usuários. Também buscaremos verificar se existem correlações entre as variáveis e se é possível identificar grupos de usuários para facilitar a definição de preferências.
   c. Sua participação nesta pesquisa consistirá em utilizar um sistema de coleta de preferência de interrupções e responder como você se comportaria dada um cenário especificado e o seu contexto naquele momento. Você responderá de forma única um questionário inicial, realizará a classificação de diferentes cenários de acordo com a sua opinião sobre o nível de sensitividade do compartilhamento e um questionário final. Você responderá de forma contínua (para cada interrupção) algumas perguntas para caracterizarmos o seu contexto.
2. A sua participação neste estudo envolve riscos como desconforto pelo uso de ferramentas em desenvolvimento e desconforto pelo compartilhamento de suas preferências.
   a. Você possui total controle sobre o experimento, podendo escolher terminá-lo a qualquer momento. Apenas pedimos que nos explique o motivo para podermos melhorar o sistema e estudo.
   b. Os dados que serão publicados desse estudo não lhe identificarão e qualquer referência será feita através de siglas e números.

c. A tecnologia será testada profusamente antes do seu uso e você terá acesso a membros da equipe para solucionar qualquer desconforto que possa ocorrer.

d. Para respeitar a privacidade de seus dados, suas preferências não serão armazenadas ou utilizadas por períodos ou propósitos além desse estudo.

3. A pesquisa ocorrerá em um horário previamente definido e terá duração de 21 dias corridos, no qual será necessária a participação contínua apenas por 10. Durante esse período contínuo você receberá notificações no intervalo das 8h até as 20h. Você terá assistência por parte membros da equipe de pesquisa e o recurso a ser utilizado é um aplicativo no seu próprio dispositivo que gerará as interrupções e coletará as suas respostas de acordo com o estabelecido em 2.c.

4. Antes, durante e após o estudo de caso você poderá solicitar esclarecimentos a respeito dos procedimentos ou qualquer outra questão relacionada com a pesquisa.

5. Você tem total liberdade de se recusar a participar ou retirar seu consentimento, em qualquer fase da pesquisa, sem penalização alguma e sem prejuízo ao seu cuidado.

a. A qualquer momento você pode desistir de participar e retirar seu consentimento.

b. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição.

6. Seus dados pessoais envolvidos na pesquisa serão confidenciais.

a. As informações obtidas nesta pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação.

b. Toda e qualquer informação coletada durante o estudo é tratada como confidencial. Os dados não serão divulgados de forma a possibilitar sua identificação. Ressalta-se que os resultados obtidos serão mostrados aos participantes após o término da pesquisa.

7. Você não terá nenhum benefício financeiro por participar desse estudo, mas os resultados obtidos através dessa pesquisa serão utilizados para investigar melhorias em sistemas computacionais para decisões automatizadas de compartilhamento de dados.

8. Você receberá uma cópia deste termo onde consta o contato do pesquisador, podendo tirar suas dúvidas sobre o projeto e sua participação, agora ou a qualquer momento.

_____

Jessica Helena Colnago

Departamento de Computação (DC) / Universidade Federal de São Carlos (UFSCar) Caixa Postal 676 / 13565-905 São Carlos-SP / Tel.: 16-33518513

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar. O pesquisador me informou que o projeto foi aprovado pelo Comitê de Ética em Pesquisa em Seres Humanos da UFSCar que funciona na PróReitoria de Pós-Graduação e Pesquisa da Universidade Federal de São Carlos, localizada na Rodovia Washington Luiz, Km. 235 - Caixa Postal 676 - CEP 13.565-905 - São Carlos - SP – Brasil. Fone (16) 3351-8110. Endereço eletrônico: cephumanos@power.ufscar.br

São Carlos, __/__/2016

_____

Participante

Appendix D

User Study Application Screenshots

For the user study an Android application was developed in order to trigger the interruptions and collect data. The different interfaces with which the participants interacted with are listed in this appendix. However, given space limitations their descriptions will not be captions, but listed below:

1. Initial Questionnaire: Demographics section
2. Initial Questionnaire: Trust and Interruption Handling section
3. Initial Questionnaire: Privacy Behavior and Privacy Concern section
4. Initial Questionnaire: Need for Control section
5. Scenario Classification with the scenario. sharing sensitivity and behavior preference options.
6. Main screen after the initial steps (questionnaire and scenario classification are completed and uploaded). The progress bar increased with every task completed – questionnaire, scenario classification or interruption triggered. The count reflected missed or canceled interruptions. The area below the missed interruptions counter was reserved for the participants to input further information whenever they selected “Other” when delegating directly.
7. Questionnaire tab after questionnaire (initial or final) was completed
8. Scenario tab after the scenarios were all classified (initial or final)

The interfaces for when an interruption was triggered were shown in Figure 19.

Por favor, responda as questões abaixo:

Sexo

- ◯ Feminino
- ◯ Masculino

Faixa etária

- ◯ 18–25
- ◯ 26–35
- ◯ 36–50
- ◯ 50+

Qual das frases abaixo melhor descreve seu conhecimento de computadores?

- ◯ Preciso de ajuda para usar computadores, celulares, etc.
- ◯ Consigo usar computadores para funções simples, como acessar a internet, escrever documentos, ouvir música, ...
- ◯ Consigo usar computadores para funções mais complexas, como uso de programas especializados para edição de vídeos, fotos, análise estatísticas, ...
- ◯ Sou capaz de programar novas funções para um computador.

Quais os principais usos que você faz de computadores, celulares, tablets, ...?

- ☐ Entretenimento
- ☐ Trabalho
- ☐ Operações bancárias
- ☐ Redes Sociais
- ☐ Compras
- ☐ E-mails
- ☐ Notícias
- ☐ Estudo
- ☐ Outros

Quanto tempo por dia você passa utilizando computadores e outros dispositivos?

- ◯ Menos que 2 horas
- ◯ Entre 2 e 6 horas
- ◯ Entre 6 e 8 horas
- ◯ Mais do que 8 horas

AVANÇAR

Por favor, indique o seu nível de concordância com as frases abaixo:

Conto com meu celular / tablet / computador para lembrar de eventos importantes.

Discordo completamente — Concordo completamente

Possuo documentos importantes no meu computador / tablet / celular sem cópias em outros lugares.

Discordo completamente — Concordo completamente

Não confio em tecnologias em geral.

Discordo completamente — Concordo completamente

Quanto mais tecnológico algo é, fico mais preocupado que algo vai dar errado.

Discordo completamente — Concordo completamente

Desligo as notificações do celular / tablet / computador sempre que posso.

Discordo completamente — Concordo completamente

Não gosto de ser interrompido enquanto estou concentrado.

Discordo completamente — Concordo completamente

AVANÇAR

Por favor, indique se você já fez alguma das opções abaixo:

- [ ] Se recusou a dar informação online porque você achou que era muito pessoal ou desnecessária.
- [ ] Decidiu não usar um site / aplicativo / programa porque você não tinha certeza como as suas informações seriam utilizadas.
- [ ] Leu a política de privacidade de um site / aplicativo / programa.
- [ ] Deletou os cookies do seu navegador.
- [ ] Ligou a opção de do not trackdo seu navegador.

Por favor, indique o seu nível de concordância com as frases abaixo:

Consumidores perderam todo o controle sobre como suas informações pessoais são coletadas e usadas pelas empresas.

Discordo completamente — Concordo completamente

A maioria dos negócios lidam com informações pessoais coletadas dos seus clientes de forma correta e confidencial.

Discordo completamente — Concordo completamente

Existem leis e práticas organizacionais que fornecem um nível razoável de proteção para a privacidade dos consumidores.

Discordo completamente — Concordo completamente

AVANÇAR

Por favor, indique a frequência com a qual as frases abaixo se aplicam a você:

Eu prefiro um emprego / uma ocupação na qual eu tenha muito controle sobre o que eu faço e quando eu faço.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Eu gosto de participar politicamente porque eu quero ter o máximo de participação que eu posso em como as políticas públicas devem ser feitas

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Eu tento evitar situações nas quais alguém me diz o que eu tenho que fazer.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Outras pessoas normalmente sabem o que é melhor pra mim.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Eu gosto de tomar as minhas próprias decisões.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Eu gosto de ter controle sobre o meu próprio destino.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Eu geralmente me considero mais capaz em lidar com situações do que outros.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

Eu queria poder deixar outra pessoa decidir por mim o máximo das minhas decisões de vida.

Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

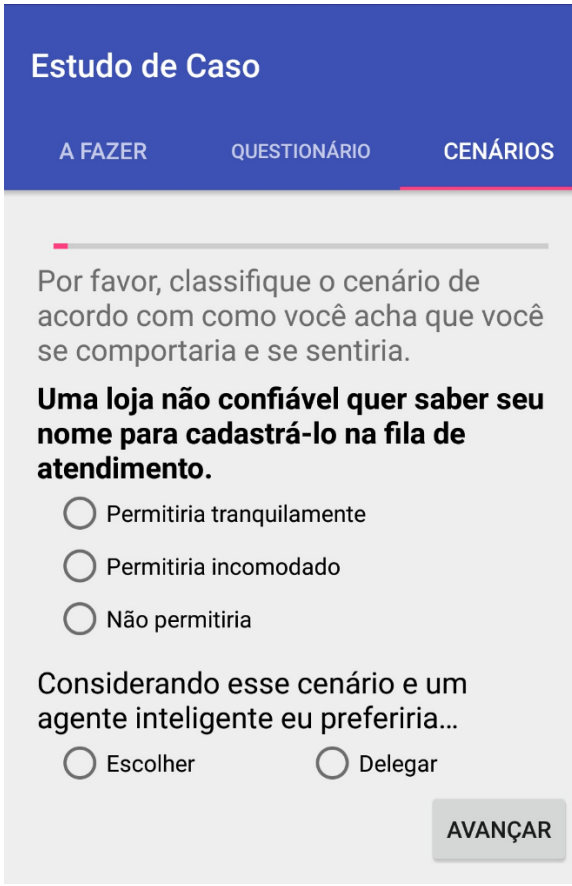
Existem muitas situações nas quais eu preferiria só ter uma opção do que ter que tomar uma decisão.

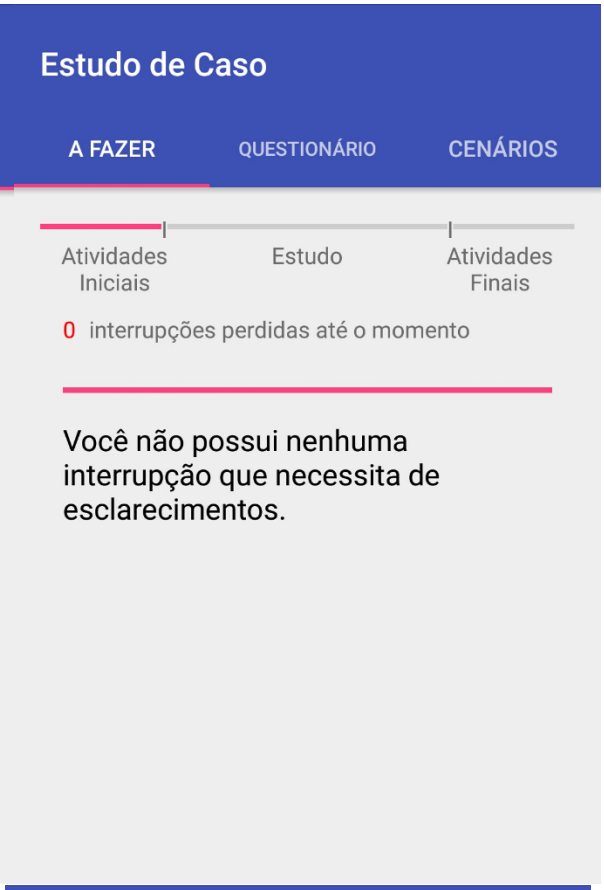
Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

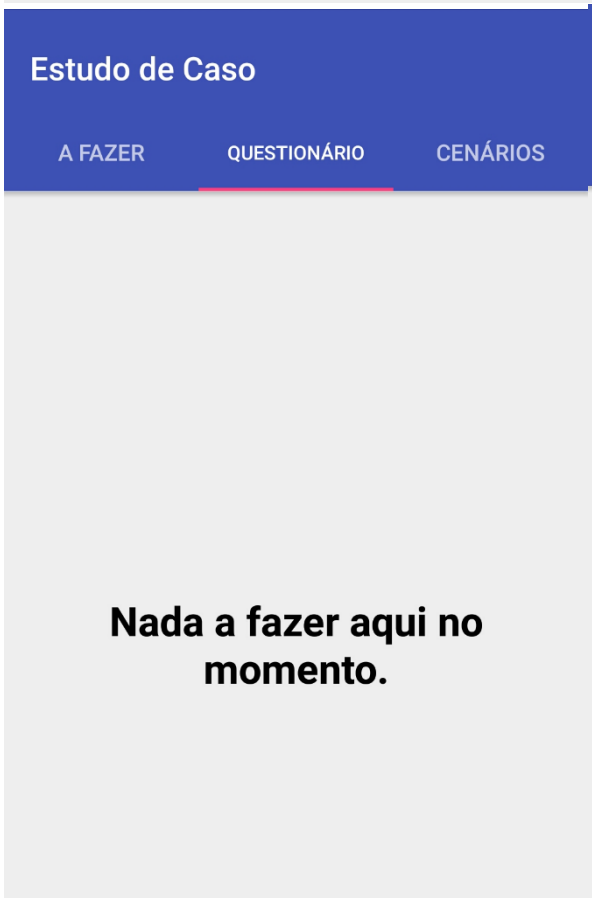
Eu gosto de esperar e ver se outra pessoa vai resolver um problema para eu não ter que me preocupar com isso.

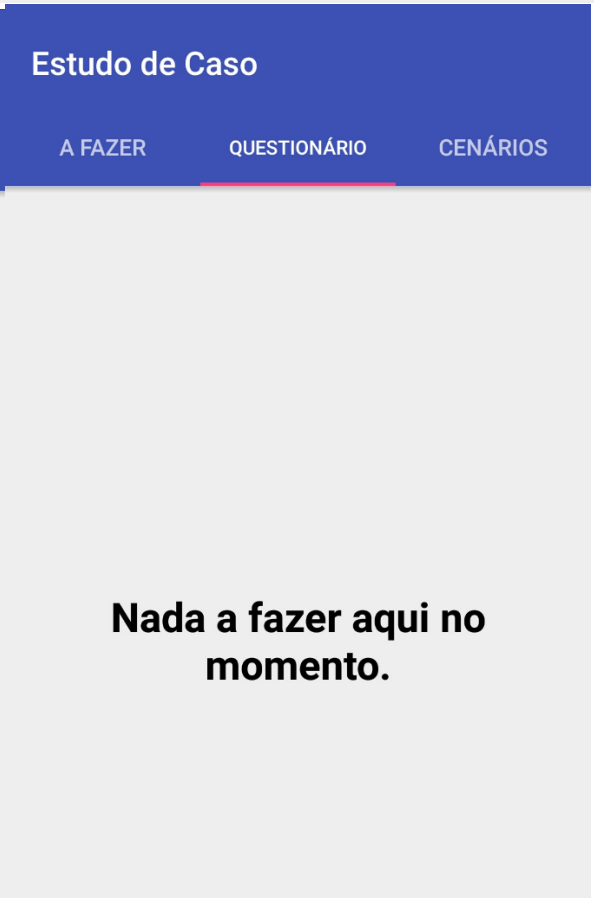
Discordo completamente — Na metade do tempo Não tenho certeza — Concordo completamente

SALVAR


Estudo de Caso
A FAZER
QUESTIONÁRIO
CENÁRIOS
Por favor, classifique o cenário de acordo com como você acha que você se comportaria e se sentiria.
Uma loja não confiável quer saber seu nome para cadastrá-lo na fila de atendimento.
Permitiria tranquilamente
Permitiria incomodado
Não permitiria
Considerando esse cenário e um agente inteligente eu preferiria...
Escolher
Delegar
AVANÇAR


Estudo de Caso
A FAZER
QUESTIONÁRIO
CENÁRIOS
Atividades Iniciais
Estudo
Atividades Finais
0 interrupções perdidas até o momento
Você não possui nenhuma interrupção que necessita de esclarecimentos.


Estudo de Caso
A FAZER
QUESTIONÁRIO
CENÁRIOS
Nada a fazer aqui no momento.


Estudo de Caso
A FAZER
QUESTIONÁRIO
CENÁRIOS
Nada a fazer aqui no momento.

Appendix E

Scenarios

In this appendix we present the scenarios that the participants of the user study classified at the beginning and end of the user study. They were presented on each interruption that the participant decided to see more information before making the decision to choose or delegate. These scenarios were a collaboration effort between the whole research group and were based on existing technology as well as imagined ones.

1. Uma loja não confiável quer saber seu nome para cadastrá-lo na fila de atendimento.
2. Um painel eletrônico deseja informações sobre seu itinerário para dicas de caminhos alternativos.
3. O serviço de táxi quer acesso aos seus dados bancários para poder cobrar a tarifa da corrida.
4. Um restaurante não confiável quer acesso aos seus dados bancários para pagamento da conta.
5. Outdoors de propaganda querem acesso às suas preferências de compras para mostrarem propagandas adequadas.
6. O serviço de táxi quer acesso ao seu horário de chegada no trabalho para enviar um táxi no horário mais adequado.
7. Uma loja não confiável quer acesso à sua data de nascimento para determinar sua prioridade de atendimento.
8. Um painel de propaganda deseja informações sobre sua renda para seleção de propagandas.
9. Uma ONG quer acesso ao seu consumo de água para sugerir planos de conservação e educação hídrica.
10. A bomba de combustível do posto de gasolina quer informações sobre o consumo do seu carro.
11. Um serviço de táxi quer acesso às suas preferências musicais para tocar músicas adequadas.
12. A sua cidade quer acesso aos dados de emissão de gás carbônico do seu carro para realizar um planejamento de meio ambiente.
13. Seu carro quer saber quem está dirigindo para manter informações estatísticas.
14. Uma loja não confiável quer acesso ao seu e-mail para envio de propagandas.
15. O seu local de trabalho quer acesso à sua localização para permitir que seus colegas lhe encontrem facilmente.

16. O seu médico quer acesso aos seus dados de saúde para acompanhar a sua saúde.
17. Seu carro quer usar informações sobre sua localização para registro em um sistema remoto.
18. Um restaurante não confiável quer acesso às suas preferências de comida para sugerir pratos adequados.
19. O termostato da sua casa quer saber o seu cronograma do dia para ajustar a temperatura de acordo e economizar energia.
20. O seu local de trabalho quer acesso à sua agenda para reservar recursos que podem ser necessários no seu dia.
21. O sistema de refrigeração do cômodo em que você está em sua casa quer saber seu tempo estimado de permanência para ajustes da refrigeração.
22. As luzes da sua sala querem saber se você está assistindo um filme para diminuir a intensidade de seu brilho.
23. Uma loja não confiável quer acesso às suas preferências de compras para fazer propaganda adequada à você.
24. O seu telefone quer acesso à sua agenda para ajustar o nível do toque de acordo com as suas tarefas.
25. O compressor de ar do posto de gasolina quer informações sobre o modelo do seu carro para determinar a pressão adequada do calibrador.
26. Um restaurante não confiável quer informações sobre sua sensação de calor no momento para adequar a temperatura do salão.
27. A farmácia quer acesso aos seus dados de sono para fazer propaganda de remédios apropriados para você.
28. O sistema de um estacionamento deseja saber se seu carro possui um mecanismo de pagamento automático para determinar a forma de cobrança.
29. Sua cadeira no escritório quer saber sua identidade para manter histórico sobre seu peso.
30. Uma loja não confiável quer acesso ao seu CPF para cadastro no sistema de sorteio de brindes.
31. O seu sistema de entretenimento quer acesso às suas buscas mais recentes de notícias para selecionar uma programação relevante.
32. Um restaurante não confiável quer acesso aos seus dados de saúde para informar decisões futuras de escolhas de receitas e marketing.
33. O seu sistema de despensa quer acesso aos seus dados de higiene bucal para adicionar mais pasta de dente na sua lista de compras.
34. A livraria quer informações sobre sua preferência de gênero literário para propor recomendações de compras.
35. Seu carro quer informações sobre seu itinerário para determinar se tem autonomia para o percurso.

Appendix F

Brazilian Privacy-related Laws

Before delving into privacy laws and regulations in Brazil it is important to note how the legal system works. As in the United States the main normative document is the country's constitution, promulgated in 1988. Furthermore, Brazil follows a coded normative system where the laws are compiled in the civil and penal code. Most of the penalties for infringing a law are defined by those codes and there's usually a lot less room for judicial decisions than in the U.S.

With that in mind the current state of privacy laws and regulations in Brazil is described and divided between broad statements of privacy rights, found mostly in the Federal Constitution, and more specific laws usually found within the penal and civil code. While some laws come to regulate on a new set of privacy rights such as the Internet Use Law of 2014, the great majority come to further specify rights delineated in the Federal Constitution. Also, while the Penal Code stipulates sentences for non-compliance with the law, there are no formal enforcement agents other than the police force and judicial system to enforce them[61].

- **Broader Privacy Rights:** The 1988 Federal Constitution in its article 5 describes the rights for citizens and residents of Brazil. The following described rights have been considered to relate to different aspects of privacy:

  X – "intimacy, private life, honor and a person's image are inviolable rights and compensation for material or moral damage are secured if violated" (broad privacy right);

  XI – "the home is an inviolable refuge in which no one can enter without consent, unless in flagrante delicto [emphasis added] or in case of a disaster, to offer help or, during the day, by court order" (right to a private refuge);

[61] The majority of the content here described can be found in Portuguese at: Fabio Condeixa. 2015. Direito de privacidade no Brasil. Revista Jus Navi gandi 20, 4335 (2015).

The Penal Code article 150 foresees that a violation of this right by an individual shall lead to detention for a minimum of 1 to a maximum of 3 months, or the application of a fine. In case there are aggravating factors, such as happening at night, with violence or by more than one person, this detention time goes to a minimum of 6 months to a maximum of 2 years plus any corresponding sentence related to the use of violence.

The Authority Abuse Law (Federal Law 4.898/1965) offers the appropriate sanctions in the case this performed by a public agent.

XII – "the secrecy of correspondence and telegraphic communication, data and telephonic communication, unless by court order, as a last resort, for the hypothesis and form that the law establish for criminal investigation" (right to private communications); and,

XXVIII, a – "[it is secured by law] the protection of the individual participation in collective works and the reproduction of human image and voice, including sporting activities" (right to private image). This has been reinforced by the Supreme Court in Brazil through Sumula 403 that states that there is no need to prove damages to be compensated by the non-authorized use of a persons image for commercial or economic reasons.

- **Specific Privacy Rights**
  - ***Financial Data:*** defined in the Financial Secrecy Law (Complementary Federal Law 105/2001) as related to operations performed within financial institutions. Article 10 of the Financial Secrecy Law stipulates that outside of the exemptions, breach of financial secret as well as obstruction in providing the financial data required by court order is a crime punishable by detention from 1 to 4 years and a fine.

    The National Tax Code article 198 states that information about a person's economic or financial status is vetoed unless by court order, administrative authorities in the interest of the public administration, or if related to penal reasons, active debt with the nation or bankruptcy. Furthermore, Internal House Committees were also allowed to breach the privacy of financial records by article 58 3 of the Federal Constitution.

The Financial Crime Law (Federal Law 7.492/1986) allows the public ministry to request to any level of authority information and documents to investigate infractions of any nature.

- ***Personal Data and Secrets:***

The Information Access Law (Federal Law 12.527/2011) identified in its article 31 that personal information is related to aspects of intimacy, private life, honor and image. The law establishes that they should be protected from governmental access for 100 years unless given explicit consent or for medical diagnosis and treatment, for surveys and scientific research of public interest, by court order, to address human rights violation, or protection of the public interest. Furthermore, this law cannot be used to avoid investigation or to limit access to historic data of major relevance. Its article 34 foresees that the State shall be responsible in case of privacy violations.

The Criminal Organization Law (Federal Law 12.850/2013) defines in its article 15 that police and the Public Ministry can have access, even without judicial approval, to suspects' registration data that exclusively inform about his/her personal qualification, affiliation, and address as kept by the Electoral Justice, telephone companies, financial institutions, internet providers and credit card agencies. Article 16 specific regulates the access to travel information, which should be kept for at least 5 years and be made directly available to law enforcement. Article 17 provides similar regulations over phone communication metadata. Lastly, article 21 states that failure to comply may lead to a fine and incarceration from 6 months to 2 years.

The Penal Code articles 153 and 154 regulates the case when there are the breach in confidentiality of personal and professional secrets, respectively. When damages can be proved, the sentences go from 1 to 6 months of detention in case of personal secrets and 3 months to a year in case of professional secrets, both possibly being waived if a fine is payed.

Penal Code article 325 regulates such breaches when performed by a public agent with the sentence going from 6 months to 2 years of detention. If the breach leads to damage to the public administration the sentence goes to 2 to 6 years of incarceration and payment of a fine. Also, in case this is breach happens through a public servant or a person naturally associated with public

service, Decree 7.724/2012 foresees a fine from one thousand to 200 thousand reais.

- ***Internet & Technology:***

  Penal Code article 154-A also known as Carolina Dieckmann Law (Federal Law 12.737/2012) regulates that detention for 3 months to 1 year and a fine are applicable in case of invasion of a technological device when security measures are breached to obtain, alter or destruct data or information without consent, or to install vulnerability to obtain illicit advantages.

  The Internet Use Law (Federal Law 12.965/2004) defines it to be the service provider responsibility to remove content that infringes a person's intimacy after being requested to do so. It does not limit law enforcement access to the information, but differently to other laws it also allows access in civil suits. Article 5, VI and VII define 'connection record' and 'internet application', where the first determines as part of the connection record information about the date and time of the start and finish of a connection, the duration and IP address. The latter being particularly significant given that it was not formerly recognized as protected information. Article 7 offers privacy rights that reflect article 5, X of the Federal Constitution, plus the secrecy of communication flow and of private communication stored, unless requested by court order. Furthermore, Article 10 added barriers to acquisition of connection and communication records, stating that need only be divulged if requested by court order. However, article 13 defines that system administrators must keep connection records under protection in a controlled and secure environment for at least a year, a responsibility that cannot be given to third-parties. This creates a potential privacy vulnerability since before this law, system administrators were not required to keep any information, thus directly avoiding any security breaches. Lastly, article 12 lists punishments that go from notice and requirement for improvement, to fines of up to 10% of the national revenues, to temporary suspension of data related activities, to prohibition of any further data related activities. In the case of foreign companies, the recommendation is to only fine them.

- ***Non-Electronic Communication:*** The Brazilian Telecommunication Code (Federal Law 4.117/1962) defines telecommunication services as 'the

transmission, emission or reception of symbols, characters, signals, text, images, sounds or information of any nature through wires, radio, electricity, optical means or any other electromagnetic means'.

The General Telecommunication Law (Federal Law 9.472/1997) foresees the protection of privacy for the users of telecommunication services. Article 3, V declares as right to have communications be inviolable and secret, except in previously excluded cases.

The Penal Code article 151 determines a fine or detention from 1 to 6 months for those that inappropriately divulge, transmits or abusively uses a telegraphic or radioelectric communication directed to a third party, or phone communication between other people. Paragraph 3 of the same article determines that if an authority commits the same crime, the sentences is detention from 1 to 3 years.

Interception Law (Federal Law 9.296/1996) article 10 defines as crime the interception of phone communications without a court order or for purposes not authorized by the law. However, it is important to note that interception only considers cases where no party is aware of the collection. When there's one consenting party, even if the collection is done by a third party, the collection is deemed legal even without a court order in cases where there is an illegal activity happening or if it is as a mechanism for defense.

There is no law against ambient collection of sound or image. So as in the U.S. the lack of a 'reasonable expectation of privacy' is applicable in public spaces.

Postal Services Law article 40 determines that to open a closed correspondence is a crime punishable by detention for up to 6 months or the payment of a fine, except when addressed to a person with the same name in the same address, if there seems to be an object that should be taxed or an object of undeclared value or illegal use, or if it has to be destroyed given the inability to deliver and return it to the sender. It is important to note that such rights do not necessarily apply to inmates as defined in the Penal Execution Law (Federal Law 7.210/1984).

Lastly, even though there is no law that directly guarantees the "right to be forgotten", this type of protection has been granted by the Supreme Court in a case-by-case basis.