



IONIAN
UNIVERSITY

Department of Informatics

**Transforming Information Privacy Behavior through
Experiential Procedures**

Doctor of Philosophy Thesis of Ioannis Paspatis

Supervisor: Associate Professor Aggeliki Tsohou

Department of Informatics, Ionian University

7 Tsirigoti Square, 49100, Corfu, Greece

This thesis may not be reproduced in whole or in part by
photocopy or other medium, without permission of the author.

Advisory Committee

Supervisor: Tsohou Aggeliki
Associate Professor, Ionian University

Advisory member: Spyros Kokolakis
Professor, University of the Aegean

Advisory Member: Magkos Emmanouil (Manos),
Professor, Ionian University

Examination Committee

Tsohou Aggeliki
Associate Professor, Ionian University

Spyros Kokolakis
Professor, University of the Aegean

Emmanouil (Manos) Magkos
Professor, Ionian University

Christoforos Ntantogian
Assistant Professor, Ionian University

Maria Karyda
Professor, University of Aegean

Adamantia Pateli
Professor, Ionian University

Costas Lambrinoudakis
Professor, University of Piraeus

Περίληψη

Οι νέες τεχνολογίες, όπως φορητές συσκευές που συνδέονται μόνιμα στο διαδίκτυο, επαυξημένη πραγματικότητα, κινητές συσκευές, καθώς και η επικράτηση των μέσων κοινωνικής δικτύωσης, έχουν δημιουργήσει τις προϋποθέσεις ώστε ταυτότητα και η προσωπικότητα των ατόμων να είναι ορατές στον κόσμο. Προσωπικά δεδομένα χρηστών των νέων τεχνολογιών μπορούν να συλλεχθούν από ιδιώτες και επιχειρήσεις μέσω διαφόρων τεχνικών, συχνά χωρίς τα υποκείμενα των δεδομένων να το γνωρίζουν. Ενδεικτικά, προσωπικά δεδομένα συγκεντρώνονται χωρίς την ενεργό διαμεσολάβηση του υποκειμένου όταν χρησιμοποιεί μέσω προηγμένες τεχνολογίες που συνδέονται στο διαδίκτυο, π.χ. έξυπνα ρολόγια ή IoT συσκευές. Αντίστοιχα, πλήθος προσωπικών πληροφοριών διαμοιράζονται μέσω της πρόθυμης δημοσίευσης αυτών σε ιστότοπους κοινωνικής δικτύωσης, όπως η δημοσίευση προσωπικών φωτογραφιών ή άλλων προσωπικών δεδομένων. Διάφοροι ερευνητές έχουν διερευνήσει τη ριψοκίνδυνη συμπεριφορά διαμοιρασμού προσωπικών δεδομένων και την αντίστοιχη έλλειψη ευαισθητοποίησης. Αντικείμενο αυτής της διατριβής αποτελεί η συμπεριφορά ιδιωτικότητας, η οποία περιλαμβάνει ενέργειες όπως αποκάλυψη προσωπικών πληροφοριών, εφαρμογή μέτρων προστασίας της ιδιωτικότητας και προσαρμογή των ρυθμίσεων ιδιωτικότητας. Η αποκάλυψη προσωπικών πληροφοριών μπορεί να είναι ριψοκίνδυνη καθώς μπορεί να έχει αρνητικές συνέπειες, όπως κλοπή ταυτότητας, πλαστοπροσωπία, κ.ά. Διάφοροι ενδιαφερόμενοι μπορεί να χρησιμοποιήσουν τα προσωπικά δεδομένα στις όφελός τους, συμπεριλαμβανομένης της δημιουργίας προσαρμοσμένων διαφημιστικών καμπανιών και επιρροής στις επιλογές ψήφου σε εκλογές, όπως φάνηκε στην περίπτωση της Cambridge Analytica. Η παρατήρηση της συμπεριφοράς της ιδιωτικότητας των ανωτέρω χρηστών καθώς και οι τρόποι μετασχηματισμού της σε μία ασφαλέστερη βρίσκεται ερευνητικά στο προσκήνιο αρκετά έτη. Παρόλα αυτά, δεν φαίνεται να έχει βρεθεί κάποια μέθοδος ή δημιουργηθεί ένα πλαίσιο που αξιόπιστα και αποδοτικά να μετασχηματίζει αυτή τη συμπεριφορά σε μία περισσότερο ασφαλή.

Η παρούσα διατριβή επικεντρώθηκε σε τρεις στόχους για τη μελέτη και αντιμετώπιση του προαναφερθέντος ερευνητικού προβλήματος. Αρχικά προσδιορίσαμε τους παράγοντες που επηρεάζουν τη συμπεριφορά ιδιωτικότητας. Τα ευρήματα της έρευνάς μας αποκάλυψαν ότι υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν την εν λόγω συμπεριφορά, τους οποίους συγκεντρώσαμε και συνθέσαμε υπό ένα ενιαίο πλαίσιο. Στη συνέχεια, μελετήσαμε τους επιστημονικούς κλάδους της ψυχολογίας, της κοινωνιολογίας, της φιλοσοφίας και της υγείας για να ανακαλύψουμε μεθόδους μετασχηματισμού της συμπεριφοράς της ιδιωτικότητας. Η Γνωστική Θεωρία και η επέκτασή της, το Μοντέλο Πεποιθήσεων στην Υγεία, έχουν εφαρμοστεί σε διάφορους κλάδους για να διευκολύνουν το μετασχηματισμό μίας συμπεριφοράς. Συνδυάσαμε τις προαναφερθείσες θεωρίες με τους παράγοντες που καθορίζουν τη συμπεριφορά της ιδιωτικότητας ενός ατόμου. Στο πλαίσιο της μελέτης μας ανακαλύψαμε

ότι οι αναφερόμενες θεωρίες εφαρμόζονται πιο αποτελεσματικά μέσω μεθόδων βιωματικής μάθησης και διδασκαλίας. Η έρευνά μας έδειξε ότι υπάρχει ευρεία επιστημονική συνέπεια ότι η Γνωστική Συμπεριφορική Θεραπεία (CBT) και ο Γνωσιακός Μετασχηματισμός Συμπεριφοράς (CBTx) έχουν δοκιμαστεί διεξοδικά και επιτυχώς στο παρελθόν ως μέθοδοι για την αλλαγή της συμπεριφοράς των ατόμων. Αυτές οι μέθοδοι μπορούν να χρησιμοποιηθούν μέσω ουδέτερων ερεθισμάτων, πρακτικών αξιολογήσεων και μεθόδων Παρακινήτικών Συνεντεύξεων (MI). Λαμβάνοντας υπόψη όλα τα ανωτέρω, αναπτύξαμε ένα νέο πλαίσιο μετασχηματισμού συμπεριφοράς ιδιωτικότητας (Privacy Behavior Transformation Framework - PBTF) το οποίο ενσωματώνει τις τρεις μεθόδους (δηλαδή ουδέτερα ερεθίσματα, πρακτικές αξιολογήσεις και μέθοδοι Παρακινήτικών Συνεντεύξεων). Προκειμένου να επικυρώσουμε την αποτελεσματικότητα του προτεινόμενου πλαισίου διεξαγάγαμε μία εμπειρική μελέτη πέντε φάσεων. Τα αποτελέσματα της έρευνας έδειξαν την επάρκεια και την αποδοτικότητα του προτεινόμενου Πλαισίου. Τα αποτελέσματα έδειξαν ότι στο σύνολο των συμμετεχόντων η συμπεριφορά ιδιωτικότητάς τους μετασχηματίστηκε σε μία περισσότερο ασφαλή. Σε ό,τι αφορά την αποδοτικότητα η μέθοδος των Ουδέτερων Ερεθισμάτων να παρουσίασαν τα καλύτερα αποτελέσματα μετασχηματισμού της εν λόγω συμπεριφοράς κατά δήλωση των συμμετεχόντων ακολουθούμενα από τη μέθοδο των Παρακινήτικών Συνεντεύξεων και τις Πρακτικές Αξιολογήσεις κατά σειρά. Το προτεινόμενο πλαίσιο θα μπορούσε να ωφελήσει εκπαιδευτικά ιδρύματα, όπως δημόσια και ιδιωτικά σχολεία και πανεπιστήμια, που επιδιώκουν την εκπαίδευση των ατόμων σε σχέση με την προστασία των προσωπικών δεδομένων τους ή στην εφαρμογή νέων προσεγγίσεων για την ενίσχυση της συμπεριφοράς των ατόμων ως προς την προστασία της ιδιωτικότητάς τους προς μια πιο προστατευτική συμπεριφορά. Επιπλέον, το πλαίσιο μας (PBTF) παρέχει ένα ευνοϊκό περιβάλλον για πρόσθετη έρευνα σχετικά με μεθόδους μετασχηματισμού της συμπεριφοράς της ιδιωτικότητας ενός ατόμου.

Abstract

Technological advancements like internet-connected wearables, augmented reality, mobile devices, and the prevalence of social media have made our uniqueness and individuality visible to the world. Data can be collected from individuals and businesses through various techniques, often without our awareness. One method is through IoT-connected gadgets, while another is by willingly sharing personal information on social networking sites, such as publishing intimate photos or other details. Researchers have been prompted to investigate privacy behavior due to the availability of enhanced information services. Privacy behavior includes acts such as disclosing personal information, implementing privacy-protective measures, and adjusting privacy settings. Disclosing personal information and presenting a risky privacy behavior can result in negative consequences for individuals, such as being vulnerable to identity theft, impersonation, and other associated dangers. External entities can use this data for their benefit, including creating customized advertising campaigns or influencing people's voting choices, as seen in the Cambridge Analytica case. Studying the privacy habits of the mentioned users and finding ways to enhance their privacy has been a primary focus of research for many years. Yet, no established method or framework has been discovered to consistently and effectively convert this behavior into a more protective one. This Thesis focused on three fundamental factors to address the aforementioned issue. We attempted to determine the factors that affect privacy behavior. Our research findings revealed that there are numerous factors that can impact the outcomes. We continuously explored the scientific disciplines of psychology, sociology, philosophy, and health to discover methods for changing behavior. The Cognitive Theory and its extension, the Health Belief Model, have been applied in various disciplines to facilitate behavioral change. We combined the aforementioned theories with aspects that determine privacy behavior to create a conceptual scheme that could influence individuals'

privacy behavior. We discovered in the same study that the mentioned theories are more effectively applied with experiential learning and teaching methods. We continuously researched the methods that have been applied to various fields and effectively changed individuals' behavior. Research indicates that there is widespread agreement among academics that Cognitive Behavior Therapy (CBT) and Cognitive Behavior Transformation (CBTx) have been thoroughly and successfully tested in the past for changing individuals' behavior. These methods can also be utilized through neutral stimuli, practical assessments, and Motivational Interviews (MI) methods. Finally, we introduced a new framework named Privacy Behavior Transformation Framework (PBTF) that incorporated all three methodologies described. We have successfully shown the effectiveness of the suggested framework in a five-phase empirical study. The research results demonstrated the suitability and effectiveness of the proposed Framework. The results indicated that the privacy behavior of all participants was enhanced to be more secure. The Neutral Stimuli method yielded the most effective behavior transformation results, as reported by the participants. This was followed by the Motivational Interviews and Practical Assessments methods. The proposed framework could benefit educational institutions, such as public and private schools and universities, in creating new structures or implementing new approaches to enhance individuals' privacy behavior towards a more protective one. Moreover, our framework provides a favorable setting for additional research on methods for transforming privacy behavior.

Research Publications

Research Publications in International Journals

- I Paspatis, A Tsohou & S Kokolakis. AppAware: a policy visualization model for mobile applications. Information & Computer Security 28 (1), 116-132, 2020. <https://doi.org/10.1108/ICS-04-2019-0049>
- I Paspatis, A Tsohou & S Kokolakis. How is Privacy Behavior Formulated? A review of current Research and synthesis of information privacy behavioral factors. Multimodal Technologies and Interactions, 2023. <https://doi.org/10.3390/jcp3030020>
- I Paspatis & A Tsohou. How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. Journal of Cybersecurity and Privacy, 2023. <https://doi.org/10.3390/mti7080076>
- I Paspatis & A Tsohou. Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement. Journal of Cybersecurity and Privacy, 2024. <https://doi.org/10.3390/jcp4010005>.

Research Publications in Proceedings of International Conferences

- I Paspatis, A Tsohou & S Kokolakis. Mobile application privacy risks: Viber users' de-anonymization using public data. I Paspatis, A Tsohou, S Kokolakis (2017). Mediterranean Conference of Information Systems (2017). <https://aisel.aisnet.org/mcis2017/32>
- I Paspatis, A Tsohou & S Kokolakis. AppAware: A Model for Privacy Policy Visualization for Mobile Applications. I Paspatis, A Tsohou, S Kokolakis (2018). Mediterranean Conference of Information Systems (2018). <https://aisel.aisnet.org/mcis2018/3>

Acronym Catalog

I.C.T.	Information Communications Technology
E.N.I.S.A.	European Union's Cybersecurity Agency
NIST	National Institute of Standards and Technology
VM	Virtual Machine
VMs	Virtual Machines
OSNs	Online Social Networks
GDPR	General Data Protection Regulation
IoT	Internet of Things
HBM	Health Belief Model
CBT	Cognitive Behavior Therapy
CBTx	Cognitive Behavior Transformation
MI	Motivational Interview
AIS	Association for Information Systems
ANOVA	Analysis of Variance
PBTF	Privacy Behavior Transformation Framework

Table of Contents

Part 1	16
1.Introduction	16
1.1 Information privacy behavior in the digital era	17
1.2 The research problem	18
1.3 Synopsis of our research	20
1.4 Results	25
1.5 Implications	27
1.6 Structure of thesis	27
2.Background	28
2.1 Information privacy behavior	28
2.2 Individuals' Privacy Behavior Rationality	29
2.3 Privacy Behavior Determinant Factors	29
2.4 Dominant Behavioral Transformation Theories	29
2.5 Experiential Methods in Education and Learning	30
2.6 Behavioral Transformation Experiments	31
3.Research Design and Methods	31
3.1 Privacy behavior determinant factors	32
3.1.1 Validity of our approach	32
3.2 Behavioral Transformation Theories and Educational and Teaching approaches	34
3.2.1 Validity of our research to other scientific disciplines	34
3.3 From behavioral transformation theory to methods	36
3.3.1 Experimental framework validation, methodology and execution	36
3.4 Behavioral transformation framework validity	38
3.5 Research Ethics	39
4.Summary of Work	40
4.1 Mobile application privacy risks: Viber users' de-anonymization using public data (Paper I)	42

4.2	AppAware: A Model for Privacy Policy Visualization for Mobile Applications (Paper II).	43
4.3	AppAware: A policy visualization model for mobile applications (Paper III - extend of paper II).	45
4.4	How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors (Paper IV).	46
4.5	How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors (Paper V).	48
4.6	Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement (Paper VI).	50
5.	Conclusion and Contributions	52
6.	References	56
Part 2 – Core Papers		60
Paper – I		60
Paper – II		93
Paper – III		126
Part 3 – Support Papers		167
Paper – IV		167
Paper – V		187
Paper – VI		206

Aknowledgements

This thesis is dedicated first of all to my three-member committee Prof. Dr. Spyros Kokolakis from the University of the Aegean who was also the person who laid the foundations for me to start the project. To Prof. Dr. Manos Magkos from Ionian University for his valuable help. Above all, I would like to thank Associate Professor Aggeliki Tsohou from the Ionian University first as a professor and supervisor for her guidance and then for the person Aggeliki who was close to me in the difficult times and in the easy times. Also, my friends Pavlos Malogridis and Panos Emmanouilidis who were from the beginning to the end on this journey to encourage me. My colleague Theodora Sanida, a PhD candidate at the University of Western Macedonia, who while simultaneously experiencing the research situations we helped each other. My friend Katerina Dacou who helped me think differently and whose opinion pushed me to want to investigate this specific field from another research point of view. But above all to my wife Pany Webber who, in addition to being a traveling companion, was also the person who in difficult times was there.

Also, this thesis is dedicated to:

My teachers and professors

Dimitris Fotakis (Professor NTUA)

Nikos Dimitriou (Dimocritos Institute, HOU)

Giannis Koletsos (Professor NTUA)

Dimitris Kalles (Professor HOU)

Nikos Megalios (Teacher)

Vaggelis Papadopoulos (Teacher)

Lilian Mitrou (Professor Aegean University)

My PHD colleagues

Stelios Karagiannis

Thanos Papaioannou

Katerina Soumelidou

Rena Lavranou

My friends

Aggeliki Kagkara

Nikos Benias

Nikos Batavanis

Panagiota Roussou

To my colleagues

Marios Statheros

Liana Grigoriadou

Aimilios Bagias

Elisavet Fiotaki

Afroditi Rapti

Kostas Tranoudis

Valia Myloni

Giorgos Paparis

Ioanna Karagianni

Nikos Nomikos

Dimitris Tsakiris

Evgenia Politou

Stratos Makridakis

Giannis Stellios

Aristotelis Meletiou

Penny Rigakou

To my wife, kids and family

Pany Webber

Jonas Paspatis Webber

Max Paspatis Webber

Alexandra Pappa

Michalis Negrís

Marianna Mexi

Michalis Paspatis

Konstantina Paspatis

Alexis Paspatis

Despina Paspatis

Danae Paspatis

Synopsis

This Thesis is constructed as follows: Part – I of the Thesis provides a thorough analysis of the doctoral research, the research objectives, the research methodology and design, the development of the proposed framework, and the empirical investigation and results. Part II consists of the main papers of this thesis. Part – III contains the support papers and the papers that contain the foundations of this thesis and its main contributions.

Part I

1. Introduction

The rapid developments in technology and the Internet over the last 30 years have created favorable conditions for both hardware and software manufacturers to develop and introduce new products and services. The speed of a typical home internet connection has increased 10000 times (futuretimes, 2020) while available data storage has increased 400000 times (Tech Musings, 2019). For technology and online product companies, a new era of presentation and targeted service promotion has been created. This targeted promotion can sometimes become a product of exploitation for the benefit of the companies towards the users. Companies have now moved to storing and processing large amounts of personal and non-personal data, often taking advantage of internet users' low privacy awareness. Privacy awareness is defined as the understanding related to the current privacy settings and policies of a "product as well as the understanding of the seriousness of the impact of potential privacy violations" (Tsohou and Kosta, 2017). This understanding is related to the respective privacy settings and policies of an online service or software product, as well as an understanding of the severity of the impact of possible privacy violations when using them.

According to Govani and Pashley (2005), the users who participated in a relevant field study did not take any relevant protection measure although they were aware of the effects of violating their privacy. In contrast, according to various researchers (Tow et al., 2008; Gross & Aquisti (2005); Cranor et al., 2006) users are either not fully aware of the above implications or believe that the probability of a breach occurring is small. In part, this may be due to users' fear that they will make modifications to the default settings, which will be worse in terms of privacy (Cranor et al. 2006). Many researchers (Acquisti & Grossklags (2005); Debatin et al. 2009, Dwyer, 2007, Govani & Pashley, 2007)) characterize this user behavior as myopic and state that this myopic assessment and perception of privacy risks arise due to their low awareness about the risks of violating their privacy. Added to the above is the new General Data Protection Regulation 2016/679 (GDPR, 2016) which, among other things, highlights the need to raise awareness among users when their consent is a requirement for the processing of their personal data. In the context of the awareness of individuals and the principle of transparency, the GDPR requires any information addressed to users to be "concise, easily accessible and easy to understand and to use clear and simple wording and, in addition, where appropriate, illustrative (GDPR, 2016; No. 58)". Based on the above, as well as political and social facts (e.g. the Cambridge Analytica scandal), users do not seem to be able to grasp the

big picture of what kind of data they share and how it is used, while they do not seem to be aware of the possible negative implications of the use of this data.

The purpose of this thesis is to create a new theoretical model that will help us understand users' privacy behavior and facilitate with the appropriate stimuli the possibility to improve it. The research problem that we address in this doctoral thesis is how can we transform individuals' information privacy behavior to a more protective one through the experience of predetermined events (e.g., privacy behavior simulations, neutral stimuli etc.).

The thesis is structured as follows: Chapter two analyzes the theoretical background of information privacy awareness. In chapter three, the bibliographic review is done that reveals and gathers the factors that influence privacy behavior. Chapter four analyzes the theoretical background of experiential education in the fields of psychology, philosophy and sociology. Chapter five presents the way and experiments that analyze privacy behavior as well as how to transform the current level of privacy behavior to a higher level. In chapter 6 the results of the experiments are presented. Finally, chapter 7 presents the conclusions of the thesis.

1.1 Information privacy behavior in the digital era

Multiple studies conducted by the academic community have shown that internet users express concerns regarding the privacy and the protection of their personal data (Kokolakis, 2017; Hallam & Zanella, 2017; Li et al., 2017; Gerber et al., 2018). Nevertheless, if this assertion is accurate, it prompts the inquiry as to why they exhibit a lack of concern for safeguarding themselves. For instance, individuals reveal extensive quantities of personal data while utilizing their favored social network (Dhir et al., 2016; Shane-Simpson et al., 2018). Researchers have endeavored to elucidate this inconsistency by employing the concept of "the privacy paradox," highlighting the disparity between individuals' attitudes towards privacy and their actual behaviors around privacy. Previous studies have examined the behavioral and psychological aspects that influence users' privacy behavior (Kokolakis, 2017; Hallam & Zanella, 2017; Li et al., 2017; Gerber et al., 2018). Information privacy behavior pertains to the actions taken by users to safeguard their own privacy while using Information Communications and Technologies (ICTs). This includes activities such as disclosing personal information, implementing controls to protect personal data, and configuring privacy settings. Research in the field of privacy behavior is challenging mainly because it relies on self-reported data provided by the participants during empirical investigations, as emphasized by numerous scholars (Kokolakis, 2017; Hallam & Zanella, 2017; Li et al., 2017; Gerber et al., 2018). The integration of ICT into our daily lives and the rapid advancement of technology have thrust our existence into the forefront of a global stage. We constantly subject ourselves to public

scrutiny in all aspects of our lives. Smartphones provide us with constant online connectivity. The wearables we use, which are connected to the internet, continuously monitor and assess our daily activities and state of health. We share our experiences and ideas on Online Social Networks or Social Network Sites (OSNs or SNS) as the Internet of Things (IoT) continues to play an increasingly intelligent role in our daily lives (Menard, 2020). Privacy consciousness among social networking site (SNS) users is a crucial element of their privacy conduct, as it impacts their choices about the divulgence of personal data on social networks. Revealing personal information can lead to adverse outcomes for individuals, including being targeted for identity theft, impersonation, and other related risks. In addition, external entities have the potential to utilize this data for their own advantage, such as implementing tailored advertising strategies (Mathews-Hunt, 2016; Palos-Sancheza et al., 2019) or influencing individuals' voting preferences, as exemplified by the Cambridge Analytica incident (Hinds et al., 2020).

1.2 The research problem

Based on the above, we argue that it is crucial to better comprehend the process by which privacy behavior is shaped. This understanding will aid policymakers in comprehending how users make judgments about privacy actions and how to enhance privacy behavior. There is a substantial body of research in this field, mainly focusing on the factors that affect privacy behavior. Gaining insight into the mechanisms that influence privacy behavior is of utmost importance for various reasons. Technological developments alone cannot ensure sufficient privacy protection, as the effectiveness of privacy safeguards ultimately relies on user decision. Furthermore, a considerable proportion of privacy breaches can be ascribed to individuals' insufficient awareness, understanding, or willingness to consciously embrace privacy safeguards (Kokolakis, 2017; Hallam & Zanella, 2017; Li et al., 2017; Gerber et al., 2018; Mathews-Hunt, 2016; Palos-Sancheza et al., 2019).

Various academics analyze the aspects that influence privacy behavior by examining a specific theory, such as the protection motivation theory (Rogers, 1975). Nonetheless, the various studies conclude in several determinant factors which have not been related to one another. The absence of a comprehensive framework that consolidates the existing fragmented perspectives may hinder policy makers from making informed decisions regarding promoting privacy behavior. Our study aims to address this gap by examining the determinant factors that have been found in the literature to affect individuals' privacy behavior in the digital realm, as well as identify effective treatments to encourage such conduct. After identifying the relevant determinant factors, we consolidated them into an integrated framework.

In sequence, we examined theories and techniques from the field of ICT or other fields, which can influence privacy behavior. We explored other fields such as psychology, sociology, and philosophy looking for similar treatments of human behavior. With the purpose of

documenting human behavior transformation methods from these fields, we performed a comprehensive literature analysis. Relevant theories that emerged are:

- The neuropsychological theory;
- The psychoanalytical theory;
- The behavioral theory;
- The cognitive theory.

We acknowledged that the cognitive theory and its extension and the Health Belief Model (HBM) are prevailing theories in the health disciplines (e.g., psychology, psychiatry) specifically in relation to behavioral change. Thus, HBM theory is more analytical than the cognitive theory's primary concept of how behavioral transformation may be occurred while at the same time its structure is more behavioral specific than the aforementioned theory. For example, explains how its three influential axes can be used to promote behavior transformation. Thus, this model is based on behavioral factors that can transform behavior and thus we selected it as a foundation for the development of our proposed information privacy behavior transformation model.

We researched what are the best practices to enable behavioral behavior based on the above theories. We discovered that when it comes to behavior transformation the best practices show that it can be facilitated through experiential learning and education (such as active engagement of the student with the objective of the educational target), which refers to the process of generating knowledge by transforming experiences. According to the literature experiential methods are more effective in behavioral transformation than traditional learning approaches, such as lectures, textbooks, and tests. Traditional educational methods have historically been the basis of education systems worldwide and can be employed to encourage privacy-conscious activities. Nevertheless, some of their characteristics may hinder learners' learning growth. For example, passive learning is a shortcoming of traditional education methods, as stated by numerous researchers (Conner & Norman, 1993; Conner & Norman, 1996, Jarvis, 2004). Traditional education often promotes passive acquisition of knowledge, when students passively receive information instead of actively engaging in the learning process. Therefore, these methods hinder students' involvement, critical thinking, and problem-solving capabilities. Another characteristic of traditional education methods that may hinder the learners' growth is the absence of tangible implementation. Traditional education methods sometimes prioritize abstract principles that lack practical relevance. The disparity between theoretical concepts and practical implementation can hinder learners' capacity to utilize their classroom knowledge and skills in real-life scenarios. Further, traditional education places significant emphasis on rote memorization and temporary retention, leading to restricted long-term memory and comprehension. The prioritization of rote memorization over profound comprehension hinders learners' capacity to establish connections between concepts and apply acquired knowledge in various contexts. Finally, traditional learning methods often adopt a uniform approach, thinking that all learners acquire knowledge in a uniform manner and at the same pace. Therefore, they neglect individual variations in learning styles, preferences, and strengths which can result in disengagement and subpar learning outcomes. Experts and

scholars [Jarvis, 2004; Dewey, 1938; Freire, 1998; Kolb, 1984; Rogers, 1999; Kokko, 2005; Mezirow, 1991, Mezirow; 1998, Mezirow, 1998b; Mezirow, 2006; Taylor, 1998; Dacou, 2018] have supported the integration of experiential learning techniques to overcome the constraints of traditional education methods.

In order to utilize the aforementioned, we developed a behavioral transformation framework, based on experiential methods and the Cognitive Behavior and HBM theories. Our proposed framework incorporates the three primary methods: Cognitive Behavioral Therapy (CBT) and Cognitive Behavioral Transformation (CBTx) that are based to the Cognitive Theory and HBM, practical evaluations, and motivating interviews. We provide evidence to suggest that if the above approaches are successfully applied to the field of ICT, they can transform individuals' privacy behavior to be more protective, hence addressing the research gap mentioned. In total, the research problem that we address in this doctoral thesis is how can we transform individuals' information privacy behavior to a more protective one.

1.3 Synopsis of the research

This thesis investigated new approaches to transform individual's privacy behavior to a more protective one. Our approach provided a novel privacy behavior transformation framework that is based on experiential theories and methods. These theories have been implemented successfully to other disciplines such as psychology, sociology, philosophy and health but to the best of our knowledge no complete framework have been implemented to the ICT context.

[Support Paper IV](#). In this paper (table 1), we investigated how application developers of popular messaging apps such as Viber can exploit users' low privacy awareness to gain an enormous amount of their personal information. Continuously, after further investigation of the Viber app we developed a methodology (Support [Paper IV](#), figure 2) to manipulate Viber's Database (Support [Paper IV](#), Figure 1). This database is available after an individual installs Viber for desktop application. After we facilitated our methodology to exploit Viber's database, we de-anonymized the 84% of a pseudorandom sample of 2000 cellular telephone numbers of the Greek mobile network. We found multiple persons' real name and surname and in some cases their address or workplace as well as some of their habits. Continuously, we conducted a questionnaire to investigate Viber users' knowledge about the data that are possible to be found through our exploitation approach. The unexpected outcome of this questionnaire resulted that individuals' privacy awareness was limited as well as their privacy behavior actions. The findings of this investigation in combination with other findings though our research made us to swift our research interest from information security to individuals' privacy behavior enchantment to a more protective one.

In [Paper I](#), we started our academic journey regarding the reasons behind individuals' privacy actions. We performed an in-depth literature review on the underlying factors that affecting ICT users' privacy behavior. The outcomes of our research find evidence that privacy behavior is affected by a variety of factors, including individual ones (e.g., demographics) and contextual ones (e.g., financial exchanges). We synthesized a framework that aggregates the scattered factors found in the literature and affect privacy behavior. We found that privacy behavior is affected by 22 factors. We grouped these factors in 11 clusters ([Paper I](#), figure 3). These outcomes led us to start planning a privacy behavior transformation framework.

In [Paper II](#), we investigated how other scientific fields such as psychology, sociology and philosophy have tried to transform individuals' behavior. Throughout our research we found that the dominant way for individuals' behavioral transformation was through experiential learning or through education methods. We examined various learning and educational methods to conclude that there is scientific consensus from all of the aforementioned fields that experiential learning is advantageous compared to other methods. Continuously, we found out that the major theory that is used when it comes to experiential learning is the Cognitive Theory ([Paper II](#), figure 2). According to this theory, to transform individuals' behavior the following steps are followed: firstly, there must be a stimulus, this stimulus will intervene with the cognitive processes of the individuals, then their behavior is depended of the outcome of their cognitive process reaction. Continuing our research, we found an extension of Cognitive Theory called the Health Belief Model (HBM) from the health field when it comes to behavioral transformation. Focusing on this model we found out that according to cognitive theory, cognitive processes are playing a significant role on behavioral transformation. Cognitive processes are consisted of three influential axes: beliefs, perceptions and attributions while each influential axe contains one or more categories ([Paper II](#), figure 2). Each influential axe is affected by behavioral transformation factors such as perceived benefit, perceived barriers, personal beliefs, expectations and productive causes. At this stage, we saw possible similarities with the privacy behavior determinant factors we investigated on our previous work ([Paper I](#)). We used the nearest neighbor theory to match the most privacy behavior determinant factor with the behavioral transformation factors of cognitive theory's influential axes and HBM's behavior transformation factors. This resulted the conceptual scheme of cognitive theory with the adapted privacy behavior determinant factors ([Paper II](#), figure 8). This conceptual scheme provided potential implications to individuals, organizations and academic institutes to create new privacy behavior transformational frameworks by aggregating the above work to the ICT environment.

Finally, on paper III we constructed and validated the efficiency of a new privacy behavior transformation framework. To develop this framework, we first investigated what methodologies are applied in other disciplines, such as psychology, sociology, philosophy and

health to transform individuals' behavior. We found that there is evidence that behavior can be modified with three main methodologies: a) neutral stimuli such as visual or hearing effects, b) by practical assessments and an a new methodology called motivational interviews (MI). For each of the above methodologies have been conducted multiple experiments.

For example, experiments have been conducted that proved that neutral stimuli presented favorable results on behavior transformation. The methodologies that most experiments followed are referred to as cognitive behavior therapy (CBT) and cognitive behavior transformation (CBTx) both derived from the cognitive theory. Another theory called practical assessment experiments also presented good results mostly in the disciplines of philosophy and sociology. Finally, the last methodology called motivational interviews (MI) present also strong influence to behavior transformation. This methodology foundations have been used in all aforementioned scientific fields. This theory consists of two parts. In the first part the interviewer tries to understand interviewees' emotional state and make them feel uncomfortable or even scared by activating a cognitive process such as fear. In the second part, the interviewer tries to encourage and motivate the interviewees by positive speeches and actions.

Our framework consists of all the above methodologies ([Paper III](#), figure 1) adjusted to the ICT environment. To validate this framework, we conducted an experiment with 9 participants. The validation process contained 5 phases: questionnaire selection, questionnaire completion, the experiment's environment creation, the experiment implementation and finally the results' analysis ([Paper III](#), figure 2). More specifically, we selected a privacy behavior questionnaire that consisted of privacy behavior questions. Each question derived through research and it should activate at least one of our privacy behavior determinant factors. The questionnaire was completed from all participants, and it was targeted to show us participants' current level of privacy behavior. The environment creation was consisted of multiple Gmail account, virtual machines, the implementation of methodologies we presented to "support papers" [IV](#) and [V](#), the selection of the visual content, the privacy behavior content and the installation of important mobile and desktop apps.

The validation process also involved a participants' mobile phone monitoring period. We provided the phones, which we specifically adjusted to provide with information about the participants. The reason behind that action was to give us more information about the participants' daily habits and other personal information. This material was used to construct part of the questions of the Motivational Interview experiential process. After the end of the experimental period all participants re-completed the questionnaire of phase 2. The results provided us evidence about the privacy behavior transformation framework's efficiency. To measure the efficiency of the results we conducted T-test to every question by comparing each

question one by one. Continuously, each participant got re-monitored again for a smaller period of time. The reason behind this action was to check not only the privacy behavior that participants stated but also to verify their actual behavior. Finally, each participant was asked to respond what method liked more and which less. The majority of the participants stated that visual content was their favorite method and the least the practical assessments.

From the results (containing the re-monitoring period) we concluded that our framework provides enough evidence that can successfully transform individuals' privacy behavior to a more protective one. This framework approach followed other scientific fields methodologies of how to transform individuals' behavior. The results confirmed our approach while the theoretical background showed us the reasons why this approach work.

This framework could prove advantageous to the academic community by facilitating the learning of privacy behavior alteration from individuals' early age and continuing even after they have completed their educational journey. Our framework can be utilized by elementary schools, academic institutes, and private schools to enhance students' adherence to protective privacy behavior. Furthermore, it has the potential to redirect the focus of privacy scholars onto novel avenues of investigation.

Table 1 presents the flow of research in this thesis.

Table 1. Research sequence

Title of Thesis	Transforming Information Privacy Behavior through Experiential Procedures
Research Focus	Identifying approaches and propose a framework to transform individuals' privacy behavior to a more protective one.
	↓
Support Paper IV	Paspatis, Ioannis; Tsohou, Aggeliki; and Kokolakis, Spyros, "Mobile Application Privacy Risks: Viber Users' De-Anonymization Using Public Data" (2017). MCIS 2017 Proceedings. 32. https://aisel.aisnet.org/mcis2017/32
Key Findings	This research showed that Viber users presented limited privacy awareness as well as non-protective behavior regarding their privacy. This led us to search to a solution to guide the individuals to a more protective privacy behavior.
	↓
Paper I	How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors (Paspatis, I., Tsohou, A., & Kokolakis, S. (2023). How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information

Privacy Behavioral Factors. Multimodal Technologies and Interaction, 7(8), 76).
<https://doi.org/10.3390/mti7080076>

Key Findings This research aims to identify the key characteristics that determine individuals' privacy behavior. Through the identification of these variables, we may facilitate the development of methodologies or frameworks that effectively safeguard privacy and prioritize user-centered design. Based on an analysis of multiple research papers, we have discovered compelling evidence that privacy behavior is influenced by 22 different factors, which we have organized into 11 distinct groups.



Paper II How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors

(Paspatis, I., & Tsohou, A. (2023). How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. Journal of Cybersecurity and Privacy, 3(3), 396-415). <https://doi.org/10.3390/jcp3030020>

Key Findings Following the findings of Paper I, our research shifted its focus towards investigating the ideas pertaining to behavioral transformation in other disciplines. We have seen that cognitive theory has been effectively applied to the fields of psychology, philosophy, and sociology. Next, we discovered the health belief model, which is an expansion of cognitive theory. This theory comprises behavioral transformation variables that are integrated into its core, known as cognitive processes and influencing axes. Ultimately, we have determined that the most beneficial approach to applying the aforementioned theories is by means of education and acquiring knowledge through experiential approaches. In order to establish a framework based on the aforementioned theories, we needed to align each behavioral aspect of the Health Belief Model (HBM) with the determining factors of privacy behavior.



Paper III Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement

(Paspatis, I., & Tsohou, A. (2023). How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. Journal of Cybersecurity and Privacy, 4(1):76-104). <https://doi.org/10.3390/jcp4010005>

Key Findings This paper examined the approaches that have been applied in the fields of psychology, philosophy, and sociology to effectively modify individuals' behavior, based on the findings of our prior research. Three primary approaches, namely neutral stimuli, practical assessments, and motivating interviews, have been employed to induce behavioral transformation. We developed a framework that incorporates all of the aforementioned techniques. In order to assess the effectiveness of our framework, we carried out a controlled experiment in a laboratory setting including a total of 9 people. The validation process comprised five phases: a) a preliminary phase in which we selected a questionnaire to determine privacy behavior, b) using the aforementioned questionnaire, we evaluated participants' initial privacy behavior, c) the establishment of the experimental environment, d) the execution of the experiment, and finally e) the analysis of the results. The findings demonstrated that participants' privacy behavior

effectively transitioned to a more secure state, even several months after the conclusion of the experiment.

1.4 Results

In our initial investigation for support [Paper IV](#), we conducted an examination of the Viber application and successfully proved the ease with which one can ascertain the identities of unidentified Viber users. We conducted a study using a pseudorandom sample of 2000 cellular telephone numbers to investigate the possibility of uncovering personal information associated with them. We conducted an empirical study that examines the behavior reported by Viber's users and compares it to their actual behavior. The findings of this study indicate that users' anonymity and privacy can be readily compromised, resulting in the exposure of their information to those with knowledge in this area. Additionally, our research revealed that Viber users have a limited understanding of privacy and, more importantly, engage in behaviors that do not effectively protect their privacy. These recent unforeseen outcomes have compelled us to redirect our focus towards discovering methods to convert individuals' privacy behavior into a more protective one.

During the in-depth literature review we conducted in [Paper I](#), we discovered compelling data indicating that privacy behavior is influenced by a multitude of circumstances. Through a comprehensive literature analysis, we identified 945 papers that examined the relevant aspects of privacy behavior. Following the application of our exclusion criteria, we identified 226 papers that investigated privacy behavioral aspects (see to [Paper I](#), figure 1). Upon analyzing the aforementioned publications, we have determined that there are 22 elements that significantly influence privacy behavior. We categorized these characteristics into 11 groups based on their similarity. These considerations formed the basis of our paradigm for transforming privacy behavior.

In order to construct this framework, in paper II, we conducted a thorough investigation of several fields in order to identify existing theories that have the potential to modify individuals' behavior. Our analysis determined that the prevailing theory in behavior modification is cognitive theory, along with its extension, the Health Belief Model (HBM), particularly when integrated with experiential learning and instructional approaches.

In paper III, we focus once on other literary works to examine the techniques that have been utilized in many fields and effectively modify individuals' behavior. Our research has demonstrated that three techniques, namely neutral stimuli, practical assessments, and motivational interviews, have consistently proven effective in modifying individuals' behavior

on several occasions. We developed a framework that incorporates all of the aforementioned methodologies. In order to assess the effectiveness and verify our framework, we performed a laboratory experiment involving a total of 9 people. The outcomes of our experiment demonstrated that our framework has the ability to successfully modify individuals' privacy behavior. The most effective strategy was found to be the neutral stimuli, while the practical assessments were found to be the least effective.

This thesis yielded four notable results. Initially, we introduced the 11 determinant factors that possess the capacity to influence individuals' conduct. As far as we know, this is the initial study that gathered the bulk of characteristics that potentially impact persons' privacy behavior. The findings of this research can be utilized by individuals, software firms, and academic institutes to develop novel programs, frameworks, apps, and other tools that cater to individual needs. Continuously, the data of our second investigation demonstrated what concepts have the capacity to transform individuals' behavior can be employed to the field of ICT. Based on our current understanding, this research not only confirms that the implementation is effective, but also provides insights into the mechanisms and reasons behind its success. Ultimately, our third research endeavor successfully developed, quantified, and validated a paradigm for transforming privacy behavior. This framework is built upon robust approaches that have been effectively employed by other fields. This framework effectively enhances individuals' privacy behavior, making it more protective. Furthermore, the result is not only a transformation framework, but also an explanation of its underlying principles. We have been conducting research on individuals' privacy behavior and associated activities for more than two decades. Nevertheless, within the academic sphere, the predominant means of influencing an individual's personal conduct mostly include traditional instructional methods, even though many individuals still depend on this strategy for acquiring knowledge or may not receive any formal education on this matter whatsoever. We found no indication of a privacy behavior change framework being implemented in primary or secondary schools through our research. However, these frameworks are primarily prevalent in higher education, namely in academic curricula that have a strong emphasis on information technology. On the other hand, fields such as sociology and psychology have performed thorough research and trials to alter the behavior of individuals. The framework that we propose for transforming privacy behavior is based on theories and experiences from the mentioned areas. Through utilizing our previous research on the factors that impact privacy behavior and conducting a thorough analysis of behavior modification theories in other fields, we have developed a strong framework for effectively changing privacy behavior.

1.5 Implications

This research has several implications. In [Paper I](#), we found and clustered the 11 determinant factors that can influence privacy behavior of an individual. These results can be facilitated by companies, programmers, individuals, researchers, universities, institutes and schools to suggest new methodologies, create frameworks etc. regarding privacy behavior. To the best of our knowledge this is the first research that aggregated the previously identified privacy behavior determinant factors in integrated research.

Continuously, the work of [Paper II](#) provided the following implications. By adjusting privacy behavior determinant factors and cognitive theory/HBM we provided new theories that we can test regarding privacy behavior. By facilitating these theories to construct methodologies and frameworks we provided new paths regarding privacy behavior transformation. Now, researchers, practitioners, academic institutes and schools can facilitate the above proven theories to suggest privacy behavior transformation frameworks, privacy behavior enchantment emulators etc. With our work on [Paper III](#), we have a validated framework that successfully transforms privacy behavior. Researchers, academic institutes and companies can step on our work, to use it or develop and provide equal or even better privacy behavior transformation frameworks to students, individuals, etc. Finally, this framework has the potential to benefit the academic community by aiding the acquisition of privacy behavior transformation at an early age and continuing throughout individuals' educational journey. The framework we have developed can be employed by primary schools, academic institutes, and private schools to improve pupils' compliance with protective privacy behavior. Moreover, it has the capacity to shift the attention of privacy researchers towards new areas of study.

1.6 Structure of thesis

The thesis is organized into three sections. Part 1 consists of 5 chapters. Chapter 1 serves as the introductory section. This encompasses the background information of the theses, the specific issue being investigated, a brief summary of the investigation, the findings, and potential consequences. Chapter 2 provides the essential theoretical framework required to comprehend the contributions made to this thesis. Chapter 3 introduces the research design and methodologies. This encompasses the philosophical framework, methodologies, and soundness, as well as the research ethics associated with this study. Chapter 4 provides a concise overview of the tasks accomplished in this thesis. Chapter 5 encompasses the last remarks and incorporates the findings of this study as well as potential future endeavors. In Part 2 of the thesis, we present three research papers that provided support to this thesis, while in Part 3, we present the three core research papers that comprise the primary body of the thesis.

2. Background

This doctoral thesis addresses the problem of enhancing individuals' privacy behavior by identifying the factors that influence their actions and exploring how these factors might be used to promote a more protective privacy behavior. The issue of enabling protective privacy behavior has been under scrutiny for several years. Privacy behavior refers to behaviors related to the individual control of personal information and involves actions such as disclosing personal information, implementing privacy-protective measures, or adjusting privacy settings (Tsohou and Kosta, 2017). The initial concerns over the way Internet users behave regarding their privacy began to emerge among researchers and academics with the advent of online social networks (OSNs). Since the emergence of OSNs, several entities including organizations, developers, and malicious attackers have attempted to take advantage of OSN users' limited privacy awareness, often in conjunction with poor privacy-related behaviors (Mathews-Hunt, 2016; Palos-Sancheza et al., 2019). Privacy awareness pertains to an individual's comprehension and acknowledgment of the significance and worth of safeguarding personal data. Companies have begun specifically targeting members of OSNs with customized adverts in an effort to entice them into purchasing products or services. Other companies, individuals, and developers have attempted to exploit ICT users' low awareness, persuading them to reveal their personal data, with or without consent (Mathews-Hunt, 2016; Palos-Sancheza et al., 2019; Hinds et al., 2020). Personal data hold inherent value that can be utilized for both beneficial and malevolent purposes. Research indicates that if personal data fall into the wrong hands, data subjects may face numerous risks such as theft or impersonation, and others.

2.1 Information privacy behavior

Privacy behavior encompasses the behaviors, choices, and tactics that individuals utilize to regulate their personal information and exert authority over its accessibility in different social situations. Privacy practices comprise a broad spectrum of measures performed by individuals to safeguard their rights to privacy and retain authority over their personal information throughout contacts with others, whether in physical or digital environments (Aquisti et al., 2015; Debatin et al., 2009). A multitude of studies have embarked on examining the underlying causes of individuals' privacy behavior acts, as well as the motivations that compel them to engage in risky privacy behaviors. After extensive research and analysis, researchers and academic institutions have concluded that individuals' risky activities regarding privacy cannot be attributed to a single cause, but rather stem from a complex set of factors. Although a scientific consensus about users' privacy behavior and risky activities has not been

reached, several theories, such as the "privacy paradox," have been established. The "privacy paradox" refers to the disparity between persons' apprehensions over privacy and their tangible actions pertaining to privacy (Kokolakis, 2017). More precisely, this refers to the phenomena wherein individuals voice apprehensions over their privacy during surveys and interviews, yet frequently fail to align their actions with these concerns in their online activities.

2.2 Individuals' Privacy Behavior Rationality

A primary focus of this thesis was to comprehend the underlying reasons behind individuals' inclination to engage in risky privacy behavior, despite knowing the potential risks that they may encounter (i.e., the privacy paradox). Upon recommencing our investigation into this subject, we have discovered two fundamental findings. First and foremost, it is the individuals themselves who bear the most responsibility in making privacy decisions. The ultimate authority over a private action, regardless of the laws or directives established by a government or organization, is with the individual. Although this decision may appear illogical in certain instances, it is a frequently employed strategy. When individuals are traveling abroad, they often discuss their experiences on online social networks (OSNs), even though they may be aware that someone could potentially use this knowledge and carry out criminal actions, such as burglarizing their home. This scenario, along with similar ones mentioned in paper I.

2.3 Privacy Behavior Determinant Factors

We conducted an extensive literature research to identify factors that could influence individuals' privacy decisions and actions. The primary discovery of this literature analysis was that behavioral factors are the underlying cause of individuals' privacy behavior. We conducted an extensive investigation in order to identify a taxonomy or, at the very least, a list of determining factors. An analysis of the existing literature revealed that a limited number of determinant factors truly play a significant role. Towards providing an integrated view of the factors that influence privacy behavior, we conducted a research study (referred to as "[Paper I](#)") where we systematically documented all the factors that determine privacy behavior, as identified in the existing literature. These factors have the potential to influence individuals' actions regarding privacy, either positively or negatively.

2.4 Dominant Behavioral Transformation Theories

Following the analysis of privacy behavior determinant factors, we began contemplating how we can use this knowledge to enable privacy protective behaviors, in [Paper](#)

II. We have extended our investigation to other scientific disciplines in order to identify theories that have been previously applied to enable behavioral transformation. We discovered that the Cognitive theory and its expansion, the Health Belief Model (HBM), yielded positive outcomes for behavioral transformation. Cognitive theory posits that cognitive processes, which are influenced by inputs and emotions, play a mediating role in shaping behavior. Weinman (1990) defines cognitive processes as encompassing beliefs, perceptions, and attributions, which are also referred to as productive causes. The HBM pertains to the scientific field of psychology that examines human behavior within the framework of health and illness (Abraham & Sheeran, 1995). Interestingly, the HBM comprises influential behavioral dimensions, denoted as axes, which in turn consist of behavioral factors. We argued that these theories would be suitable for utilizing them in order to comprehend and transform individuals' privacy behavior.

2.5 Experiential Methods in Education and Learning

Our research revealed an academic consensus that the most efficient approach to applying behavioral transformation theories is through experiential learning and educational approaches (Jarvis (2004); Dewey (1938); Freire (1998); Kolb (1984); Rogers (1999); Kokko (2005); Mezirow (1991, 1998, 1998b, 2006); Taylor (1998)). Experiential learning refers to the method by which knowledge is generated through the conversion of experience, as stated by Kolb (1984). We have discovered that these approaches offer more benefits for modifying behavior compared to traditional methods of education. While traditional education methods have been the prevailing strategy for behavioral modification for centuries, experiential methods have shown to yield superior outcomes (Kolb (1984); Rogers (1999); Kokko (2005); Mezirow (1991, 1998, 1998b, 2006)). Excluding Aristotle, who voiced this belief in the 4th century B.C. (Brown & Brown, 2009), there is ample evidence in the literature and several scientific domains that behavior can be more effectively transformed through experiential learning approaches. Experiential learning entails engaging learners in practical activities, encouraging reflection, and promoting active experimentation, hence offering numerous benefits. Experiential learning promotes active engagement and personal investment, enabling students to establish clear correlations between academic ideas and real-world encounters. This engagement promotes a more profound comprehension, as well as a feeling of significance and practicality. Experiential learning facilitates the acquisition of practical skills by engaging learners in authentic situations, simulations, and problem-solving tasks. This enhances students' capacity to effectively apply their knowledge and skills in real-life contexts, thereby equipping them to tackle real-world challenges. Experiential learning enhances understanding and meaningful learning by actively involving learners in real-life situations. This leads to better retention and the ability to apply knowledge and skills in new and unfamiliar scenarios.

Various scholars, such as Jarvis (2004), Dewey (1938), Freire (1998), Kolb (1984), Rogers (1999), Kokko (2005), Mezirow (1991, 1998, 1998b, 2006), Taylor (1998), and Dacou (2018), have supported this idea. Responding to the above results, paper III engaged to find ways to utilize three things:

- The privacy behavior transformation factors
- The theories that can effectively affect behavior
- Experiential methodologies that can utilize the behavioral transformation theories.

Upon reviewing the literature, we found no research model or theory for privacy behavior transformation, which can take into account all identified factors which can influence privacy behavior nor can utilize experiential learning methods. In response to the aforementioned gap, we developed a privacy behavior transformational framework.

2.6 Behavioral Transformation Experiments

Addressing the aforementioned issue poses a formidable challenge. Diverse approaches have been employed in the past to modify individuals' behavior, with successful outcomes in numerous scientific domains. However, ethical concerns have been raised. It appears that in the past, the level of acceptance of ethical standards was different compared to the present. Numerous scientific experiments have effectively altered participants' behavior, but their methodologies were excessively invasive and, in few instances, caused injury to both human and non-human participants. In the 21st century, certain procedures, such as the Watson and Rayner (1920) experiment, may be prohibited.

From this standpoint, we have taken a reflective approach to identify non-intrusive experiential methods that can yield positive outcomes. The key criterion is that these methods should be easily accessible to participants, allowing them to discontinue the process at any time without facing any adverse consequences. In paper III, we identified the modules of a behavioral transformation framework, based on the theoretical background described in section 2.2. Based on the implementation of empirical research, we demonstrated that the proposed framework can effectively transform privacy behavior, resulting in increased protection. This approach not only addresses the question of **whether** it is effective, but also delves into the underlying reasons behind its effectiveness and answering **why** it is effective.

3. Research Design and Methods

In the doctoral thesis we focused our attention on studying individuals' privacy behavior and understanding the underlying reasons behind their privacy activities. Our

approach can be segmented into three significant milestones. Our first objective was to comprehend the underlying motivations behind individuals' decisions regarding privacy, as outlined in the conclusions of [Paper I](#). Our second objective was to explore strategies to effectively influence and transform individuals' behavior towards a more protective stance, as indicated by the findings of Paper II. Our third objective was to develop a framework for transforming privacy behavior towards proactive privacy practices (Paper III). In the following subsections, we explain how we ensured the soundness of the design and methodology employed in each of the papers ([I](#), [II](#), [III](#)).

3.1 Privacy behavior determinant factors

In Paper I, we implemented a comprehensive literature evaluation on the factors that may influence privacy behavior. We examined the fundamental elements that impact individuals' privacy behavior, as well as identify effective treatments to encourage such behavior. In the paper, we discussed how privacy decisions related to the sharing of personal information can lead to adverse outcomes for individuals, such as identity theft or impersonation. Furthermore, external entities have the potential to utilize this data for their personal gain, such as implementing focused advertising strategies. Through the identification of the factors that can influence users' privacy behavior, we can contribute to the development of strategies for efficient privacy safeguarding.

3.1.1 Validity of our approach

We implement various criteria and safeguards to maintain the integrity of the articles we include when conducting our study for Paper I. As an initial precaution, we exclusively incorporated the scientific search engines of the most reputable journals in the information systems area, commonly referred to as a collection of eight. Additionally, we added internationally recognized journals that are part of the science citation index. The Association for Information Systems (AIS) considers the "basket of eight" to be one of the most significant and influential journals in the subject of Information Systems. Therefore, we selected the journals that are published in the proceedings of international conferences, ensuring that only conferences recognized by the AIS were included as an additional measure of protection. The important terms employed were: Privacy behavior, privacy attitude, determinants of privacy behavior, determinants of privacy attitude. In the initial exploration of elements that affect privacy behavior, researchers came across studies that examine the concept of the "privacy paradox". As a result, this phrase was added in the literature review. Table 2 displays the journals included in the "basket of eight" list, as well as the journals and conferences affiliated with the AIS. It also provides the article count for each journal and conference proceedings.

Table 2. Number of articles we chose per search source.

Source	Number of Articles
European Journal of Information Systems (EJIS)	55
Strategic Information Systems (Search in Science Direct)	58
MIS Quarterly (MISQ)	32
International Conference on Information Systems (ICIS)	14
Information Systems Research (ISR)	13
Americas Conference on Information Systems (AMCIS)	11
European Conference on Information Systems (ECIS)	9
Journal of the Association for Information Systems (JAIS)	12
Pacific Asia Conference on Information Systems (PACIS)	7
Journal of Information Management Systems	5
Recognized international journals with citation index	10
Total number of articles	226

By employing the aforementioned sampling methodology, we were able to identify a total of 945 papers. Nevertheless, certain papers that examined the respective occurrences failed to uncover the elements that influence privacy behavior. Consequently, we excluded the studies that, despite meeting the search criteria, did not specifically investigate the elements that impact privacy behavior and did not provide corresponding data. Hence, we eliminated 648 papers as they did not specifically investigate our targeted subject matter. After completing this procedure, a total of 297 papers were left that examined or identified particular characteristics that have a direct or indirect impact on privacy behavior. Additionally, we rejected 71 publications that focused on factors that have an indirect impact on privacy behavior. Specifically, these studies examined characteristics that only influence other factors that ultimately determine privacy behavior. Consequently, a total of 226 publications were identified that demonstrated direct impacts on privacy behavior. The findings of our research concluded that there are 22 determinant factors that can influence individuals' privacy behavior. We categorized these characteristics into 11 groups based on their similarities. Each factor group might consist of one to four elements. The aforementioned factors are depicted in figure three of [Paper I](#).

3.2 Behavioral Transformation Theories and Educational and Teaching approaches

In order to harness the factors that determine privacy, in [Paper II](#) we performed a thorough examination of existing literature to identify hypotheses that have proven to be helpful in triggering behavioral changes. Due to the lack of relevant literature in the domain of computer science, we have redirected our focus towards other scientific disciplines, including psychology, sociology, and philosophy. As psychology originated in the realm of philosophy but later shifted to the domain of health, we have likewise incorporated the entire scientific field of health into our research concepts. The results of this study demonstrated that cognitive theory and its expansion, the Health Belief Model, are effective theories for changing behavior. Our research revealed that the most effective way to use the specified theories for behavior transformation is through experience and educational methods, rather than traditional ways.

3.2.1 Validity of our research to other scientific disciplines

In order to ensure the validity of our research, given that it falls outside our areas of expertise, in [paper II](#) we conducted an initial investigation into which search engines are recognized as reliable sources for scientific research in the fields of psychology, sociology, philosophy, and health. Subsequently, we implemented a methodical approach to explore several scholarly databases. In order to conduct comprehensive research across many scientific disciplines, we specifically focused on utilizing the most prevalent search engines within each respective topic. In order to locate papers pertaining to philosophy, we employed the following search engines: PhilPapers, Jstor, PubMed, and the Stanford Encyclopedia of Philosophy. In order to locate papers pertaining to sociology, we utilized three resources: Sociological Abstracts available at www.proquest.com/sociologicalabstracts, ProQuest Social Science Journals accessible through search.proquest.com/socialsciencejournals, and SocArXiv. In order to locate publications pertaining to psychology and health, we utilized the search engines PubMed, PsycINFO (www.apa.org/pubs/databases/psycinfo), and PsycARTICLES (www.apa.org/pubs/databases/psycarticles). In addition, we incorporated broader databases such as Google Scholar and Scopus. The search was performed with pertinent keywords including "experiential learning", "experiential learning methods", "theory selection for experiential learning and behavior modification", and "behavior modification methods and theories". A comprehensive search initially produced a substantial quantity of articles, which were subsequently narrowed down using predetermined criteria for inclusion and exclusion.

The theory selection process involved a comprehensive analysis of the theories and models identified in the literature. We assessed the pertinence, empirical substantiation, and practicality of each theory within the framework of behavior modification, behavior enhancement, and the manipulation of human behavior. The chosen theories were picked based on their capacity to offer insights into comprehending and altering human behavior across all age groups, with a bias for ideas that are specifically applicable to adults. The rationale behind this decision is our primary objective to verify the effectiveness of our approach in future studies with adult participants. The selected theories formed the basis of our study framework. In order to uncover pertinent learning theories, we undertook a comprehensive examination of studies that explored diverse methodologies for modifying human behavior. We examined multiple learning theories, such as experiential learning and persuasive technology. The selected theories were chosen based on their probable efficacy in promoting individuals' adoption of privacy-conscious conduct.

We abstained from imposing any restrictions on the temporal scope or sorts of publications. Instead, we considered journal articles and conference pieces to be appropriate sources for obtaining satisfactory results. The keywords included were: experiential learning, experiential education, experiential learning methods in psychology, experiential learning methods in sociology, and experiential learning methods in philosophy. In addition, we have included other works that examine experiential techniques and experiments that impact learning and education through the use of experiential procedures in the aforementioned disciplines. The majority of these books are available only in physical format and are not accessible online. The process of theory selection involved a comprehensive analysis of the theories and models found in the existing literature. We assessed the pertinence, empirical substantiation, and practicality of each theory within the framework of behavior modification, behavior enhancement, and the manipulation of individuals' behavior. The chosen theories were picked based on their capacity to offer insights into comprehending and altering human behavior across all age groups, with a bias for ideas that are specifically applicable to adults. The rationale for these selections is because our primary demographic for doing future research on our framework consists of individuals aged 18 and above. The selected theories formed the basis of our study framework. In order to uncover pertinent learning theories, we undertook a comprehensive examination of studies that explored diverse methodologies for modifying human behavior. We examined multiple learning theories, such as experiential learning and persuasive technology. The hypotheses were selected based on their probable efficacy in promoting privacy-conscious behavior.

In order to determine pertinent learning theories, we conducted an extensive study of studies that examined various methods of altering individuals' behavior. We examined multiple learning theories, including experiential learning and persuasive technologies, among other

options. The chosen theories were picked based on their probable efficacy in fostering privacy-conscious behavior.

To adapt the privacy behavior determinant factors with the cognitive theory and HBM we used the nearest neighbor theory. We chose this theory because the nearest neighbor matching method is especially advantageous when the number of variables is limited. This method is applicable in various domains including epidemiology, economics, and psychology. It is used to assess the similarities between observed variables, the close correlations among observed variables, or the outcome of a statistical or medical experiment.

3.3 From behavioral transformation theory to methods

As previously stated in section 3.2, as well as in Paper II and chapters [1](#) and [2](#), it appears that behavior can be effectively transformed using experiential methods. In order to identify the strategies that have effectively been applied to different fields and resulted in behavioral changes, we conducted a thorough investigation of the pertinent literature. The same criteria as in section 3.2 were utilized, with the following keywords: "experiential transforming behavioral methods," "experiential modification behavioral methods," and "transforming behavioral methods in psychology, sociology, philosophy, or health." The results of our research were highly conclusive, demonstrating that behavior has been effectively modified by the implementation of three techniques: neutral stimuli, practical assessments, and motivating interviews. The trials conducted during the last 50 years but are still regarded as genuine and accurate, despite some of them not being relevant to the 21st century.

3.3.1 Experimental framework validation, methodology and execution

The behavioral transformation framework comprised all three methods outlined in section 3.2. The inclusion of all approaches was motivated by two primary objectives: to enhance the potential for individuals to modify their privacy behavior, and to determine the preferred methodology within the experimental group. In order to pilot test the framework, we enlisted the participation of 9 individuals, who were unknown to us to mitigate any potential prejudice. In order to assure the framework's applicability to diverse groups, we have established the following recruitment criteria: The selection criteria were primarily based on three factors: participant unfamiliarity to mitigate potential bias, absence of personal connections such as family, academic affiliation, or university enrollment to ensure impartiality, and adulthood to meet the consent form requirements for participation in the

experiment. The majority of the participants were enlisted through the utilization of the "friends of a friend" strategy. The selection of individuals was conducted using a stratified procedure. More precisely, we carefully chose volunteers from a diverse spectrum of age, gender, educational attainment, and occupation. We intentionally strived to achieve a balanced inclusion of both genders, encompassing participants from diverse professional backgrounds. In addition, each participant had to have a minimum age gap of 5 years from all other participants, regardless of their gender. The purpose of the stratification method was to evaluate the efficacy of the framework in every possible combination. Each subject completed an analytical consent form in order to participate in the study. Aside from the consent form, all participants were provided with other details about the experiment, which may not have been thoroughly addressed in the consent form. The provided material encompassed a comprehensive analysis of the experiment, along with the potential benefits expected for the participants, researchers, and society. The consent form and the experiment complied with the ethical requirements of our university and conformed to Cope's best practices (COPE).

In order to guarantee the privacy of the participants, we have constructed virtual machines that are identical for each participant. Using this process, we segregated the individuals' data from one another. This methodology serves as a protective measure for ensuring data security and safeguarding the privacy of every individual. After concluding the studies, all data can be securely erased by eliminating each virtual computer and its associated stored data. As an additional precaution, we have established the process of securely erasing the unused storage space allocated to the virtual machines. In order to implement the aforementioned technique, we integrated all virtual machines into our on-premise infrastructure and dedicated a separate disk partition specifically for storing the data of each virtual machine. This partition can be readily destroyed or securely wiped to ensure that no data can be recovered.

In order to validate both our results and our approach, we used the following procedure. The results were initially analyzed using a two-factor quantitative ANOVA technique without replication. We used the ANOVA method since it is recommended for instances with multiple factors that impact an independent variable. As previously demonstrated in Chapter 2, our instance consists of a grand total of eleven determining factors. Moreover, ANOVA is recommended for evaluating multiphase approaches, which we will carry out in our particular scenario. We conducted Cronbach's Alpha Analysis on the participants' responses to the initial questionnaire. The Cronbach's Alpha technique was employed to evaluate the questionnaire's validity. Given the small sample size of 9 participants, this methodology was chosen as it is regarded as the most direct method for testing a questionnaire. Moreover, as the purpose of this questionnaire is not to uncover or explain any phenomenon, but rather to compare the results before and after the experiential transformation, we have determined that more complex

quantitative analysis methods are unneeded. Regarding the descriptive data, it was clear that every participant consistently displayed unsafe privacy behavior in response to all questions, with an average score of 4.09. This implies, for instance, that privacy settings are infrequently or rarely altered, or that the participants exhibit a limited degree of privacy-aware conduct. The overall and individual question averages are presented in Table 4 of [Paper III](#). Regarding the implementation of the ANOVA, it is clear that the participants' responses to each question do not show a statistically significant difference ($F = 1.19$, $P\text{-value} = 0.31$, $p=0.5$), despite a high chance of being inaccurate. However, each individual exhibits a noticeable variation for each question ($F = 3.57 > F \text{ critical } 2.07$, $P\text{-Value} = 0.001$, $p = 0.05$). The results of the ANOVA analysis are displayed in Table 5 of [Paper III](#). Cronbach's analysis revealed a performance validity coefficient of 0.71961223 (table 6 of Paper III). The questionnaire replies are deemed sufficient and dependable, as evidenced in Tables 4-6 of [Paper III](#).

3.4 Behavioral transformation framework validity

Our proposed behavioral transformation framework comprises five phases, as illustrated in Figure 2 of [Paper III](#). Phase 1 involves the creation of a questionnaire that is used to evaluate the level of privacy behavior exhibited by individuals both before and after the adoption of frameworks. The validity of this phase is contingent upon two things. Firstly, the question was chosen based on a thorough examination of relevant literature on privacy behavior. Furthermore, each question in [Paper I](#) was associated with a minimum of one and a maximum of four privacy behavior determinant factors. In order to determine matching criteria, we employed the closest neighbor theory that was previously discussed in sections [1.3](#) and [3.3](#). Therefore, as stated in section 3.7 about the responses, we performed ANOVA and Cronbach's Alpha, both of which are widely accepted in academia for their validity. Ultimately, the performance validity coefficient of Cronbach's Alpha confirmed the legitimacy of the answers. The last also guarantees phase-2 validity (Phase-2 Questionnaire Completion). Based on the information provided, we conclude that the questionnaire is legitimate.

The legitimacy of Phase 3 (Environment Creation) has already been addressed in section 3.3. The technique is simple and relies on the technical measures we implemented.

Phase 4 - Experiment implementation consists of three sections. Phone surveillance, experiential methods, and phone re-monitoring. Both the initial and final elements are derived from the surveillance of actual data by autonomous applications, so we have confidence that there are no concerns regarding their validity to be scrutinized. Conversely, experiential approaches were founded upon two specific theories: the cognitive theory and the Health Belief Model (HBM), which are widely acknowledged for their academic value. In order to utilize them, we relied on established methods such as Cognitive Behavioral Therapy and Cognitive

Transformation (CBT), CBTx, practical evaluations, and motivational interviews (MI). By employing the aforementioned universally recognized theories and methodologies, we are confident that our approach is firmly grounded in providing not only an answer to **whether** it will be effective, but also an explanation as to **why** it was successful. Based on the information provided, we conclude that Phase-4 is likewise present and acknowledged for its authenticity.

Finally, Phase-5 (Results' Analysis) was a straightforward process. In addition to ANOVA, we utilized a paired T-test for each item to ascertain the statistical significance of the observed disparities. According to the results, we can infer that the self-reported privacy behavior of each participant has improved in almost all of the questions (Table 7 of [Paper III](#)). The T-tests we performed indicated that the p-values for each question were significantly below 0.05, suggesting a large and meaningful alteration in behavior. We are confident that the application of widely established scientific analysis methodologies confirms the validity of our approach and guarantees the substantial alteration of privacy behavior for each participant.

3.5 Research Ethics

This thesis relied on publicly available data and individuals' personal data, particularly during the validation phase of our transformation framework we proposed. We implemented rigorous safeguards to protect the anonymity of participants and both their personal data. Throughout the tests, all participants were explicitly notified that we implemented comprehensive procedures to safeguard their data against any potential breach. We explicitly notified them that we do not disclose any of their data to third parties. The personal data underwent anonymization, while any location data that could potentially reveal personal information, such as the street address on Google Maps, was intentionally masked. Exclusive access to the unprocessed data from the experiment was limited to the researchers involved in this investigation.

4. Summary of Work

This chapter provides a concise overview of the research conducted for this thesis. Table 4 presents a compilation of the articles that are included in this thesis, providing information such as the year of publication, the type of publication, the title, and the outlet where they were published. Each work is succinctly recounted, commencing with the research inquiry, proceeded by a concise overview, thorough examination, and a seamless transition to the subsequent published publication. The primary inquiry that this research sought to address was:

“How to Transform Individuals’ Privacy Behavior through Experiential Procedures”

In order to address the main research topic, each research paper inside this thesis was constructed with several research questions or objectives. Each contribution had a distinct objective aimed at providing a solid foundation for the study, while also progressing towards the subsequent phase of our project. The thesis comprises six research papers, which include both support papers and core papers:

- I. Paspatis, I., Tsohou, A., & Kokolakis, S. (2017). Mobile application privacy risks: Viber users’ de-anonymization using public data. <https://aisel.aisnet.org/mcis2017/32>
- II. Paspatis, I., Tsohou, A., & Kokolakis, S. (2018). AppAware: A Model for Privacy Policy Visualization for Mobile Applications. <https://aisel.aisnet.org/mcis2018/3>
- III. Paspatis, I., Tsohou, A., & Kokolakis, S. (2020). AppAware: a policy visualization model for mobile applications. Information & Computer Security, 28(1), 116-132. <https://doi.org/10.1108/ICS-04-2019-0049>
- IV. Paspatis, I., Tsohou, A., & Kokolakis, S. (2023). How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors. Multimodal Technologies and Interaction, 7(8), 76. <https://doi.org/10.3390/jcp3030020>
- V. Paspatis, I., & Tsohou, A. (2023). How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. Journal of Cybersecurity and Privacy, 3(3), 396-415. <https://doi.org/10.3390/mti7080076>
- VI. Paspatis, I., & Tsohou, A. (2024). Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement. Journal of Cybersecurity and Privacy. <https://doi.org/10.3390/jcp4010005>

Table 3. Articles published in Scientific Conferences and Journals

Paper	Year	Type	Title	Outlet
I	2017	Conference	Mobile application privacy risks: Viber users' de-anonymization using public data	Mediterranean Conference on Information Systems (MCIS 2017). https://aisel.aisnet.org/mcis2017/32
II	2018	Conference	AppAware: A Model for Privacy Policy Visualization for Mobile Applications	Mediterranean Conference on Information Systems (MCIS 2018). https://aisel.aisnet.org/mcis2018/3
III	2020	Journal	AppAware: a policy visualization model for mobile applications.	Information & Computer Security, 28(1), 116-132. https://doi.org/10.1108/ICS-04-2019-0049
IV	2023	Journal	How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors	Multimodal Technologies and Interaction, 7(8), 76. https://doi.org/10.3390/mti7080076
V	2023	Journal	How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors	Journal of Cybersecurity and Privacy, 3(3), 396-415. https://doi.org/10.3390/jcp3030020
VI	2024	Journal	Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement	Journal of Cybersecurity and Privacy 4(1):76-104. https://doi.org/10.3390/jcp4010005

4.1 Mobile application privacy risks: Viber users' de-anonymization using public data (Paper I)

The objective of this study was to demonstrate the ease with which one may ascertain the identity of unidentified Viber users. To be more precise, we generated a sample of 2000 cellular telephone numbers using a pseudorandom method and investigated the possibility of uncovering their personal information. We developed and applied a systematic approach to analyze Viber's database (below figure 1), enabling us to accurately identify 85% of the pseudorandom dataset we generated. We conducted an empirical study that examines the correlation between the activity reported by Viber's users and their real behavior. The findings of this study indicate that users' anonymity and privacy can be easily compromised, resulting in the exposure of their information to others with expertise in the field. We offer comprehensive guidelines aimed at enhancing privacy awareness and mitigating privacy infringements for both mobile application users and developers. Furthermore, we administered an empirical questionnaire to users of Viber in this study. The empirical questionnaire yielded results indicating a lack of privacy awareness among Viber users. Furthermore, our empirical investigation revealed the alarming privacy practices adopted by Viber users, which persist even after being presented with the survey's findings. It demonstrated how effortlessly an educated individual may get their personal information, including their real identity, and in certain instances, their residential or workplace details.

Abstract: Mobile application developers define the terms of use for the applications they develop, which users may accept or decline during installation. Application developers on the one hand seek to gain access to as many users' information as possible, while users on the other hand seem to lack awareness and comprehension of privacy policies. This allows application developers to store an enormous number of personal data, sometimes even irrelevant to the application's function. It's also common that users choose not to alter the default settings, even when such an option is provided. In combination, the above conditions jeopardize users' rights to privacy. In this research, we examined the Viber application to demonstrate how effortless it is to discover the identity of unknown Viber users. We chose a pseudorandom sample of 2000 cellular telephone numbers and examined if we could reveal their personal information. We designed an empirical study that compares the reported behavior with the actual behavior of Viber's users. The results of this study show that users' anonymity and privacy is easily deprived and information is exposed to a knowledgeable seeker. We provide guidelines addressed to both mobile application users and developers to increase privacy awareness and prevent privacy violations.

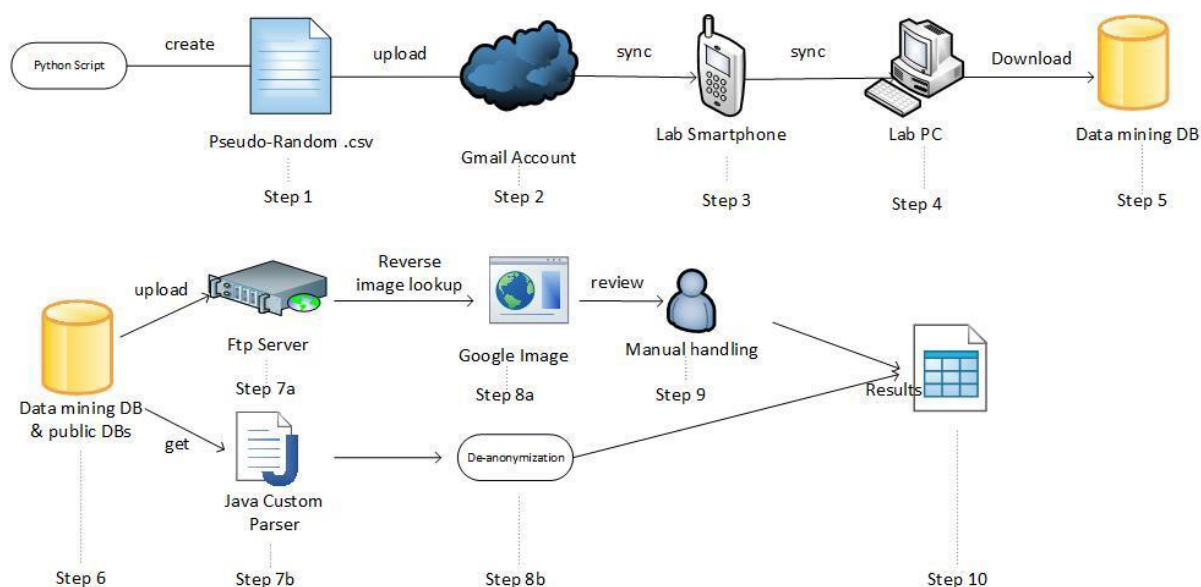


Figure 1. Viber's information extraction methodology.

Synthesis and bridge to the following paper: One of the findings of this study was that the vast majority of the respondents in the questionnaire admitted to not reading the privacy policy of the Viber App. The findings of this study prompted us to investigate the factors behind the failure of the mentioned participants to read the privacy policy, which explicitly stated that their personal data will be shared with third-party firms. Furthermore, it was disclosed that they were unaware that their personal data is classified as public data once they make it accessible to the public, even if through indirect means.

4.2 AppAware: A Model for Privacy Policy Visualization for Mobile Applications (Paper II).

Summary: AppAware is a versatile solution created to enhance the presentation of privacy rules for mobile applications across different platforms. It generates an aesthetically pleasing report that incorporates the authorization settings of an application, facilitating comprehension and acceptance of privacy policies by users. The approach addresses the challenge of comprehending privacy policies and Android's intricate permission system. AppAware receives above-average ratings from users in all categories, giving it a more effective and precise method for presenting privacy policies. This strategy does not necessitate any extra efforts from mobile app developers and operates in both a proactive and reactive

manner. It assists users in comprehending any risks they may face when agreeing to the terms and conditions of a specific mobile app. We conducted an empirical study to assess the utility and effectiveness of AppAware. The results indicated that Android users have a preference for viewing AppAware's graphical privacy policy over the conventional policy provided by each application's vendor. The study revealed an unforeseen result that aligns with the findings of paper 1, indicating that app users exhibit a deficiency in their understanding of privacy and engage in risky behavior, likely stemming from this lack of privacy awareness. Furthermore, it has been demonstrated that visualization techniques can be a helpful resource in enhancing app users' knowledge of privacy.

Abstract: Privacy policies emerge as the main mechanism to inform users on the way their information is managed by online service providers, and still remain the dominant approach for this purpose. Literature notes that users find difficulties in understanding privacy policies because they are usually written in technical or legal language even, although most users are unfamiliar with them. These difficulties have led most users to skip reading privacy policies and blindly accept them. In an effort to address this challenge this paper presents AppWare, a multiplatform tool that intends to improve the visualization of privacy policies for mobile applications. AppWare formulates a visualized report with the permission set of an application, which is easily understandable by a common user. AppWare aims to bridge the difficulty to read privacy policies and android's obscure permission set with a new privacy policy visualization model. To validate AppAware we conducted a survey through questionnaire aiming to evaluate AppAware in terms of installability, usability, and viability-purpose. The results demonstrate that AppAware is assessed above average by the users in all categories.

Synthesis and bridge to the following papers 3 and 4: The results of this study validated three assertions. Firstly, app users generally lack awareness of concerns related to privacy. Secondly, visualizing complex information can help them better understand the complex language used in privacy policies and demonstrate the potential dangers they may face. Most importantly, these users exhibit risky privacy behavior. These findings prompted us to enhance AppAware (paper 3) by incorporating additional functionalities. Moreover, they compelled us to shift our focus from computer science to comprehending and enhancing consumers' privacy behavior, with an emphasis on adopting more protective measures.

4.3 AppAware: A policy visualization model for mobile applications (Paper III - extend of paper II).

Summary: In order to further augment the capabilities of AppAware, we suggest the development of an additional application known as AppAware Parser. The underlying philosophy of AppAware Parser can be summarized in the following key points: i) the AppAware Parser examines the installed applications on a specific mobile device and generates a report listing those applications, ii) upon obtaining the mobile device user's consent, the list can be submitted to AppAware's worldwide database, iii) AppAware Parser generates a mobile-friendly visual privacy report for each application in AppAware's database, iv) it notifies the user of the mobile device about the permissions acquired by each installed application and the potential risks that the user may encounter. and finally, v) notifies the mobile device user regarding programs that are absent from the AppAware's comprehensive worldwide database. Once the initial inspection of the installed programs on a certain mobile device is completed, AppAware Parser will continue to operate in the background, monitoring the manifest.xml file of each application. If there are any modifications, the AppAware Parser will notify the user and suggest generating a fresh graphical privacy report. Additionally, when a new program is installed, the AppAware parser will suggest creating a graphical privacy report for that application. At present, the AppAware Parser remains in the conceptual stage of development. Our objective is to implement it in the future and assess its efficacy in enhancing user awareness of privacy.

Abstract: Purpose: Privacy policies emerge as the main mechanism to inform users on the way their information is managed by online service providers, and still remain the dominant approach for this purpose. Literature notes that users find difficulties in understanding privacy policies because they are usually written in technical or legal language even, although most users are unfamiliar with them. These difficulties have led most users to skip reading privacy policies and blindly accept them. In an effort to address this challenge this paper presents AppAware, a multiplatform tool that intends to improve the visualization of privacy policies for mobile applications. Design: AppAware formulates a visualized report with the permission set of an application, which is easily understandable by a common user. AppAware aims to bridge the difficulty to read privacy policies and android's obscure permission set with a new privacy policy visualization model. Thus, we propose AppAware Parser, a mobile add-on that acts complementary with AppAware and helps mobile devices users to monitor the applications they installed to their smart device. Findings: To validate AppAware we conducted a survey through questionnaire aiming to evaluate AppAware in terms of installability, usability, and viability-purpose. The results demonstrate that AppAware is assessed above average by the

users in all categories. Originality: In the best of our knowledge, there is no such approach as AppAware as an application nor AppAware parser as add-on.

Synthesis and bridge to the following paper: As previously stated in the last two papers, the individuals exhibit a deficiency in their understanding of privacy. This appears to compel them to exhibit a precarious privacy conduct. This activity could expose them to different possible hazards, such as becoming a victim of theft or impersonation. In order to tackle this issue, we redirected our academic focus towards investigating the factors that can influence individuals' privacy behavior, with the potential to induce a shift towards a more safeguarding approach.

4.4 How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors (Paper IV).

Research Question:

What factors have been found to influence ICT users' privacy behavior?

Summary: This study investigated the determinants that affect the privacy-related actions of individuals who use Information Communications and Technology (ICT). Our investigation of this behavior was primarily motivated by users' professed concern for their personal data, but frequently engaging in risky behaviors, such as neglecting to configure privacy settings. The study sought to examine the fundamental elements that impact privacy-conscious behavior in the digital realm and provide effective treatments to encourage such conduct. We presented the pertinent literature which established that privacy decisions can result in adverse outcomes, such as identity theft and impersonation. Furthermore, we have shown that, in accordance with the existing literature, third parties might potentially utilize this information for their own advantage, specifically through targeted advertising methods. The research discovered multiple elements that influence privacy behavior, such as individual aspects like demographics and environmental factors like financial transactions, as illustrated in Figure 2 and at the same time answering the research question we set: “*What factors have been found to influence ICT users' privacy behavior?*”. We also asserted that a conceptual framework that consolidates and integrates these aspects can be advantageous to scholars and professionals in both the private and public domains. The results can be utilized to develop specific courses on information privacy, encompassing both theoretical and practical

components. To the best of our knowledge, this was the first study that conclude the majority of factors that can influence individuals' privacy behavior.

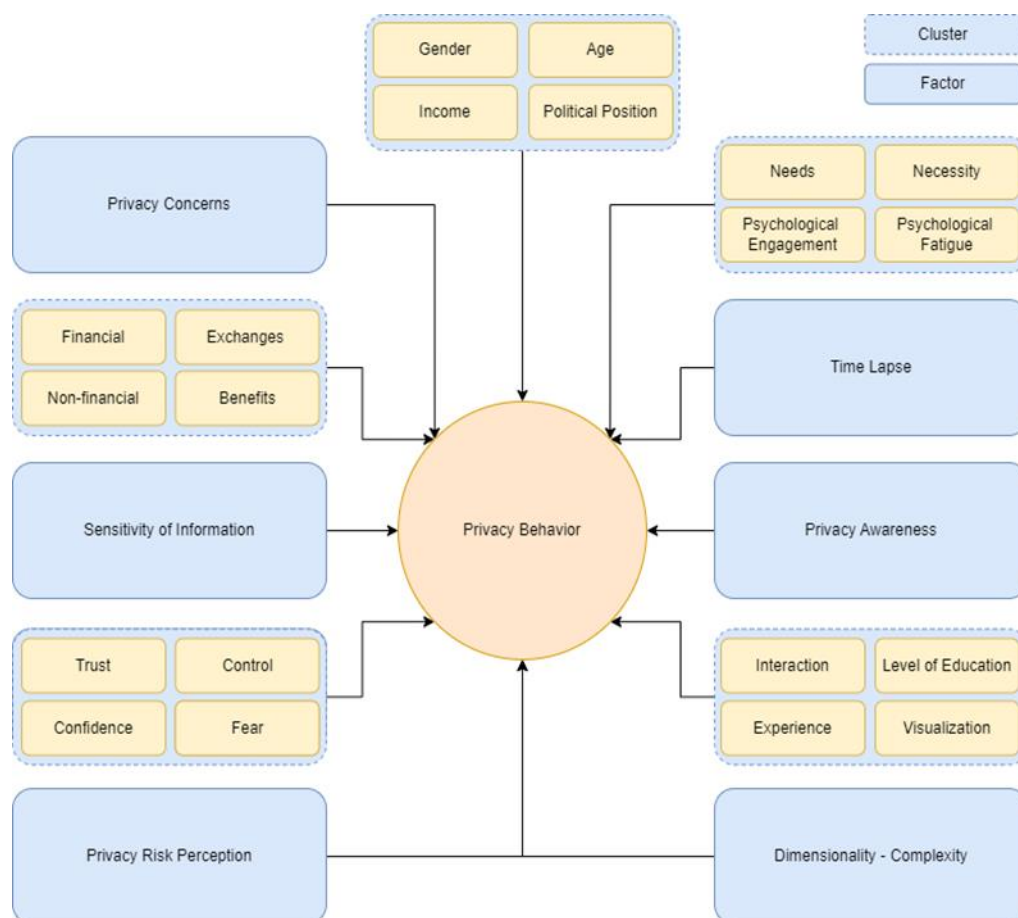


Figure 2. Conceptual scheme.

Abstract: What influences Information Communications and Technology (ICT) users' privacy behavior? Several studies have shown that users state to care about their personal data. Contrary to that though, they perform unsafe privacy actions, such as ignoring to configure privacy settings. In this research, we present the results of an in-depth literature review on the factors affecting privacy behavior. We seek to investigate the underlying factors that influence individuals' privacy-conscious behavior in the digital domain, as well as effective interventions to promote such behavior. Privacy decisions regarding the disclosure of personal information may have negative consequences on individuals' lives, such as becoming a victim of identity theft, impersonation, etc. Moreover, third parties may exploit this information for their own benefit, such as targeted advertising practices. By identifying the factors that may affect SNS users' privacy awareness, we can assist in creating methods for effective privacy protection and/or user-centered design. Examining the results of several research studies, we found evidence that privacy behavior is affected by a variety of factors, including individual ones (e.g., demographics) and contextual ones (e.g., financial exchanges). We synthesize a

framework that aggregates the scattered factors that have been found in the literature to affect privacy behavior. Our framework can be beneficial to academics and practitioners in the private and public sectors. For example, academics can utilize our findings to create specialized information privacy courses and theoretical or laboratory modules.

Synthesis and bridge to the following paper: This study addressed the research inquiry of the factors that have been identified as influencing the privacy behavior of ICT users. With this answer in our possession, we can now begin contemplating strategies for leveraging these crucial determinants of privacy behavior. These findings compelled us to go into the literature of several scientific disciplines in order to identify theories that can exert an influence on behavior and understand the mechanisms behind it.

4.5 How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors (Paper V).

Research Question 1:

What empirical methods and practices have been followed in other fields, such as philosophy or psychology, to influence human behavior via experiential techniques and could be used in the field of information privacy towards enabling privacy-protective behaviors?

Research Question 2:

How can we influence privacy behavior determinant factors to guide ICT users' privacy behaviors using experiential methods?

Summary: In this research we demonstrated that the conventional method of learning is suboptimal when our goal is to change the actual privacy behaviors of individuals. In this study we provided a comprehensive examination of the theories employed in several disciplines to alter human behavior through a literature survey. The findings of our study indicated that cognitive theory and its extension the health belief model yield positive outcomes. Our analysis of different learning approaches determined that experiential learning offers distinct advantages when compared to alternative ways. This research aimed to consolidate the components that determine privacy behavior as identified in our previous research. Additionally, we employed cognitive theory to provide a comprehensive theoretical framework. To create this framework, we had to match the privacy behavior determinant factors with the HBM influential axes as it is presented to the following figure 3. To match the

mentioned factors, we used the nearest neighbor theory. By these results both of our research questions we set answered.

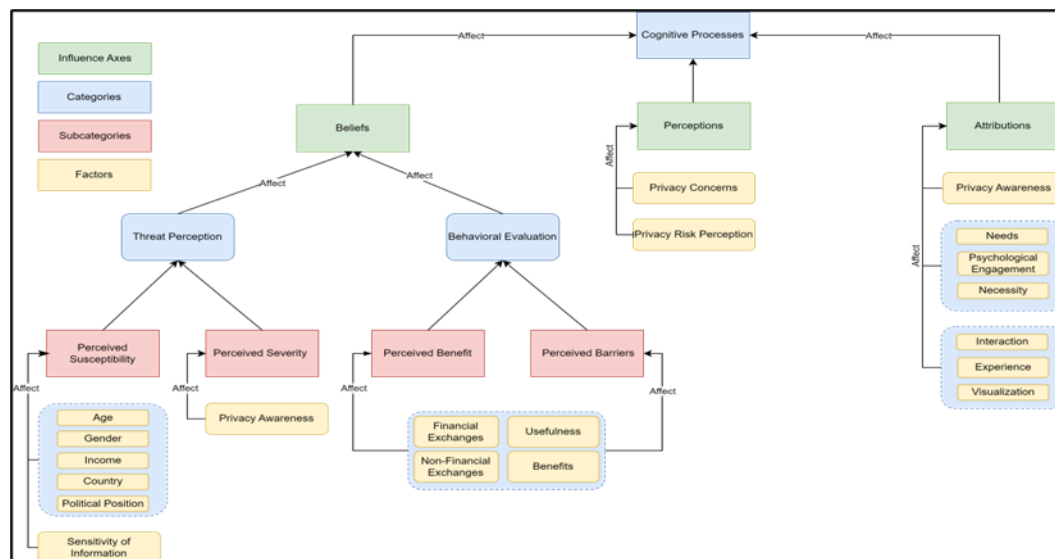


Figure 3. Cognitive theory with adapted privacy behavior factors.

Abstract: Several studies have shown that the traditional way of learning is not optimal when we aim to improve ICT users' actual privacy behaviors. In this research, we present a literature review of the theories that are followed in other fields to modify human behavior. Our findings show that cognitive theory and the health belief model present optimistic results. Further, we examined various learning methods, and we concluded that experiential learning is advantageous compared to other methods. In this paper, we aggregate the privacy behavior determinant factors found in the literature and use cognitive theory to synthesize a theoretical framework. The proposed framework can be beneficial to educational policymakers and practitioners in institutions such as public and private schools and universities. Also, our framework provides a fertile ground for more research on experiential privacy learning and privacy behavior enhancement.

Synthesis and bridge to the final paper: In aim to apply the results of the preceding study, we identified theories that have the potential to effectively impact behavior, as well as ways that can be employed to apply these ideas. By including the cognitive theory and the Health Belief Model (HBM) into the analysis of privacy behavior determinant elements, we have identified that experiential approaches can successfully leverage these theories. Consequently, our focus now shifts towards discovering strategies that can be employed to modify individuals' behavior. Consequently, we embarked on further research to identify effective methodologies employed in several scientific fields.

4.6 Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement (Paper VI).

Research Question 1:

Can an individual's privacy behavior be transformed through experiential methods?

Research Question 2:

Which experience method is more effective in transforming an individual's privacy behavior?

Summary: Based on our previous research depicted several studies have shown that the traditional approach to learning is not ideal when our objective is to improve individuals' authentic privacy behavior. This study presented a novel framework for transforming privacy behavior in order to improve individuals' privacy practices and achieve a higher level of secrecy. We conducted an experiment on a restricted sample size to authenticate the effectiveness of our proposed transformation framework. This approach is based on the following elements: Privacy behavior is influenced by multiple factors, as indicated in our paper 4. Furthermore, we established a solid basis for investigating the potential impact of privacy behavior determining factors by aligning them with the cognitive theory and its extension, the HBM influential axes, as demonstrated in our paper 5. In this study, we conducted a literature analysis to investigate the effectiveness of applying the aforementioned theories in transforming individuals' privacy behavior. The objective was to gain a deeper understanding of why these theories are used and how they can successfully influence behavior. The integration of privacy behavior analysis with experiential behavior changes approaches, such as neutral stimuli (e.g. Cognitive Behavioral Transformation - CBTx), practical assessments, and motivational interviews from different scientific domains, resulted in our proposed framework. While these tactics have proven effective in fields like psychology and sociology, they have not yet been applied in the realm of ICT. We have successfully showcased the effectiveness of the proposed framework by conducting a comprehensive five-phase experiment in this study as figure 4 presents.

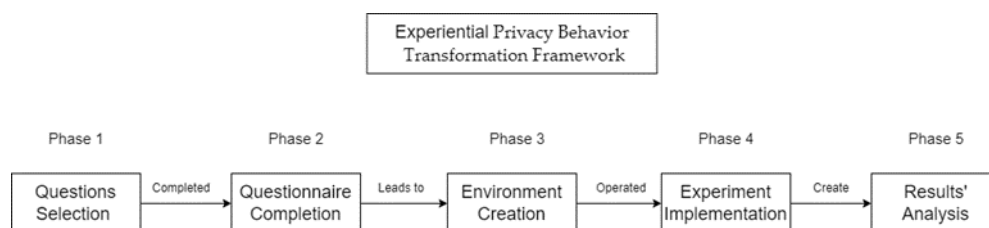


Figure 4. Capture of experimental phases

The proposed framework offers potential benefits for educational institutions, encompassing both public and private schools, as well as universities, to establish new frameworks or devise new approaches for promoting individuals' transition towards a more secure approach to privacy behavior. Moreover, our framework provides a favorable setting for further exploration of methodologies for transforming privacy behavior. Our framework answers the following two important aspects; Not only did it illustrate its functionality, but more importantly, it elucidated the underlying reasons for its effectiveness. We offered definitive responses grounded in robust principles. Our approach utilizes standard methods such as Cognitive Behavioral Therapy and Transformation (CBT, CBTx), Motivational Interviewing (MI), and practical assessments. These methodologies are grounded in well-regarded theories from different fields, including Cognitive Theory and the Health Belief Model (HBM). The analysis of our framework confirmed that the neutral stimuli methodology outperforms MI and practical assessments in terms of privacy behavioral modifications, in that specific order. From all of the above both of our research questions answered. To the very best of our knowledge, this framework is the first to be proven for its effectiveness in transforming privacy behavior, while also providing an explanation for the mechanisms behind its ability to bring about behavioral change.

Abstract: Multiple researches have demonstrated that the conventional method of learning is suboptimal when our goal is to enhance individuals' genuine privacy behavior. This study introduces a framework for transforming privacy behavior, with the objective of enhancing individuals' privacy practices to a higher level of confidentiality. We performed an experiment on a limited number of persons to validate the efficacy of our suggested transformation framework. This framework combined determining aspects of privacy behavior with experiential behavior modification methodologies such as neutral stimuli (e.g. Cognitive Behavioral Transformation - CBTx), practical assessments and motivational interviews from other disciplines. While these methods have proven effective in fields like psychology and sociology, they have not yet been applied to the realm of Information Computer and Technology (ICT). In this study, we have effectively demonstrated the efficacy of the proposed framework through a five-phase experiment. The suggested framework has the potential to be advantageous for educational institutions, including both public and private schools as well as universities to construct new frameworks or develop new methodologies regarding individuals' privacy behavior transformation to a more protective one. Furthermore, our framework offers a conducive environment for further investigation into privacy behavior transformation methodologies.

5. Conclusion and Contributions

5.1 Contributions

This thesis contributes to the literature and practice by addressing the necessity to strengthen individuals' privacy behavior and promote a more protective approach. Currently, information privacy behavior is risky given that for example, many unknowingly disclose their personal information on social media, without realizing that once they post it, this data is no longer deemed private but rather public. Individuals' personal data can be inadvertently disclosed, for instance, through Internet of Things (IoT) devices or background operations on mobile devices, often unbeknownst to them. Individuals' privacy risky behavior was a challenge for us. Our primary objective was to comprehend the aforementioned phenomenon and identify the factors that impact it. Further, we explored theories that have been employed to shape behavior from other scientific disciplines' literature. We considered that the Cognitive theory and its extension, the Health Belief Model (HBM), were promising candidates for application in our domain of expertise. We combined the factors that determine privacy behavior from Paper I with the Health Belief Model (HBM) from Paper II. This effort enhanced our comprehension of how various factors impact privacy behavior in a comprehensive manner. According to the literature, the most effective way to apply the aforementioned theories is through experiential approaches, as indicated in Paper II. We conducted a thorough investigation to identify the experiential techniques employed in various scientific disciplines. Through this analysis, we discovered three primary experiential techniques: the use of neutral stimuli in conjunction with Cognitive Behavior Therapy/Transformation (CBT/CBTx) methods, practical assessments, and motivational interviews (MI) (Paper III). We employed the aforementioned three techniques to develop a framework named Privacy Behavior Transformation Framework (PBTF). We assessed and validated the effectiveness of our framework through an empirical study including nine participants. The results of our empirical investigation demonstrated that PBTF effectively altered the declared and actual privacy behavior of all participants. Furthermore, our empirical investigation revealed that the participants predominantly favored neutral stimuli as a method after undergoing the motivational interview technique and practical assessments.

Contributions in four key areas can be identified:

1. This thesis contributed to the identification of the 22 factors that determine privacy behavior. We classified these factors into 11 clusters based on their similarity, with each cluster having one or more components. To the best of our knowledge, this is the first study that examined and aggregated the factors that determine privacy behavior.

The results of our research can be applied by academic institutions, professionals, and businesses to develop educational materials, software, and other tools that encourage individuals to adopt more protective privacy practices. Additionally, it paves the way for new and promising avenues of research in academia aimed at gaining a deeper comprehension of individuals' activities around privacy behavior.

2. This thesis integrated the factors that determine privacy behavior with the cognitive theory and the Health Belief Model (HBM). Despite the long-standing existence of these theories, they have not been applied to the realm of privacy behavior. Through this research, we have offered robust theories for examining individuals' privacy behavior and constructing frameworks or approaches that make use of these theories. Furthermore, it offered a novel avenue of investigation to enhance comprehension of individuals' propensity for engaging in risky behavior with regards to their personal data and actions.
3. By utilizing experiential techniques from other scientific disciplines to the field of ICT, new research possibilities and insights can be generated by effectively transforming privacy behavior. The majority of education programs in the field of ICT has relied on traditional teaching methods, spanning from elementary schools to universities and academic institutions. In this thesis, we presented experiential methodologies that have the potential to revolutionize the learning experience for students at any academic level, offering a more effective and distinct approach. Our findings not only offered efficient experiential techniques within our domain but also elucidated the underlying reasons for their effectiveness, as outlined in the following sequence:

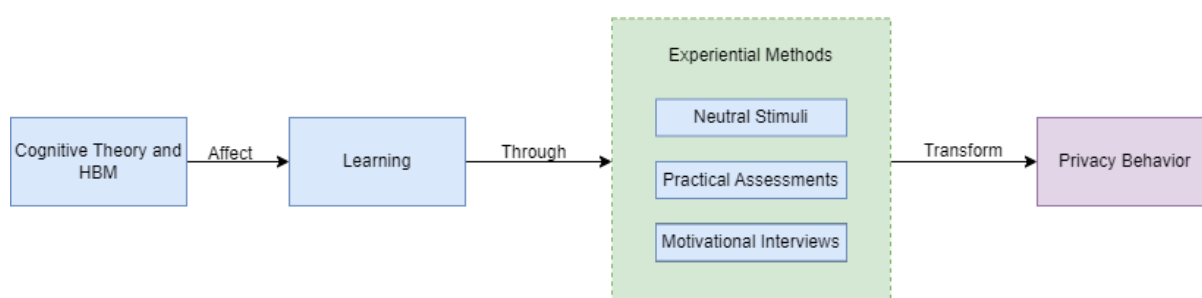


Figure 5. From Theory to Behavior

Our thesis examined the aforementioned theories and approaches in relation to privacy behavior. However, our framework may also have advantages for other research topics, such as security behavior, privacy risk behavior, and others.

4. The main focus of this thesis is to offer a Privacy Behavior Transformation Framework (PBTF). The PBTF was developed on a solid foundation derived from the determinant factors influencing privacy behavior as identified by the literature. These factors were incorporated into the well-established cognitive theory and HBM. Furthermore, we applied these theories by employing the three most esteemed techniques for experiential behavior transformation. We validated the efficiency of PBTF using a five-phase empirical investigation. The results of our investigation indicate that our framework is established and has effectively influenced the privacy behavior of the participants in the empirical study. Our methodology not only addresses the topic of **whether** and **how** it can modify individuals' privacy behavior, but also provides insights into the **underlying reasons** for this behavioral transformation.

5.2 Implications

Several implications may emerge from our research findings and results as follow:

- Paper I demonstrated that privacy behavior is influenced by multiple determinant factors. The conceptual framework we presented combines and incorporates these factors and can be beneficial to academics and practitioners in both the private and public sectors. The findings can be employed to create specialized curricula on information privacy, incorporating both theoretical and practical elements. To our understanding, this study is the first to aggregate under a single framework the majority of factors that potentially impact individuals' privacy behavior.
- The findings of Paper II indicated that the combination of cognitive theory and the Health Belief Model (HBM) yield positive effects in influencing behavior, particularly when used in conjunction with experiential learning methods. We developed a conceptual framework that combines the aspects that determine privacy behavior with the theories presented before. The suggested framework holds potential advantages for educational policymakers and practitioners in many institutions, including both public and private schools as well as universities. Furthermore, our framework offers a conducive environment for further investigation into experiential privacy learning and the improvement of privacy behavior.

- The results of Paper III can provide a strong foundation for transforming privacy behavior. This approach has the potential to benefit the academic community by enabling the acquisition of privacy behavior transformation from an early age and the learning results to persist after learners have finished their educational journey. The framework we have developed can be employed by elementary schools, academic institutes, and private schools to improve students' compliance with protective privacy measures. Moreover, it has the capacity to shift the attention of privacy researchers towards new areas of study.

5.3 Limitations and Future Work

The below limitations were faced during our research. The realm of privacy behavior is always evolving, and further modifications are inevitable. In our study described in Paper I, we made significant contributions by identifying 22 factors that determine privacy behavior. Furthermore, we successfully classified these factors into 11 distinct clusters. Although our research extensively delved into the literature, we cannot guarantee that we have exhaustively included all criteria or accounted for potential future additions. We consider that the determinants of privacy behavior are an ongoing exploration in the realm of privacy behavior. This study aggregated determinants factors for information privacy that had been identified by previous studies, which relied on various theories. Although we validated the proposed privacy behavior transformation framework, we did not assess the influence of each determinant factor or their interplay. For instance, individuals may exhibit distinct behavior when utilizing their preferred OSN on a mobile device versus a desktop computer. Further, the experimental study was conducted with limited resources and among a small sample of participants. Our goal is to identify any potential improvements for our framework and then refine.

Future works can focus on conducting further evaluation of our framework with a larger sample size, as well as investigating enhanced strategies to encourage individuals to prioritize privacy while minimizing our interference. This entails exploring other approaches to phone surveillance than the ones that we utilized, opting for a strategy that is less invasive of privacy. In our forthcoming research endeavors, our objective will be to undertake quantitative empirical investigations involving larger sample of participants to investigate this. Further, we will assess the efficacy of various experiential methods and their respective procedures by employing diverse groups and control groups for each approach.

Finally, we aim to develop two initiatives for the foreseeable future. The primary objective of our initial project is to construct our framework across three distinct platforms. We aim to produce a client-server application using the Java programming language, a mobile application using the React Native Language, and a web application using the React programming language. The material utilized in all three applications will be consistent with the material supplied in section 3. The primary objective of our second project is to develop an application that serves as a complementary tool to risk analysis applications, with a specific emphasis on presenting the outcomes of a risk assessment. In accordance with Paper V, our program will retrieve the outcomes of the aforementioned risk assessment and generate visual reports. Subsequently, our application will propose an instructional strategy for transform privacy behavior via PBTF for those who may be associated with the risk assessment through any methods.

6. References

1. Abraham, C.; Sheeran, P. The Health Belief Model in Conner and Norman, Predicting Health Behaviour. Research and Practice with Social Cognition Models; Open University Press: Buckingham, UK, 1995; p. 23-61.
2. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
3. Acquisti, A.; Grossklags, J. Privacy and rationality in individual decision making. *IEEE Secur. Priv.* 2005, 3, 26–33.
4. Association for Information Systems. Senior Scholars' of Journals. Available online: <https://aisnet.org/page/SeniorScholarBasket?&hhsearchterms=%22basket%22> (accessed on 10 June 2022).
5. Brown, R.; Brown L. The Nicomachean Ethics. Oxford; Oxford University Press: New York, NY, USA, 2009.
6. Conner, M.; Norman, P. Predicting Health Behaviour. Research and Practice with Social Cognition Models; Open University Press: Buckingham, UK, 1996; pp. 1–22.

7. Conner, M; Norman P (1993). Pros and cons of social cognition models in health behaviour, in *Health Psychology. Update Volume 14*, pages 24-31, 1993, https://fhs.thums.ac.ir/sites/fhs/files/user31/P_R_E_D_I_C_T_I_N_G.pdf (accessed on 30 May 2023).
8. COPE Core practices. Available at: <https://publicationethics.org/core-practices> (Accessed on 23 January 2024).
9. Cranor, L., Guduru, P. and Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction*, [online] 13(2), pp.135-178. Available at: <http://lorrie.cranor.org/pubs/privacy-bird-20050714.pdf> [Accessed 21 Jan. 2017].
10. Dacou, E. Educational Biography influences and determines the career path of adults. The case of educational institutions. Hellenic Open University. 2018. Available online: <https://apothesis.eap.gr/handle/repo/39397> (accessed on 29 January 2020).
11. Debatin, B., Lovejoy, J., Horn, A. and Hughes, B. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, [online] 15(1), pp.83-108. Available at: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2009.01494.x/full> [Accessed 21 Jan. 2017].
12. Dewey, J. *Experience and Education*; Macmillan: New York, NY, USA, 1938.
13. Dhir, A.; Kaur, P.; Lonka, K.; Nieminen, M. Why do adolescents untag photos on Facebook? *Comput. Hum. Behav.* 2016, 55, 1106–1115, ISSN 0747-5632, <https://doi.org/10.1016/j.chb.2015.11.017>.
14. Dwyer, C. (2007). Digital Relationships in the "MySpace" Generation: Results From a Qualitative Study. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). [online] Available at: <http://csis.pace.edu/dwyer/research/DwyerHICSS2007.pdf> [Accessed 21 Jan. 2017].
15. ENISA (2010). The new users' guide: How to raise information security awareness. Available at : https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide [Accessed 10 Oct. 2017]
16. Freire, P. *Teachers as Cultural Workers—Letters to Those Who Dare to Teach*; Boulder, Westview Press, 100 pp., ISBN 0 8133. 2304-5 1998.
17. Futuretimes, 2020. Global average Internet speed, 1990-2050. Available at: <https://futuretimeline.net/data-trends/2050-future-internet-speed-predictions.htm> . Accessed on [17-01-2024].
18. GDPR (2016). Κανονισμός Ευρωπαϊκής Ένωσης 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. [online] Available at: <https://eur-lex.europa.eu/legal-content/el/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

19. Gerber, N.; Gerber, P.; Volkamer, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Comput. Secur.* 2018, 77, 226–261.
20. Govani T., Pashley H. (2007). Student Awareness of the Privacy Implications while Using Facebook. Unpublished manuscript, 2007. [online] Available at :<http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf> . [Accessed 25 Jun. 2017].
21. Hallam, C.; Zanella, G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput. Hum. Behav.* 2017, 68, 217–227.
22. Hinds, J.; Williams, E.; Joinson, A. “It wouldn’t happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *Int. J. Hum. Comput. Stud.* 2020, 143, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>.
23. Holmes, C.C.; Adams, N.M. Likelihood Inference in Nearest-Neighbour Classification Models. *Biometrika* 2003, 90, 99–112. <https://doi.org/10.2307/30042022> .
24. Jarvis, P. *Adult Education & Lifelong Learning*; RoutledgeFalmer: London, UK, 2004.
25. Kokko, A. *Adult Education Methodology: Theoretical Framework and Learning Conditions*. Volume A. Patras: EAP. 2005.
26. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* 2017, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>.
27. Kolb, D.A. *Experiential Learning: Experience as the Source of Learning and Development*. Pearson Education LTD. United States of America. ISBN-10: 0-13-389240-9; 1984.
28. Li, H.; Luo, X.; Zhang, J.; Xu, H. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Inf. Manag.* 2017, 54, 1012–1022.
29. Mathews-Hunt, K. CookieConsumer: Tracking online behavioural advertising in Australia. *Comput. Law Secur. Rev.* 2016, 32, 55–90.
30. Menard, P.; Bott, G. Analyzing IOT users’ mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Comput. Secur.* 2020, 95, 101856.
31. Mezirow, J. Transformative learning and social action: A response to Inglis. *Adult Educ. Q.* 1998, 49, 70–72. American association for adult and continuing education: Sage publications.
32. Mezirow, J. On critical reflection. *Adult Educ. Q.* 1998b, 48, 185–198. American association for adult and continuing education: Sage publications.
33. Mezirow, J. *Transformative Dimensions of Adult Learning*; Jossey-Bass: San Fransisco, CA, USA, 1991.
34. Mezirow, J. *Transformative learning*. Metaichmio Publications, Vol.1 ISBN: 978-960-455-226-9.2006..

-
35. Palos-Sancheza, P.; Saurab, J.R.; Martin-Veliciaa, F. A study of the effects of programmatic advertising on users' concerns about privacy overtime. *J. Bus. Res.* 2019, 96, 61–72.
 36. Rogers, A. *Adult education*. Metaichmio Publications, Vol. 1 ISBN: 978-960-566-840-2. 1999.
 37. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1), 93-114.
 38. Shane-Simpson, C.; Manago, A.; Gaggi, N.; Gillespie-Lynch, K. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Comput. Hum. Behav.* 2018, 86, 276–288,. <https://doi.org/10.1016/j.chb.2018.04.041>.
 39. Taylor, W.E. *The Theory and Practice of Transformative Learning: A Critical Re-View*. ERIC Clearinghouse on Adult, Career, and Vocational Education; The Ohio State University: Columbus, OH, USA, 1998.
 40. Tow W, Dell P, Venable J. (2008). Understanding information disclosure behaviour in Australian Facebook users. *J Inform Technol* 2008;25(2):126–36. [Online] Available at: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1004&context=acis2008> [Accessed 25 Jun. 2017]
 41. Tsohou, A., & Kosta, E. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. *Computer law & security review*, 33(4), 434-457.
 42. Tsohou, Aggeliki & Kosta, Eleni. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. *Computer Law & Security Review*. 10.1016/j.clsr.2017.03.027.
 43. Watson, J. B., & Rayner, R. (1920). Conditioned emotional reactions. *Journal of Experimental Psychology*, 3(1), 1-14. <https://doi.org/10.1037/h0069608>. Available at: <https://psycnet.apa.org/record/2006-01667-001> (Accessed on 8/9/2023).
 44. Weinman, J. *Health Psychology: Progress, Perspectives, and Prospects*, Current Developments in Health Psychology; Hard-wood Academic Publishers: London, UK, 1990; pp. 9–33.

Part 2 – Core Papers

Paper – I



Systematic Review

How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors

Ioannis Paspatis ^{1,*}, Aggeliki Tsohou ¹ and Spyros Kokolakis ²

Citation: Paspatis, I.; Tsohou, A.; Kokolakis, S. How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors. *Multimodal Technol. Interact.* **2023**, *7*, x. <https://doi.org/10.3390/xxxxx>

Academic Editor(s): Cristina Portalés Ricart

Received: 23 June 2023

Revised: 21 July 2023

Accepted: 26 July 2023

Published: date



Copyright: © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

¹ Department of Informatics, Ionian University, 49100 Corfu, Greece; atsohou@ionio.gr

² Department of Information and Communication Systems Engineering, University of Aegean; 83200 Samos, Greece; sak@aegean.gr

* Correspondence: ipaspatis@ionio.gr; Tel.: +30-26610-87760

Abstract: What influences Information Communications and Technology (ICT) users' privacy behavior? Several studies have shown that users state to care about their personal data. Contrary to that though, they perform unsafe privacy actions, such as ignoring to configure privacy settings. In this research, we present the results of an in-depth literature review on the factors affecting privacy behavior. We seek to investigate the underlying factors that influence individuals' privacy-conscious behavior in the digital domain, as well as effective interventions to promote such behavior. Privacy decisions regarding the disclosure of personal information may have negative consequences on individuals' lives, such as becoming a victim of identity theft, impersonation, etc. Moreover, third parties may exploit this information for their own benefit, such as targeted advertising practices. By identifying the factors that may affect SNS users' privacy awareness, we can assist in creating methods for effective privacy protection and/or user-centered design. Examining the results of several research studies, we found evidence that privacy behavior is affected by a variety of factors, including individual ones (e.g., demographics) and contextual ones (e.g., financial exchanges). We synthesize a framework that aggregates the scattered factors that have been found in the literature to affect privacy behavior. Our framework can be beneficial to academics and practitioners in the private and public sectors. For

example, academics can utilize our findings to create specialized information privacy courses and theoretical or laboratory modules.

Keywords: privacy behavior; determinant factors

1. Introduction

The academic community has demonstrated through various studies that internet users state to care about their personal data [1–4]. However, if this is true, it raises the question of why do they behave as if they are not interested in their protection? For example, they disclose vast amounts of personal information when using their preferred social network [5,6]). Some researchers have attempted to explain this contradiction using the term “the privacy paradox”, pointing out the difference between privacy attitude and actual privacy behavior. Other researchers aired behavioral and psychological factors behind users’ privacy behavior [1–4]. The term information privacy behavior refers to users’ actions with regard to the protection of one’s own privacy when using Information Communications and Technologies (ICTs), for example, as personal information disclosure, the application of controls to protect own personal data, or the configuration of privacy settings. Many researchers highlight that research in the domain of privacy behavior is challenging, mostly because it mainly relies on self-reported data from the participants in empirical investigations.

The “intrusion” of ICT in our lives and the growth of technology has put our life on the front scene of a global theater. We expose ourselves everywhere and all the time. We are continuously connected to the internet through smartphones. Our internet-connected wearables are constantly measuring our daily activities and health condition. We post our moments and thoughts on Online Social Networks or Social Network Sites (OSNs or SNS) while the Internet of Things (IoT) play a “smarter” role in our lives day by day [7]. Privacy awareness among SNS users is a fundamental aspect of privacy behavior, as it influences their decisions regarding the disclosure of personal information on social networks. Self-disclosure of information may have negative consequences on individuals’ lives, such as becoming a victim of identity theft, impersonation, etc. Moreover, third parties may exploit this information for their own benefit, such as targeted advertising practices [8,9] or affecting people’s voting opinion, as Cambridge Analytica’s scandal showed us [10]. By recognizing the reasons that can influence the privacy awareness of SNS users, we can contribute to the development of effective privacy protection strategies and/or user-centered design approaches. Our privacy behavior [4] may have a bigger effect than in the past as a result of greater opportunities for self-exposure on social media and the internet.

Based on the above, we argue that we need to understand how privacy behavior is formulated so as to assist policymakers to understand how users make privacy decisions and how to improve privacy behavior. There is a significant stream of work in this domain, but the academic

community has provided fragmented views about what influences privacy behavior. Several researchers identify factors that determine privacy behavior relying on the lenses of a specific theory (e.g., protection motivation theory). Despite the merits of the existing scattered views, the lack of a holistic framework that aggregates those findings may prevent policy makers from taking action based on a holistic understanding of various factors that collectively affect privacy behavior. This research seeks to investigate the underlying factors that influence individuals' privacy-conscious behavior in the digital domain, as well as effective interventions to promote such behavior. Understanding how to influence human privacy-related behavior is crucial for a number of reasons. First, technological advancements cannot guarantee adequate privacy protection on their own, as the success of privacy measures ultimately depends on user behavior. Second, a significant number of privacy incidents can be attributed to individuals' lack of awareness, knowledge, or motivation to adopt privacy measures consciously.

This study can contribute to the development of strategies and interventions that may lead to enhanced privacy behavior by investigating how individuals' privacy behavior can be effectively influenced. This study examines theoretical frameworks, empirical studies, and interventions from the ICT field and other related disciplines in order to address this research gap. Our research seeks to shed light on the factors influencing privacy behavior, identify how privacy behavior is formulated, and provide actionable recommendations for ICT users, service providers, and policymakers by drawing on these interdisciplinary perspectives. To fill this gap, in this paper, we conduct an in-depth literature review to bring together these works and the factors that they identify as determinants of ICT users' privacy behavior and actions. Our research question is:

RQ: What factors have been found to influence ICT users' privacy behavior?

We argue that providing a holistic framework that aggregates the factors that influence ICT users' privacy behavior can be beneficial for many stakeholders, such as ICT users, privacy and information systems researchers, Internet Service Providers (ISP), ICT specialists, Internet Security Operation Centers (SOCs or ISOCs) (The function of the security operations center (SOC) is to monitor, prevent, detect, investigate, and respond to cyber threats around the clock. Link: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/>). For example, an SOC can propose and create new frameworks and services that can affect or protect privacy behavior, and thus our findings can inform SOC's towards building those frameworks and services in a way that facilitates privacy practices. As another example, researchers could contribute to the educational curriculum(s) that promote(s) an enhancement of students' privacy behavior.

In conclusion, this research provides the following main contributions:

- A list of all identified in the literature determinant factors of ICT users' privacy behavior
- A framework that synthesizes and classifies the identified factors

- A fertile environment for future research to stimulate privacy-protective behavior
- Inter-disciplinary perspective and favorable environment for further research opportunities in the privacy behavior domain

After the introduction, the paper continues with the presentation of the literature review methodology. In Section 3, we present the findings of the literature review. In Section 4, we analyze the results of the previous section. In Section 5, we discuss our results and the possible implications of our findings. Finally, Section 6 concludes the paper and provides possible solutions and future research.

2. Literature Review Scope and Methodology

2.1. Sampling Methodology

For our literature research, we used the scientific search engines of the most recognized journals in the field of information systems, also known as a basket of eight, as well as recognized international journals included in the science citation index. The “basket of eight” is considered by the Association for Information Systems (AIS) [11] one of the most representative and influential journals in the field of Information Systems. We also included the journals that are published in the proceedings of international conferences and are recognized by the AIS. We used the keywords: Privacy behavior, privacy attitude, factors that affect privacy behavior, factors that affect privacy attitude. During the initial search for factors influencing privacy behavior, studies appeared that analyze the phenomenon of “privacy paradox”, so it was included as a search term in the literature review. Table 1 shows the journals that are contained in the “basket of eight” list, the journals and conferences that are associated with the AIS, and the number of articles of each journal or conference proceedings.

Table 1. Number of articles we chose per search source.

Source	Number of Articles
European Journal of Information Systems (EJIS)	55
Strategic Information Systems (Search in Science Direct)	58
MIS Quarterly (MISQ)	32
International Conference on Information Systems (ICIS)	14
Information Systems Research (ISR)	13
Americas Conference on Information Systems (AMCIS)	11
European Conference on Information Systems (ECIS)	9
Journal of the Association for Information Systems (JAIS)	12
Pacific Asia Conference on Information Systems (PACIS)	7
Journal of Information Management Systems	5

Recognized international journals with citation index	10
Total number of articles	226

2.2. Exclusion Criteria

Using the above sample methodology, we identified 945 papers. However, some of the resulting articles did not identify factors influencing privacy behavior, although they studied respective phenomena. Subsequently, we removed the studies that, although they matched the search criteria, did not focus on identifying factors that influence privacy behavior and they did not present respective results. Consequently, we excluded 648 papers because they did not specifically study our focus subject. Following this process, 297 papers remained that studied or identified specific factors that affect privacy behavior directly or indirectly. Finally, we also excluded 71 articles that studied factors that only indirectly affect privacy behavior, i.e., only factors that affect other factors that determine privacy behavior. As a result, 226 articles remained that were found to show immediate effects on privacy behavior. Figure 1 visualizes the sampling process.

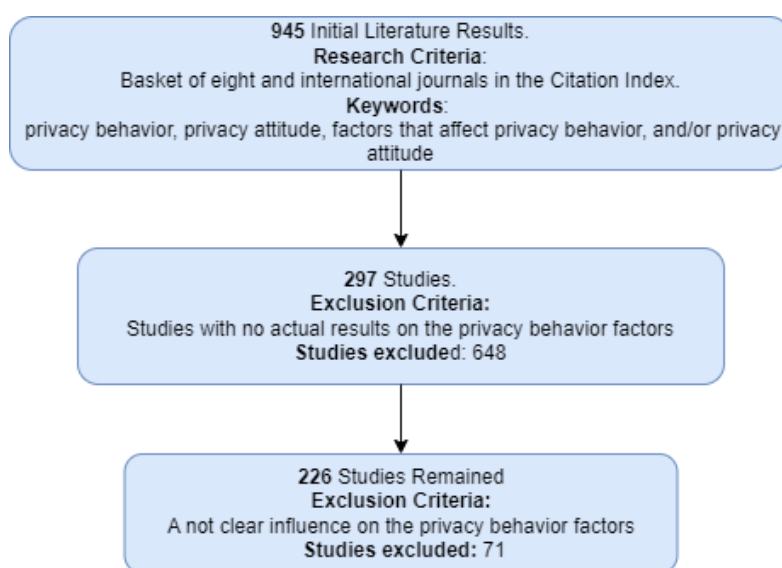


Figure 1. Literature sampling process and results.

Figure 2. shows the published articles by the year, and based on the results, we can notice an incremental trend per year, indicating an increased academic and research interest in the phenomenon.

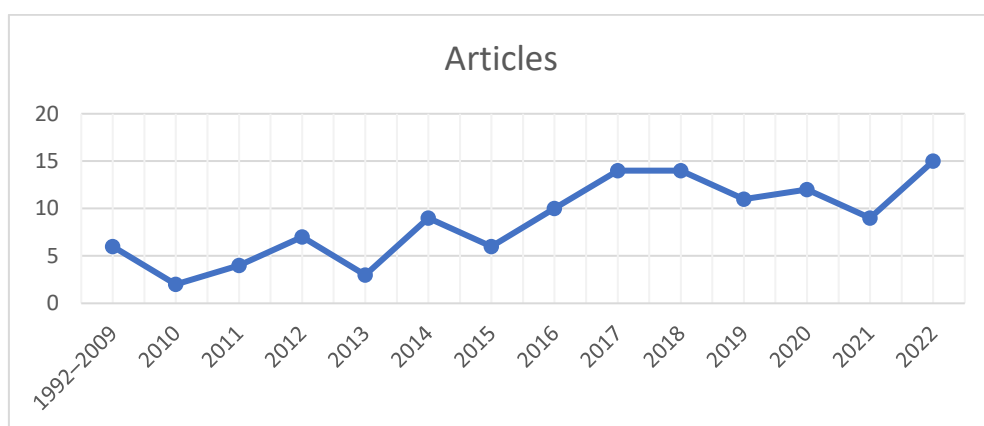


Figure 2. Number of articles published per year.

3. Factors That Affect ICT Users' Privacy Behavior

We studied each one of the papers selected using the methodology analyzed in Section 2, seeking the identification of factors that influence the privacy behavior of ICT users. Following this process, we identified eleven dominant factors. In studies that generally examine the factors that influence privacy behavior, the most prevailing factors are privacy concerns and the perception of risk. From the analysis of the current literature, the factors that most often appear in the literature to influence ICT users' privacy behavior are (Table 2). We have to mention that the studies were conducted with different criteria and methods. Some were conducted with qualitative methods and others with quantitative methods and different variables as input. We also have to mention that there is no scientific consensus on the definition of the term privacy behavior, and it depends on the view or the objective of the study.

Table 2. Number of Articles per Factor.

Factors	Number of Articles That Identify the Factor
Financial Exchanges/benefits/usefulness	31 articles
Privacy Risk Perception	27 articles
Trust/Control/confidence/fear	35 articles
Privacy Concerns	63 articles
"Needs" psychological engagement/necessity	16 articles
Sensitivity of information	3 articles
Privacy Awareness	21 articles
Time lapse	7 articles
Education/Visualization/Interaction/ Experience	19 articles
Demographics (age/gender/country, political position, income, etc.)	24 articles

Dimensionality/Complexity of a privacy decision making

10 articles

In some cases, we categorized the above factors into broader clusters depending on how much they have in common. For example, gender, age, income, and political position have been categorized in the group “Demographics” as a single cluster. Similarly, the necessity, needs, and psychological entanglement formed a cluster. To make it clearer, as a necessity we define the need for someone to provide personal data to an authority for a specific reason, such as to board a plane or to book a hotel room. As “needs” or psychological entanglement, we define the need of someone to receive a non-mandatory product or service and they must provide their personal data in order for this to happen. We have to define that we do not depict any relationships between these two factors. The remaining clusters are: Financial exchanges, financial benefits, and usefulness as one cluster, trust, control, confidence, and fear as another cluster, education, visualization, interaction and experience as another cluster, and finally, the dimensionality and the complexity of taking a privacy decision as a cluster. Following this clustering process, we created the following conceptual scheme shown in Figure 3, while Table 3 aggregates the research (checked in the table) that studied what influences ICT users’ privacy behavior.

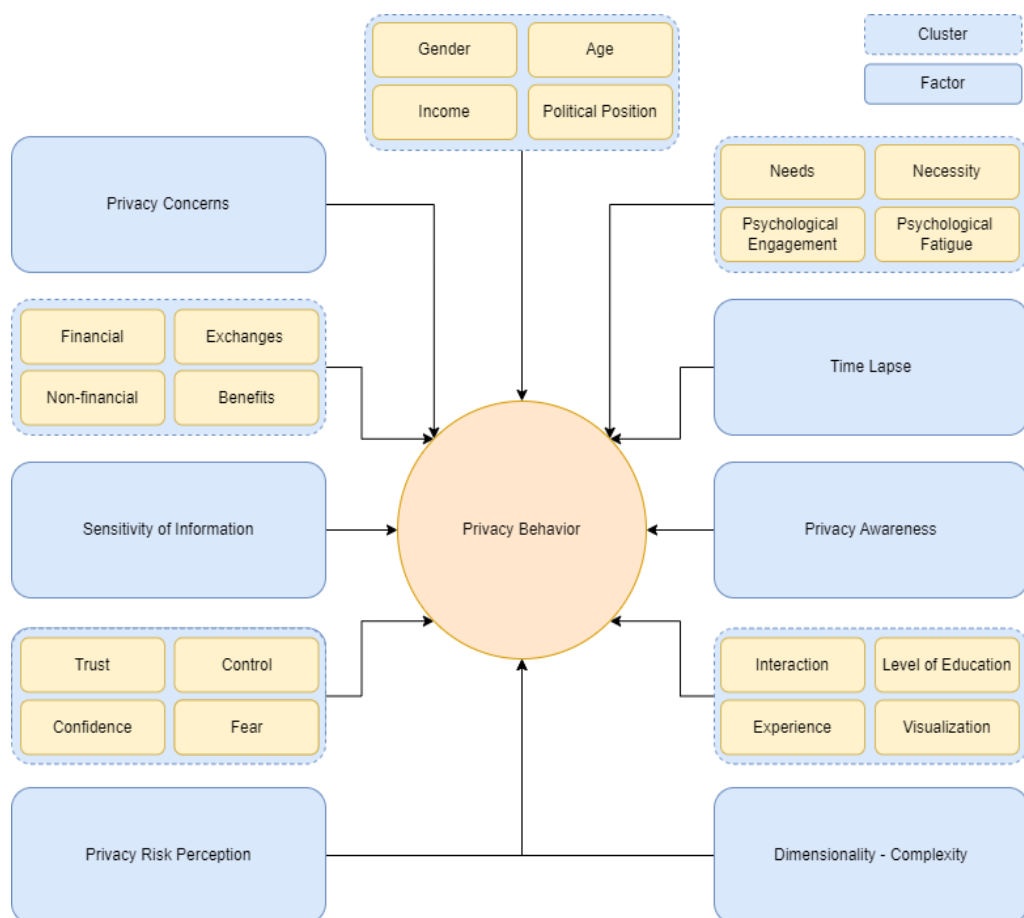


Figure 3. Conceptual scheme.

Table 3. Factors influencing ICT users' privacy behavior in the literature.

References	Demographics	Privacy Risk Perception	Financial Exchanges/Benefits/Fatigue	Needs Necessity	Privacy Concerns	Trust/Control/Confidence/Fear	Sensitivity of Information	Time	Education/Visualization/Interaction/Experience	Dimensionality/Complexity	Privacy Awareness
[12] Acquisti et al. (2015)					√						
[13] Alashoor et al. (2018)			√								
[14] Alawadhia and Hussain (2019)					√						
[15] Ameen et al. (2021)					√	√					
[16] Arica et al. (2022)					√						
[17] Avshalom and Yaron (2017)	√	√	√		√	√			√		
[18] Ayaburi and Treku (2020)					√	√					
[19] Bal (2014)		√				√					
[20] Bachura et al. (2022)						√					
[21] Becker (2018)					√						
[22] Bhagat et al. (2018)									√		
[23] Buchanan et al. (2007)										√	
[24] Buck (2017)					√			√			
[25] Cerruto et al. (2022)					√						
[26] Chakraborty et al. (2013)	√			√							
[27] Chawla and Kumar (2021)						√					
[28] Choi et al. (2018)			√	√	√						
[29] Chou et al. (2019)	√	√							√		
[30] Cloarec et al. (2022)		√	√		√	√					
[31] D'Souza and Phelps (2009)			√		√						
[32] Davazdahemami et al. (2018)					√	√					
[5] Dhir et al. (2016)	√										

[33] Dienlin and Treppe (2015)				√					√
[34] Ermakova et al. (2014)		√		√	√			√	
[35] Figl et al. (2020)								√	
[36] Flender and Müller (2012)							√		
[37] Fox et al. (2018)				√				√	√
[38] Gabel et al. (2019)		√		√					
[39] Gaurav (2008)			√	√					√
[4] Gerber et al. (2018)	√	√			√		√	√	√
[40] Ghose et al. (2020)		√		√	√				
[41] Gómez-Barroso (2018)			√	√					
[2] Hallam and Zanella (2017)			√	√				√	
[42] Hatamian et al. (2019)		√							
[43] Heravi et al. (2018)	√			√	√			√	√
[44] Hew et al. (2017)	√		√						
[45] Hofstra et al. (2016)	√			√		√			
[46] Ioannou et al. (2020)			√	√	√	√	√	√	
[47] Ioannou and Tussydiah (2021)					√	√			
[48] Jensen et al. (2017)			√		√				
[49] Jeong and Kim (2017)	√				√				
[50] Jia and Xu (2016)			√		√				√
[51] Jiang (2018)	√								
[52] Johnson (2013)								√	
[53] Jordaan and Van Heerden (2017)				√	√	√			√
[54] Jozani et al. (2020)		√	√						
[55] Junga and Park (2018)					√				
[56] Kang et al. (2016)				√		√			
[57] Kayes and Iamnitchi (2017)									√
[58] Keith et al. (2012)			√			√			√
[59] Keith et al. (2014a)		√	√				√		
[60] Keith et al. (2014b)			√		√				
[61] Kim et al. (2022)					√			√	
[62] Kitsios et al. (2022)						√			

[63] Knijnenburg et al. (2013)	√				√			√	√
[64] Korunovska et al. (2020)				√				√	
[65] Kosinski et al. (2013)								√	
[66] Krasnova et al. (2014)			√						
[67] Kraus et al. (2017)				√					
[68] Kurt (2010)	√				√			√	
[69,70] Kwee-Meier et al. (2016a, b)			√		√				
[71] Lankton et al. (2017)	√	√	√		√	√		√	√
[72] Lee et al. (2022)			√	√					
[73] Li and Chau (2019)					√	√			
[74] Li et al. (2015)	√	√			√		√		
[3] Li et al. (2017)	√			√	√			√	
[75] Li et al. (2019)				√					
[76] Li et al. (2020)	√	√	√						
[77] Li et al. (2022)					√				
[78] Liao et al. (2011)					√				
[79] Lidynia et al. (2018)					√				
[80] Lu et al. (2020)		√			√				
[81] Mager et al. (2021)			√						
[82] Marreiros et al. (2017)								√	√
[8] Mathews-Hunt (2016)					√	√			√
[83] McCoy et al. (2017)							√		
[7] Menard and Bott (2020)		√			√	√		√	
[84] Mosafer et al., 2021		√	√		√				
[85] Moshki and Barki (2014)					√			√	
[86] Mousavi et al. (2022)					√				
[87] Mullins et al. (2022)					√				
[88] Mutimukwe et al. (2020)		√			√	√			
[89] Nikkhah and Grover (2022)						√	√		
[90] Nikkhah and Sabherwal (2017)			√		√	√			
[91] Niknejad et al. (2020)				√	√	√			
[92] Nyshadham and Castano (2012)		√				√			

[9] Palos-Sanchez et al. (2019)					√			√	
[93] Park (2011)	√								
[94] Park (2015)	√								
[95] Paspatis et al. (2020)								√	√
[96] Pilton et al. (2021)									√
[97] Quayyum et al. (2021)	√		√						√
[98] Rangedda et al. (2022)				√					
[99] Reith et al. (2019)				√		√	√		
[100] Reith et al. (2021)						√	√		
[101] Renaud and Zimmermann (2018)								√	√
[102] Reynolds et al. (2011)	√								√
[103] Risius et al. (2020)							√		√
[104] Schomakers et al. (2019)	√		√					√	√
[105] Schreiber et al. (2013)				√		√	√		
[106] Schreiner and Hess (2015)			√	√		√	√		
[107] Segura et al. (2018)						√			
[108] Senarath and Arachchilage (2018)			√		√	√	√		
[6] Shane-Simpson et al. (2018)	√					√			
[109] Sharma and Crossler (2014)			√	√		√			√
[110] Spiekermann et al. (2012)				√		√			
[111] Sschwaig et al. (2013)						√			
[112] Strycharz et al. (2021)							√		
[113] Stutzman et al. (2011)	√					√			
[114] Taddicken (2014)						√			
[115] Terlizzi et al. (2019)					√	√	√		
[116] Tsai et al. (2011)						√	√		
[117] Tsai and Kelley (2014)						√		√	
[118] Tse et al. (2014)									√
[119] van Zoonen (2016)			√			√	√		√
[120] Venkatesh et al. (2012)				√					
[121] Viswanath et al. (2020)			√	√			√		
[122] Wall and Warkentin (2019)						√	√		

4. How Behavioral Factors Affect ICT Users' Privacy Behavior

Depending on the nature of each factor that affects privacy behavior, there is a different perspective on how and why it affects privacy behavior, while almost all factors get affected and affect the above behavior positively and/or negatively. Factors influencing privacy behavior can be differentiated according to their effect (i.e., how strongly they tend to influence behavior according to the relevant study) or depending on how often they appear as an influencing factor in the literature or the type of influence they exercise on behavior (i.e., positive, negative). There is no existing classification of privacy behavior determinant factors in the literature. In this work, we bring together the various factors that had been identified by researchers. Those factors are driven by multiple theories (e.g., protection motivation theory) or the researchers' point of view. Thus, they vary in level of abstraction, nature, and scope. Creating classification categories and assigning the identified factors into the relevant categories was a challenging task to ensure consistency and avoid duplication of factors in more than one category. For example, we examined the factors needs: When is something necessary, "needs": When is something psychologically necessary, and necessity under the same cluster. However, even though some factors, such as privacy risk perception, privacy concerns, and privacy awareness, have similar meanings or outcomes, we chose to separate them because many researchers have examined them separately and their findings present different results. For instance, the phenomenon of the privacy paradox is more associated with privacy concerns than with privacy awareness and privacy risk perception [1–4], while privacy awareness examines a more general behavior. On the other hand, privacy risk perception is highly associated with the potential result of someone's privacy action. Among the 11 factors we identified in the literature, we found in the respective papers that six factors show strong influence (i.e., quantitative studies have verified a strong correlation between them and privacy behavior). From the 11 factors, the literature analysis showed that eight of them appear frequently as determinants of privacy behavior. From the 11 factors, four show only positive influence on privacy behavior, two only negative behavior, and the remaining five factors may have positive or negative behavior depending on the situation of appearance.

4.1. Demographics

We discuss the factors "gender and age" of the "Demographics" cluster. Research shows that gender plays an important role in the self-exposure of personal information on the internet

[26,45,51,94,102], with age contributing to it [4,26,45,71,73]. For example, females tend to post more often and with fewer privacy restrictions on OSNs than males, while older users claimed to be more concerned with privacy, and this is reflected in their posting practices [107]. However, it is important to note that there are contrasting findings in the literature as well. One study found that demographics, such as gender, may have little to no influence on privacy behavior [68]. These contradictions suggest that the relationship between gender and privacy behavior is complex and may be influenced by various contextual factors. Because this study was conducted in an Asian country (Turkey), in contrast to all others, we assume that ethnicity or even religion or a combination of them may play a significant role in privacy behavior. The combination of gender and age plays a role in choosing which OSN will be preferred for a post, with female students preferring Facebook and male students preferring Instagram [6]. Adolescent men tend to post less data on OSNs and untag their older photographs as they age [5]. Even political position plays a role in US citizens, with the Democrats being more privacy-concerned than Republicans [40]. In the same research, authors found that low-income populations and females were more privacy-conscientious and more likely to opt out of location-tracking apps.

In conclusion, while there are contradictions in the literature regarding the influence of gender and other demographic factors on privacy behavior, there is a consensus that gender and age can indeed shape individuals' self-exposure of personal information on the internet. The complex nature of these relationships calls for further research to explore the underlying mechanisms and contextual factors that contribute to privacy behaviors across different demographic groups.

4.2. Privacy Risk Perception

The perception of risk directly affects the privacy behavior of a user when (s)he wants to post personal information on the internet [80] and especially to OSNs [5,6]). In the e-commerce context, consumers tend to undervalue the probability of risks and have difficulty separating their existing risk exposure from potential new threats [58]. The higher the risk perception, the lower the information that a user shares on the internet [58,84] and limiting the posts to OSNs [5].

Nonetheless, even if risk perception affects privacy behavior, this is mediated by financial exchanges/benefits. Further, privacy risk perception seems to have a stronger influence on privacy behavior when the person is young, and as the individuals become more mature, their privacy behavior is modified [29]. In combination with other factors from the cluster demographics, such as age [45,26,71,4,73] and gender [102], individuals weigh the risk of self-disclosure against the financial exchanges/benefits and modify their privacy behavior accordingly [84,109]. If the individual considers that the risk of disclosure is greater than what they can accept in relation to the perceived benefit, then they will disclose less personal information [19,84,109] or they will reject the financial offer. Reith et al. [99] research showed that ICT users' risk perception is important when they must choose what kind of mobile payment solution, they should choose to make a payment on the internet [99]. Terlizzi et al. [115] research showed similar results. More specifically, their research showed that privacy risk perceptions were also important when ICT users had to choose and use a banking application, and users tend to prefer the applications they trust more. In conclusion, while there are some inconsistencies in the literature, the impact of risk perception on privacy behavior is clear. Individuals' decisions about self-disclosure and information sharing are influenced by the interplay of risk perception, financial exchanges/benefits, demographics, and trust. As we mentioned in Section 4.1, more research is required to delve deeper into these relationships and comprehend the nuanced factors that shape privacy behavior in various contexts.

4.3. Financial Exchanges, Benefits, and Fatigue

Financial and non-financial exchanges and benefits are also factors that have a strong and direct effect on privacy behavior. According to the literature, individuals seem receptive to modifying their behavior according to the economic and non-economic exchanges, regardless of the beliefs they state to hold and the privacy awareness and privacy concerns they state to have [46,54,109,71,130,81,90]. Financial and non-financial exchanges, even if they do not change the individuals' perception, are able to persuade individuals to put aside their fears and give their personal data to third parties and consent to the terms they will be asked to accept [44,54,130,41,127]. Experimental evidence provides insights into individuals' behavior regarding financial and non-financial exchanges. For instance, in an experiment

in 2021 with 1274 consumers, the majority consented to trade their internet cookies for a 10-euro coupon value [81]. In another experiment, Schreiner and Hess [106] found that consumers are willing to pay an overhead amount of money for a privacy-freemium model in a service they want to be provided. Krasnova et al. [66] research also found that users are willing to change their privacy protection settings on mobile apps in exchange for a lesser price or extended functionality, with the functionality being less valued than the cost.

Healthcare patients seem to accept disclosing personal health information if the output benefit compensates for the value of the personal information [38]. Additionally, experimental evidence suggests that the limitation of the information that is given, rather than a deliberate evaluation of costs and benefits of privacy, affects people's privacy behaviors [92]. Alashoor et al. [13] showed that the positive effect of perceived benefits on disclosure likelihood was amplified under a positive mood state, whereas the negative effect of perceived privacy risks on disclosure likelihood was trivial under a positive mood state.

Some researchers also cite privacy fatigue as a category of non-financial rewards [28,59], with consumers stating that the fatigue comes from the privacy control complexity and that it affects their self-disclosure behavior [59]. Choi et al. [28] conducted a survey with 324 internet users to examine how privacy fatigue affects privacy behavior. Their findings showed that privacy fatigue (or, according to them, privacy burnout) has a stronger impact on privacy behavior than privacy concerns. This factor showed a strong correlation with other factors, such as privacy perception and privacy concerns [84,99,100]. In another example, Reith et al. [99] conducted research with 466 participants that got paid with a 20-euro voucher. Their results showed that gadget lovers would step aside from their privacy concerns while using mobile payment solutions [99]. Finally, the literature highlights the importance of financial and non-financial exchanges, privacy fatigue, and the importance of information in shaping privacy behavior. While there are some contradictions in the literature, it is clear that individuals are influenced by a variety of factors when making decisions about self-disclosure. The complex interplay of these factors necessitates additional research to better understand the mechanisms underlying privacy behavior in various contexts.

4.4. Needs and Necessity

Another important factor found to influence privacy behavior is the necessity of the information for the service provided. This factor seems to influence whether disclosure of information is required for the satisfaction of a real need, such as to present your identification documents to an aviation company when traveling [28,46], and in some cases, maybe even a medical necessity enforces to show medical records, such as COVID vaccination certificate [134] or a virtual need e.g., the need that has arisen from psychological charging [28,67,53] such as downloading an application from the internet that requires personal data for its download [45] or the need that arises for socialization in ONSs [26,53].

4.5. Privacy Concerns

Another factor influencing privacy behavior is privacy concerns. The factor privacy concerns seem to affect other clusters of factors [28,74,46] and is affected [49,73] by almost all the factors mentioned above. For example, it seems to influence and be influenced by the trust factor that an individual shows [46,127,47,90] and is influenced by the lack of awareness and risk perception factor [73,119,53,37]. Nikkhah and Sabherwal [90] found that the main inhibitor of disclosing personal information to Mobile Cloud-Computing apps (MCC) is perceived privacy concerns, and the main enablers are perceived usefulness and trust. It is worth noting that this factor has been discussed at length in relation to the paradox of privacy. According to studies, privacy concerns, although reported by many study subjects, do not seem to have a real effect on privacy behavior [1-4],103]. They may partially alleviate the attitude of users to post personal information on the internet, but eventually, users do adopt this behavior [80]. In conclusion, the literature highlights privacy concerns as an influential factor in privacy behavior, with intricate relationships with other factors. However, contradictions arise regarding the actual impact of privacy concerns on individuals' behavioral choices. Despite reporting concerns, individuals often proceed with posting personal information online. These contradictions underscore the complexity of the relationship between privacy concerns and behavior, necessitating further research to gain a deeper understanding of the underlying mechanisms and dynamics.

4.6. Trust, Control, and Confidence

Trust in an application or a service affects an individual's privacy behavior, and when it is acquired, it bypasses other factors, especially in the presence of the factor age of the cluster demographics (i.e., when users are older, trust acts more as a factor that bypasses other factors) [3]. According to Xu et al. [130], trust could play a primary role in addressing privacy concerns pertaining to OSNs, especially in the absence of well-established legal resources. Other models state that trust reduces privacy concerns [90,105] and thus affects privacy behavior. If there are communication channels that effectively build trust or be transparent to consumers about how their personal data are processed while using mobile apps consumers' privacy behavior can be modified [73,90,105,47]. For example, Wilson et al., [127] proposed a theoretical model and validated it through a controlled experiment that shows how empowering individuals with a sense of control over their personal information can help mitigate their privacy concerns. According to Ermakova et al. [34], trust plays a significant role in mitigating privacy concerns when a patient needs to upload medical records to a cloud service. Another study suggests that transparency of the practices of service leads to more accurate risk and trust perceptions and provides an improved foundation for informed decision-making [34]. In another study, the findings show that the important roles of political trust and the belief that governments need to be proactive in protecting peoples' welfare during a crisis can increase acceptance of surveillance and thus assist in the management of the health crisis [47]. Even though the literature contains contradictions, the influence of trust on privacy behavior is evident. Trust can act as a significant mitigating factor for privacy concerns and influence individuals' personal information-related decisions [1–4]. The complex and multifaceted character of trust, however, necessitates additional research into its dynamics and effects in various contexts.

4.7. Education, Interaction, Experience, Sensitivity of Information, Visualization, and Time-Lapse

Other factors found, such as: (a) The level of education, (b) the time available to make a decision [60], and (c) the sensitivity of the information we may need to disclose [74], showed having little

influence on privacy behavior. A person's level of education affects almost all the above factors [29,104]. Some studies show even a strong influence of education on privacy behavior depending on the presence of other factors, such as privacy concerns [43]. In addition, privacy-related knowledge, privacy-related IT knowledge, and general involvement with IT-related privacy seem to reduce privacy concerns [85].

The time available to make a decision to give personal data seems to affect our privacy behavior [60,101]. Studies show that the less response time is available for the individual to decide to give his/her personal information, the more expected a person's behavior is depending on the current level of privacy awareness. Thus, people with greater patience and self-control are less willing to disclose information through apps when first presented with the choice [59]. In addition, individuals are less tempted to disclose information as the time frame of risks is extended further into the future. The available time between a given information and making a decision in a complex matter seems to influence the decision in a potentially negative way. When an event lasts or is repeated at frequent intervals, it seems to affect privacy behavior [83,101].

In combination with the above paragraph, when a frequent interval event uses visual stimuli, such as repetitive advertisements, they seem to modify privacy concerns [9]. As soon as people get the knowledge and acquire the experience that someone is interested in their personal information, they value their information much more than before [110]. Thus, these people may alter their privacy behavior to a more secure one. In addition, privacy behavior can be improved by using visualization technics, such as privacy labels that promote privacy best practices to consumers [37] or better privacy policy designs [60]. In a relationship with the above paragraph and the factor time-lapse, Buck's [24] results on how time and experience affect privacy behavior show a significant effect on the concerns users have about their privacy—an increasing future self-continuity is related to greater concerns. Regarding visualization, according to Fox et al. [53], privacy labels seem to enhance privacy knowledge and reduce consumers' privacy concerns. In addition, Figl et al. [35] concluded that privacy nudging encourages users to choose the settings that meet their privacy needs without increasing any cognitive cost.

4.8. Privacy Awareness

Finally, one factor that can have a small to a very large effect depending on the context is how privacy-aware a person is [39,43,74]. This factor influences and is influenced by other factors, such as risk perception, and is strongly associated with privacy concerns and demographic factors (age, gender) [4,26,45,71,74], and level of education [5,74]. Furthermore, a person's lack of privacy awareness can heighten privacy concerns. Tse [118] stated that only a few persons change the default privacy protection configuration in OSNs, due to a lack of basic security knowledge and the perspective of perceptible threats. Risius et al. [103] found that if users' privacy education is successful in building short-term commitment and intentions, that translates into actual privacy-protecting behaviors. Pilton et al. [96], during their research, created a web-browser extension called "paradox" that modifies a website's privacy policy to an easier-to-read one. Their results showed that users' privacy awareness was enhanced to a more secure one. The same results showed in Paspatis et al. [95] research. Their browser extension for mobile applications called "AppAware extension" and AppAware Client-Server App was modifying apps' privacy policy using the app's permission set to an easiest-to-read one. After a questionnaire survey, ICT users' who participated in the survey stated that their privacy awareness was enhanced after using the AppAware App.

5. Discussion

Our research has shed light on the various factors that have been found to influence ICT users' privacy behavior. Various research works show that different factors influence privacy behavior and, thus, it is a multi-factor issue. From the systematic literature review that we performed, we aggregated the multiple factors that affect individuals' privacy behavior. We organized the identified factors into groups of eleven clusters. Our classification also includes per factor the severity of influence on privacy behavior, the frequency in which it is mentioned by researchers, and whether the factor has a positive or negative effect (or both).

The identified factors seem to influence privacy behavior with different strengths depending on the context in which it takes place, as well as the subject that it is influenced. Not all researchers have agreed on the strength and significance of the influence that each factor has. One possible explanation for these variations could be that the different empirical works were conducted in different cultures or with different sample sizes. For example, Kurt [68] conducted a survey at the University of Ankara with $n = 163$ females and $n = 42$ male

students participating in privacy behavior and OSNs. The researcher found out that “there is not any statistical significance between privacy behaviors and genders” when it comes to posting personal information on OSNs. Kurt’s results [68] are opposite to the majority of other research works that point out that gender plays a significant role in the self-exposure of personal information on the internet [26,45,51,74,94,102]. However, he does not offer any explanation regarding this deviation. One potential explanation could be the cultural characteristics of the sample, given that the participants were only students and only from one country.

Another finding from our research refers to the difficulty of studying existing literature and compare existing works due to the lack of common terminology in the academic community that studies the subject. The respective researchers utilize different terms to describe the same concept or interpret in different ways the same term. For example, researchers Nikkhah and Sabherwal [90] use the risk factor when they actually refer to the trust factor. In another example, researchers Ermakova et al. [34] discuss the trust factor when they seem to actually refer to the concept of control. This is also evident when encountering research on the time-lapse factor. Some researchers use the time factor, while they actually discuss the age of the individual, e.g., people tend to publish more personal data to the OSNs when they are young [5].

Based on the analysis of existing works, we have clustered the identified factors and we presented a collective view of the factors that influence individuals’ privacy behavior.

Within the scope of our research, we noticed that some of the factors of privacy behavior appear in the literature with particular frequency. The fact that several studies have addressed the “privacy paradox” phenomenon has greatly influenced the privacy concerns factor, with 74 surveys analyzing, discovering, or studying it. Demographics have been analyzed by 23 surveys. As this factor contains sub-factors, such as age, gender, etc., it creates favorable conditions for its appearance. Several studies dealing with privacy behavior were analyzed by groups such as gender, age groups such as adolescents, students, adults, or combinations thereof. The third most common factor is the perception of privacy risk. This can be explained by the fact that this factor seems to indirectly affect almost all other factors and directly the privacy behavior but it is also influenced by other factors.

5.1. Recommendations for the Private Sector and Practitioners

This paper provides findings from literature analysis regarding what influences ICT users' privacy behavior, which can be beneficial to the private sector. Companies and ICT or IT individual specialists that create mobile applications or application stores can utilize our findings to modify the way that they present to the users their privacy policies, i.e., what personal data they collect, why they need them and store them, and how they use them or to show that they satisfy the data minimization principle. Our analysis showed two things, respectively. As our analysis demonstrates, the factor of financial exchanges and benefits affects privacy behavior, and it becomes evident that ICT users are willing to pay more for a premium application that promotes personal data transparency or even personal data-free collection—privacy premium [106]. Respectively, from the cluster trust, control, and confidence, it becomes evident that ICT users tend to choose mobile applications and online stores if they feel secure about their personal data or if they feel they have control over them [73,90,105]. Companies that offer SoC as a service (SoCaaS) can also benefit from our research, for example, by utilizing the demonstrated privacy behavior factors they can create and apply privacy policies for their clients and at the same time, they can identify the weak spots in a company and recommend applying more privacy and security controls. ISPs can suggest and offer new privacy controls to their clients by knowing what affects privacy behavior, i.e., more parental control when they know that minors and adolescents are less inclined to apply protective privacy behaviors when using the home internet for browsing, school homework, and using their social media.

5.2. Recommendations for Policy Makers and Educational Institutes

The understanding of what affects privacy behavior can create a favorable ground in academia for further research. Teachers and researchers can use the knowledge that results from understanding the factors that influence privacy behavior to create teachable and learned knowledge. For example, professors and teachers can utilize our findings to create specialized information privacy courses or

theoretical/laboratory modules. The findings of this paper can also be used by designers of privacy awareness programs to promote privacy behavior. Our literature review showed that younger people tend to publish often personal data, and this is probably due to the lower risk perception they have. Thus, the state and respective authorities who design privacy awareness campaigns can benefit by targeting young people and students aiming to augment their privacy awareness and raise their risk perception levels. In our opinion, our review showed that what affects privacy behavior remains an open research subject. Focusing and trying to exploit the factors we analyzed, we may find new research paths and try to understand why the aforementioned factors influence privacy behavior.

6. Conclusions and Future Work

Privacy behavior seems to have an important role in our daily computerized life. More than two hundred studies researched and tried to identify the reasons behind our privacy actions while we browse the internet. They proposed various reasons and solutions, but still, we are not sure if we can see the whole picture behind what influences ICT users' privacy behavior. The studies we reviewed in this paper revealed multiple factors that, under the proper conditions, can influence privacy behavior. To the best of our knowledge, this is the first literature review that studied the set of factors that influence privacy behavior and not an individual factor or individual. We argue that our findings provide an answer to the research query posed in the introduction of what factors can influence ICT users' privacy behavior. To the best of our knowledge, this is the first research that concentrated on privacy behavior determinant factors, examined them, and categorized them into single factors and clusters of factors. We believe that our results can shift the attention of the academia and private companies to more targeted directions to provide better services and products to ICT users, as we mentioned in the previous section. We will continue our research by studying how we can exploit the knowledge of the identified factors to alter ICT users' privacy behavior towards more protective privacy actions. We aim to study how those factors were utilized in other fields, such as psychology, sociology, and philosophy, in order to modify behaviors. Our target is to be able to empirically explore through experiments how the technological context can trigger the modification of privacy behaviors and understand how privacy behavior is formulated in real technological contexts (e.g., e-government services, mobile applications), and propose mechanisms to promote protective

behaviors. Our future research will focus on utilizing the aforementioned privacy behavior determinant factors to propose techniques to enhance protective privacy behavior, based on similar research that had been conducted in other fields, such as psychology, sociology, sociology, and health.

Aside from the above, our investigation reveals numerous research opportunities. Changes in privacy behavior are a subject that still requires extensive study. Researchers may examine the efficacy of psychological factors in privacy behavior change and the durability of behavior modification interventions over the long term. Our research may create opportunities for further research in several areas, such as the utilization of privacy determinant factors to enable privacy-protective behaviors.

Our findings provide a comprehensive perspective on the significance of privacy behavior enhancement and inspire further research by addressing the potential benefits and research opportunities and promoting inter-disciplinary collaborations.

This limits our study because it leads to the lack of a definition of what constitutes a strong or weak influence that a specific privacy behavior factor has on privacy behavior. Therefore, our findings related to the influence of privacy behavior determinant factors (i.e., Table 4) are limited, respectively.

Table 4. Severity, Frequency, and Influence of Factors.

Factor	Strong Influence	Frequency of Appearance in Literature	Positive Influence	Negative Influence
Financial/Non-Financial Exchanges/Benefits/Usefulness	√	√	√	√
Privacy Risk Perception	√	√	√	√
Trust/Control/Confidence/Fear		√	√	
Privacy Concerns	√	√	√	
Needs/necessity/Psychological Engagement		√		√
Sensitivity of information			√	
Privacy Awareness	√	√	√	√
Time Lapse			√	
Level of Education/Visualization/Interaction/Experience	√	√	√	√
Demographics	√	√	√	√
Dimensionality/Complexity				√

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions: Conceptualization, I.P. and A.T.; methodology I.P.; formal analysis, A.T., and S.K.; investigation, I.P.; writing—original draft preparation, I.P.; writing—review and editing, I.P., A.T., and S.K.; visualization, I.P.; supervision, A.T., and S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>.
2. Hallam, C.; Zanella, G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput. Hum. Behav.* **2017**, *68*, 217–227.
3. Li, H.; Luo, X.; Zhang, J.; Xu, H. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Inf. Manag.* **2017**, *54*, 1012–1022.
4. Gerber, N.; Gerber, P.; Volkamer, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Comput. Secur.* **2018**, *77*, 226–261.
5. Dhira, A.; Kaur, P.; Lonka, K.; Nieminen, M. Why do adolescents untag photos on Facebook? *Comput. Hum. Behav.* **2016**, *55*, 1106–1115, ISSN 0747-5632, <https://doi.org/10.1016/j.chb.2015.11.017>.
6. Shane-Simpson, C.; Manago, A.; Gaggi, N.; Gillespie-Lynch, K. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Comput. Hum. Behav.* **2018**, *86*, 276–288, <https://doi.org/10.1016/j.chb.2018.04.041>.
7. Menard, P.; Bott, G. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Comput. Secur.* **2020**, *95*, 101856.
8. Mathews-Hunt, K. CookieConsumer: Tracking online behavioural advertising in Australia. *Comput. Law Secur. Rev.* **2016**, *32*, 55–90.
9. Palos-Sanchez, P.; Saurab, J.R.; Martin-Velicia, F. A study of the effects of programmatic advertising on users' concerns about privacy overtime. *J. Bus. Res.* **2019**, *96*, 61–72.
10. Hinds, J.; Williams, E.; Joinson, A. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *Int. J. Hum. Comput. Stud.* **2020**, *143*, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>.
11. Association for Information Systems. Senior Scholars' of Journals. Available online: <https://aisnet.org/page/SeniorScholarBasket?&hhsearchterms=%22basket%22> (accessed on 10 June 2022).
12. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and human behavior in the age of information. *Science* **2015**, *347*, 509–514.
13. Alashoor, T.; Al-Maidani, N.; Al-Jabri, I. The Privacy Calculus under Positive and Negative Mood States. In Proceedings of the International Conference on Information Systems, San Francisco, CA, USA, 13–16 December 2018.

14. Alawadhia, R.; Hussain, T. A Method Toward Privacy Protection in Context-Aware Environment. In Proceedings of the 2nd International Conference on Emerging Data and Industry 4.0 (EDI40), Leuven, Belgium, 29 April–2 May 2019.
15. Ameen, N.; Hosany, S.; Paul, J. The personalisation-privacy paradox: Consumer interaction with smart technologies and shopping mall loyalty. *Comput. Hum. Behav.* **2021**, *126*, 106976. <https://doi.org/10.1016/j.chb.2021.106976>.
16. Arica, R.; Cihan, C.; Onur, Ç.; Abdülkadir, C.; Hsu, M.-J.; Valentina, C. Travel experience sharing on social media: Effects of the importance attached to content sharing and what factors inhibit and facilitate it Travel. *Int. J. Contemp. Hosp. Manag.* **2022**, *34*, 1566–1586.
17. Avshalom, G.; Yaron, A. An analytical framework for online privacy research: What is missing? *Inf. Manag.* **2017**, *54*, 948–957.
18. Ayaburi, E.; Treku, D. Effect of penitence on social media trust and privacy concerns: The case of Facebook. *Int. J. Inf. Manag.* **2020**, *50*, 171–181.
19. Bal, G. Explicitness of Consequence Information in Privacy Warnings: Experimentally Investigating the Effects on Perceived Risk, Trust, and Privacy Information Quality. In Proceedings of the 35th International Conference on Information Systems (ICIS 2014), Auckland, New Zealand, 14–17 December 2014.
20. Bachura, E.; Valecha, R.; Chen, R.; Rao, R. The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter. *MIS Q.* **2022**, *46*, 881–910. <https://doi.org/10.25300/MISQ/2022/15596>.
21. Becker, M. Understanding users' health information privacy concerns for health wearables. In: Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, Hawaii, USA, 3–6 January 2018; Volume 9, pp. 3261–3270. <https://doi.org/10.24251/hicss.2018.413>.
22. Bhagat, S.; Saminathan, K.; Agarwal, A.; Dowsley, R.; De Cock, M.; Nascimento, A. Privacy-preserving user profiling with Facebook likes. In Proceedings of the IEEE International Conference on Big Data, Seattle, WA, USA, 10–13 December 2018; pp. 5298–5299.
23. Buchanan, T.; Paine, C.; Joinson, A.N.; Reips, U.D. Development of measures of online privacy concern and protection for use on the internet. *J. Am. Soc. Inf. Sci. Technol.* **2007**, *58*, 157–165.
24. Buck, C. Stop Disclosing Personal Data about Your Future Self. AIS Electronic Library (AISeL). In Proceedings of the AMCIS 2017, Boston, MA, USA, August 10–12, 2017.
25. Cerruto, F.; Cirillo, S.; Desiato, D.; Gambardella, S.M.; Polese, G. Social network data analysis to highlight privacy threats in sharing data. *J. Big Data* **2022**, *9*, 19.
26. Chakraborty, R.; Vishik, C.; Rao, H. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decis. Support Syst.* **2013**, *55*, 948–956.
27. Chawla, N.; Kumar, B. E-Commerce and Consumer Protection in India: The Emerging Trend. *J. Bus. Ethics* **2021**, *180*, 581–604. <https://doi.org/10.1007/s10551-021-04884-3>.
28. Choi, H.; Park, J.; Jung, Y. The role of privacy fatigue in online privacy behavior. *Comput. Hum. Behav.* **2018**, *81*, 42–51.
29. Chou, H.; Liu, Y.; Chou, C. Privacy behavior profiles of underage Facebook users. *Comput. Educ.* **2019**, *128*, 473–485.
30. Cloarec, J.; Meyer-Waarden, L.; Munzel, A. The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychol. Mark.* **2022**, *39*, 647–661. <https://doi.org/10.1002/mar.21587>.
31. D'Souza, G.; Phelps, J.E. The privacy paradox: The case of secondary disclosure. *Rev. Mark. Sci.* **2009**, *7*, 4.
32. Davazdahemami, B.; Hammer, B.; Luse, A.; Kalgotra, P. The Role of Parallelism in Resolving the Privacy Paradox of Information Disclosure in Social Networks. In Proceedings of the Thirty Ninth International Conference on Information Systems, San Francisco, CA, USA, 13–16 December 2018.

33. Dienlin, T.; Trepte, S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *Eur. J. Soc. Psychol.* **2015**, *45*, 285–297.
34. Ermakova, T.; Fabian, B.; Zarnekow, R. Acceptance of Health Clouds—A Privacy Calculus Perspective. In Proceedings of the ECIS 2014 Proceedings—22nd European Conference on Information Systems, Tel Aviv, Israel, 9–11 June, 2014.
35. Figl, K.; Lehrer, C. Privacy Nudging: How the Design of Privacy Settings Affects Disclosure in Social Networks. European Conference on Information Systems (ECIS 2020) virtual conference, June 2020.
36. Flender, C.; Müller, G. Type indeterminacy in privacy decisions: The privacy paradox revisited. In *Quantum Interaction*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 148–59.
37. Fox, G.; Tonge, C.; Lynn, T.; Mooney, J. Communicating compliance: Developing a GDPR privacy label. In Proceedings of the Americas Conference on Information Systems, New Orleans, LA, USA, 16–18 August 2018.
38. Gabel, M.; Nils, F.; Nüesch, S. The (In)Effectiveness of Incentives—A Field Experiment on the Adoption of Personal Electronic Health Records. In Proceedings of the ICIS 2019, Munich, Germany, 15–18 December 2019.
39. Gaurav, B. Three Research Essays on Examining Online Privacy Concerns: The Role of Personal Dispositions, Contexts and Privacy-Assurance Features. In Proceedings of the AMCIS 2007 Keystone, Colorado, USA, 9–12 August, 2007; Volume 381. <https://aisel.aisnet.org/amcis2007/381> Accessed on 1 May 2023.
40. Ghose, Anindya and Li, Beibei and Macha, Meghanath and Sun, Chenshuo and Foutz, Natasha Zhang, Trading Privacy for Public Good: How Did America React During COVID-19?. NYU Stern School of Business, <http://dx.doi.org/10.2139/ssrn.3624069>(accessed on January 1, 2022).
41. Gómez-Barroso, J. Experiments on personal information disclosure: Past and future avenues. *Telemat. Inform.* **2018**, *35*, 1473–1490.
42. Hatamian, M.; Serna, J.; Rannenbergh, K. Revealing the unrevealed: Mining smartphone users privacy perception on app markets. *Comput. Secur.* **2019**, *83*, 332–353.
43. Heravi, A.; Mubarak, S.; Raymond Choo, K. Information privacy in online social networks: Uses and gratification perspective. *Comput. Hum. Behav.* **2018**, *84*, 441–459.
44. Hew, J.; Tan, G.; Lin, B.; Ooi, K. Generating travel-related contents through mobile social tourism: Does privacy paradox persist? *Telemat. Inform.* **2017**, *34*, 914–935.
45. Hofstra, B.; Corten, R.; van Tubergen, F. Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Comput. Hum. Behav.* **2016**, *60*, 611–621.
46. Ioannou, A.; Tussyadiah, I.; Lu, Y. Privacy concerns and disclosure of biometric and behavioral data for travel. *Int. J. Inf. Manag.* **2020**, *54*, 102122.
47. Ioannou, A.; Tussyadiah, I. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technol Soc.* **2021**, *67*, 101774. <https://doi.org/10.1016/j.techsoc.2021.101774>.
48. Jensen, C.; Potts, C.; Jensen, C.D. Privacy practices of Internet users: Self-report versus observed behavior. *Int. J. Hum.-Comput. Stud.* **2017**, *98*, 82–91.
49. Jeong, Y.; Kim, Y. Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Comput. Hum. Behav.* **2017**, *69*, 302–310.
50. Jia, H.; Xu, H. Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology J. Psychosoc. Res. Cyberspace* **2016**, *10*, 4. <https://doi.org/10.105817/CP2016-1-4>.
51. Jiang, J. Social Login Acceptance: A DIF Study of Differential Factors. In Proceedings of the PACIS 2018, Jokohama, Japan 2018; Volume 20. Available online: <https://aisel.aisnet.org/pacis2018/20> (accessed on 1 May 2023).
52. Johnson, D.G. Human-computer interaction: Psychology as a science of design. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and*

- Emerging Applications*, 3rd ed.; Jacko, J., Ed.; CRC Press: Boca Raton, FL, USA, 2013; pp. 3–18.
53. Jordaan, Y.; Van Heerden, G. Online privacy-related predictors of Facebook usage intensity. *Comput. Hum. Behav.* **2017**, *70*, 90–96.
 54. Jozani, M.; Ayaburi, E.; Ko, M.; Choo, K. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Comput. Hum. Behav.* **2020**, *107*, 106260.
 55. Junga, Y.; Park, J. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *Int. J. Inf. Manag.* **2018**, *43*, 15–24.
 56. Kang, H.; Shin, W.; Tam, L. Differential responses of loyal versus habitual consumers towards mobile site personalization on privacy management. *Comput. Hum. Behav.* **2016**, *56*, 281–288.
 57. Kayes, I.; Iamnitchi, A. Privacy and security in online social networks: A survey. *Online Soc. Netw. Media* **2017**, *3–4*, 1–21.
 58. Keith, M.; Thompson, S.; Hale, J.; Greer, C. Examining the rationality of information disclosure through mobile devices. In Proceedings of the International Conference on Information Systems (ICIS 2012), Orlando, FL, USA, 16–19 December 2012; Volume 3.
 59. Keith, M.; Maynes, C.; Lowry, P.; Babb, J. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In Proceedings of the International Conference on Information Systems (ICIS 2014), Auckland, New Zealand, 14–17 December 2014. <https://doi.org/10.13140/2.1.3164.6403>.
 60. Keith, M.; Ngo, N.; Babb, J. The effects of consumer self-regulation and risk immediacy on mobile information disclosure. In Proceedings of the International Conference on Interaction Sciences, Savannah, Georgia, USA, 7–9 August, 2014.
 61. Kim, J.; Kim, T.; Wojdyski, B.; Jun, H. Getting a Little Too Personal? Positive and Negative Effects of Personalized Advertising on Online Multitaskers. *Telemat. Inform.* **2022**, *71*, 101831. <https://doi.org/10.1016/j.tele.2022.101831>.
 62. Kitsios, F.; Mitsopoulou, E.; Moustaka, E.; Kamariotou, M. User-Generated Content behavior and digital tourism services: A SEM-neural network model for information trust in social networking sites. *Int. J. Inf. Manag. Data Insights* **2022**, *2*, 100056.
 63. Knijnenburg, B.; Kobsa, A.; Jin, H. Dimensionality of information disclosure behavior. *Int. J. Hum.-Comput. Stud.* **2013**, *71*, 1144–1162.
 64. Korunovska, J.; Kamleitner, B.; Spiekermann, S. The Challenges and Impact of Privacy Policy Comprehension. In Proceedings of the Systematic Bias in Notice Comprehension Twenty-Eighth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco, 15–17 June, 2020.
 65. Kosinski, M.; Stillwell, D.; Graepel, T. Private traits and attributes are predictable from digital records of human behavior. *Proc. Natl. Acad. Sci.* **2013**, *110*, 5802–5805.
 66. Krasnova, H.; Eling, N.; Abramova, O.; Buxmann, P. Dangers of ‘Facebook Login’ for Mobile Apps: Is There a Price Tag for Social Information? In Proceedings of the International Conference on Information Systems, Auckland, New Zealand, 14–17 December, 2014.
 67. Kraus, L.; Wechsung, I.; Möller, S. Psychological needs as motivators for security and privacy actions on smartphones. *J. Inf. Secur. Appl.* **2017**, *34*, 34–45.
 68. Kurt, M. Determination of in internet privacy behaviours of students. *Procedia—Soc. Behav. Sci.* **2010**, *9*, 1244–1250. [10.1016/j.sbspro.2010.12.314](https://doi.org/10.1016/j.sbspro.2010.12.314).
 69. Kwee-Meier, S.; Bützler, J.E.; Schlick, C. Development and validation of a technology acceptance model for safety-enhancing, wearable locating systems. *Behav. Inf. Technol.* **2016**, *35*, 394–409. <https://doi.org/10.1080/0144929X.2016.1141986>.
 70. Kwee-Meier, S.; Sonja Th Altendorf, E.; Mertens, A.; Schlick, C.M. Safety enhancing locating wearables on passenger ships: Privacy and security perceptions by the elderly. *IFIP Adv. Inf. Commun. Technol.* **2016**, *474*, 34–48. https://doi.org/10.1007/978-3-319-44805-3_4.

71. Lankton, N.; McKnight, D.; Tripp, J. Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Comput. Hum. Behav.* **2017**, *76*, 149–163.
72. Lee, E.; Kim, J.; Kim, J.; Koo, C. Information Privacy Behaviors during the COVID-19 Pandemic: Focusing on the Restaurant Context. *Inf. Syst. Front.* **2022**, 1–17. Epub ahead of print. PMID: 36000075; PMCID: PMC9388979. <https://doi.org/10.1007/s10796-022-10321-1>.
73. Li, C.; Chau, P. Leveraging Communication Tools to Reduce Consumers' Privacy Concern in the On-demand Services: An Extended S-O-R Model of Perceived Control and Structural Assurance. In Proceedings of the PACIS 2019, X'ian, China, 8-12 July, 2019, Volume 48. <https://aisel.aisnet.org/pacis2019/48> (Accessed on 5 April 2023).
74. Li, K.; Lin, Z.; Wang, X. An empirical analysis of users' privacy disclosure behaviors on social network sites. *Inf. Manag.* **2015**, *52*, 882–891.
75. Li, P.; Cho, H.; Goh, Z. Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. *Telemat. Inform.* **2019**, *41*, 114–125.
76. Li, K.; Cheng, L.; Teng, C.-I. Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Inf. Process. Manag.* **2020**, *57*, 102128.
77. Li, Y.-J.; Cheung, C.M.K.; Shen, X.-L.; Lee, M.K.O. When Socialization Goes Wrong: Understanding the We-Intention to Participate in Collective Trolling in Virtual Communities. *J. Assoc. Inf. Syst.* **2022**, *23*, 678–706. <https://doi.org/10.17705/1jais.00737>.
78. Liao, C.; Liu, C.; Chen, K. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electron. Commer. Res. Appl.* **2011**, *10*, 702–715.
79. Lidynia, C.; Brauner, P.; Ziefle, M. A step in the right direction—Understanding privacy concerns and perceived sensitivity of fitness trackers. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, 17-21 July 2018; pp. 42–53. https://doi.org/10.1007/978-3-319-60639-2_5.
80. Lu, Y.; He, L.; Wu, H.; Feng-Kwei, W.; Shiqiao, J. A meta-analysis to explore privacy cognition and information disclosure of internet users. *Int. J. Inf. Manag.* **2020**, *51*, 102015.
81. Mager, S.; Kranz, J. Consent Notices and the Willingness-to-Sell Observational Data: Evidence from User Reactions in the Field. In Proceedings of the European Conference on Information Systems, Virtual, 2021.
82. Marreiros, H.; Tonin, M.; Vlassopoulos, M.; Schraefel, M. “Now that you mention it”: A survey experiment on information, inattention and online privacy. *J. Econ. Behav. Organ.* **2017**, *Vol. 140*, 1–17.
83. McCoy, S.; Everard, A.; Galletta, D.F.; Moody, G.D. Here we go again! The impact of website ad repetition on recall, intrusiveness, attitudes, and site revisit intentions. *Inf. Manag.* **2017**, *54*, 14–24. <https://doi.org/10.1016/j.im.2017.03.005>.
84. Mosafer, H.; Sarabadani, J.; Sohrabi BYazdani, H.R.; Manian, A. The Role of IT Identity in Self-disclosure Behavior on Social Networking Sites. In Proceedings of the AMCIS 2021 (Virtual Conference), 9–13 August 2021; Volume 16. https://aisel.aisnet.org/amcis2021/adopt_diffusion/adopt_diffusion/16.
85. Moshki, H.; Barki, H. Individuals' IT-related privacy concerns: A two-phase cognitive model. 8th International Conference, UAHCI 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, 22-27 June, 2014, Proceedings, Part IV 2014.
86. Mousavi, R.; Zhao, K. Examining the Impacts of Airbnb Review Policy Change on Listing. *J. Assoc. Inf. Syst.* **2022**, *23*, 303–328.
87. Mullins, J.K.; Stewart, P.A.; Greitens, T.J. Facing Forward: Policy for Automated Facial Expression Analysis. *J. Assoc. Inf. Syst.* **2022**, *23*, 1347–1353. <https://doi.org/10.17705/1jais.00788>.
88. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Gov. Inf. Q.* **2020**, *37*, 101413.

89. Nikkhah, H.R.; Grover, V. An Empirical Investigation of Company Response to Data Breaches. *MIS Q.* **2022**, *46*, 2163–2196. <https://doi.org/10.25300/MISQ/2022/16609>.
90. Nikkhah, H.R.; Sabherwal, R. Mobile Cloud-Computing Applications: A Privacy Cost-Benefit Model. In Proceedings of the Americas Conference on Information Systems, Boston, MA, USA, 10–12 August 2017.
91. Niknejad, N.; Ismail, W.B.; Mardani, A.; Liao, H.; Ghani, I. A comprehensive overview of smart wearables: The state of the art literature, recent advances, and future challenges. *Eng. Appl. Artif. Intell.* **2020**, *90*, 103529. <https://doi.org/10.1016/j.engappai.2020.103529>.
92. Nyshadham, E.; Castano, D. Affect and Online Privacy Concerns. *SSRN Electron. J.* **2012**, *5*. <https://doi.org/10.2139/ssrn.2051044>.
93. Park, Y.J. Digital literacy and privacy behavior online. *Commun. Res.* **2011**, *40*, 215–236.
94. Park, Y.J. Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Comput. Hum. Behav.* **2015**, *50*, 252–258.
95. Paspatis, I.; Tsohou, A.; Kokolakis, S. AppAware: A policy visualization model for mobile applications. *Inf. Comput. Secur.* **2020**, *28*, 116–132. <https://doi.org/10.1108/ICS-04-2019-0049>.
96. Pilton, C.; Faily, S.; Henriksen-Bulmer, J. Evaluating privacy—Determining user privacy expectations on the web. *Comput. Secur.* **2021**, *105*, 102241. <https://doi.org/10.1016/j.cose.2021.102241>.
97. Quayyum, F.; Cruzes, D.; Jaccheri, L. Cybersecurity awareness for children: A systematic literature review. *Int. J. Child-Comput. Interact.* **2021**, *30*, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>.
98. Ragnedda, M.; Ruiu, M.L.; Addeo, F. The self-reinforcing effect of digital and social exclusion: The inequality loop. *Telemat. Informatics.* **2022**, *72*, 101852. <https://doi.org/10.1016/j.tele.2022.101852>.
99. Reith, R.; Buck, C.; Dennis, W.; Bettina, L.; Eymann, T. How privacy affects the acceptance of mobile payment solutions. In Proceedings of the 27th European Conference on Information Systems (ECIS) Stockholm and Uppsala, Sweden, Association for Information Systems: 8–14 June 2019.
100. Reith, R.; Fortagne, M.A.; Diel, S.; Buck, C.; Lis, B.; Eymann, T. Pandemic Containment with Digital Measures: Acceptance and Privacy Aspects of Contact Tracing Apps. In Proceedings of the ECIS 2021, Marrakech, Morocco, 2021 (open date); Volume 6. Available online: https://aisel.aisnet.org/ecis2021_rp/6 (accessed on 1 May 2023).
101. Renaud, K.; Zimmermann, V. Ethical guidelines for nudging in information security & privacy. *Int. J. Hum.-Comput. Stud.* **2018**, *120*, 22–35.
102. Reynolds, B.; Venkatanathan, J.; Goncalves, J.; Kostakos, V. Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. In *Human-Computer Interaction—INTERACT 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 204–215. https://doi.org/10.1007/978-3-642-23765-2_14.
103. Risius, M.; Baumann, A.; Hanna, K. Developing a New Paradigm: Introducing the Intention-Behaviour Gap to the Privacy Paradox Phenomenon. In Proceedings of the Twenty-Eighth European Conference on Information Systems (ECIS2020) 15–17 June 2020, virtual conference, Marrakesh, Morocco, 2020.
104. Schomakers, E.; Lidynia, C.; Müllmann, D.; Ziefle, M. Internet users' perceptions of information sensitivity—Insights from Germany. *Int. J. Inf. Manag.* **2019**, *46*, 142–150.
105. Schreiber, T.; Deuker, A.; Albers, A.; Neves, M. The Privacy Trade-Off: App Usage on OSN. In Proceedings of the AMCIS 2013, 15–17 August 2013, Chicago, Illinois, USA.
106. Schreiner, M.; Hess, T. Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies. In Proceedings of the 23rd European Conference on Information Systems, Münster, Germany, 26–29 May.
107. Segura, A.; Alsadoon, A.; Costadopoulos, N.; Prasad, P.W.C. Ethical implications of user perceptions of wearable devices. *Sci. Eng. Ethics* **2018**, *24*, 1–28. <https://doi.org/10.1007/s11948-017-9872-8>.

108. Senarath, A.; Arachchilage, N. Understanding user privacy expectations: A software developer's perspective. *Telemat. Inform.* **2018**, *35*, 1845–1862.
109. Sharma, S.; Crossler, R. Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electron. Commer. Res. Appl.* **2014**, *13*, 305–319.
110. Spiekermann, S.; Korunovska, J.; Bauer, C. Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy. In Proceedings of the International Conference on Information Systems (ICIS 2012), Orlando, Florida, USA, 16–19 December, 2012; Volume 4. <https://doi.org/10.2139/ssrn.2148886>.
111. Sschwaig, S.; Grover Segars, A.; Fiedler, K.A. Model of Consumers' Perceptions of the Invasion of Information Privacy. *Inf. Management.* **2013**, *50*, 1–12. <https://doi.org/10.1016/j.im.2012.11.002>.
112. Strycharz, J.; Smit, E.; Helberger, N.; van Noort, G. No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Comput. Hum. Behav.* **2021**, *120*, 106750. <https://doi.org/10.1016/j.chb.2021.106750>.
113. Stutzman, F.; Capra, R.; Thompson, J. Factors mediating disclosure in social network sites. *Comput. Hum. Behav.* **2011**, *27*, 590–598.
114. Taddicken, M. The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-Disclosure. *J. Comput.-Mediat. Commun.* **2014**, *19*, 248–273. <https://doi.org/10.1111/jcc4.12052>.
115. Terlizzi, M.; Brandimarte LBrown, S.; Sanchez, O. Privacy Concerns and Protection Motivation Theory in the Context of Mobile Banking. In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, 8–14 June 2019; ISBN 978-1-7336325-0-8; Research Papers. Available online: https://aisel.aisnet.org/ecis2019_rp/24 (accessed on) 1 May 2023.
116. Tsai, J.; Egelman, S.; Cranor, L.; Acquisti, A. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Inf. Syst. Res.* **2011**, *22*, 254–268.
117. Tsai, J.Y.; Kelley, P.G. Who's viewed you? The impact of feedback in a mobile location-sharing application. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ACM, Toronto, ON, Canada – 26 April - 01 May 2014; pp. 2005–2008.
118. Tse D., Xu, X., Bai M., Chen Z., Meng X., and Wang, Y., (2014). "Privacy Issues in online social networks: User behaviors and third-party applications". PACIS 2014 Proceedings. 42. <http://aisel.aisnet.org/pacis2014/42>
119. van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480.
120. Venkatesh, V.; Thong, J.Y.L.; Xu, X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Q.* **2012**, *36*, 157–178.
121. Viswanath, A.; Das, S. Would you Trust a Bot for Healthcare Advice? An Empirical Investigation. In Proceedings of the 24th Pacific Asia Conference on Information Systems, PACIS 2020, Dubai, United Arab Emirate, 22–24 June 2020.
122. Wall, J.; Warkentin, M. Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Inf. Manag.* **2019**, *56*, 103157.
123. Wang, C.; Zhan, N.; Wang, C. Managing Privacy in the Digital Economy. *Fundam. Res.* **2021**, *1*, 543–551. <https://doi.org/10.1016/j.fmre.2021.08.009>.
124. Wiegard, R.B.; Breitner, M.H. Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. *Electron. Mark. Vol.* **2017**, *29*, 1–17. <https://doi.org/10.1007/s12525-017-0274-1>.
125. Wieneke, A.; Lehrer, C.; Zeder, R.; Jung, R. Privacy-related decision-making in the context of wearable use. In Proceedings of the Pacific Asia Conference on Information Systems, Chiayi, Taiwan, 27 June – 1 July 2016; Paper 67.

126. Wilson, D.W.; Valacich, J. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. In Proceedings of the International Conference on Information Systems (ICIS 2012), Orlando, Florida, USA, 16-19 December, 2012; Volume 5, pp. 4152–4162.
127. Wilson, D.; Schuetzler, R.; Dorn, B.; Proudfoot, J.G. When Disclosure is Involuntary: Empowering Users with Control to Reduce Concerns. In *Information Systems and Quantitative Analysis Faculty Proceedings & Presentations*; Omaha, Nebraska, March 18 2015; Volume 17, Dr. C.C. and Mabel L. Criss Library. Available online: <https://digitalcommons.unomaha.edu/isqafacproc/17> (accessed on 1 May 2023).
128. Wisniewski, P.; Knijnenburg, B.; Lipford, H. Making privacy personal: Profiling social network users to inform privacy education and nudging. *Int. J. Hum.-Comput. Stud.* **2017**, *98*, 95–108.
129. Wu, C.; Li, W. Why Do Consumers Boycott Personalization Marketing? A Perspective from Multidimensional Development Theory and Psychological Contract Violation. In Proceedings of the PACIS 2019, 8-12 July, 2019, Volume 200.
130. Xu, H.; Parks, R.; Chu, C.; Zhang, X. Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding. In Proceedings of the 16th Americas Conference on Information Systems 2010 (AMCIS 2010) 12-15 August, 2010, Lima, Peru; Volume 7, p. 503.
131. Zhang, Y.; He, W.; Peng, L. How Perceived Pressure Affects Users' Social Media Fatigue Behavior: A Case on WeChat. *J. Comput. Inf. Syst.* **2020**, *62*, 337–348. <https://doi.org/10.1080/08874417.2020.1824596>.
132. Zareef, M.; Gurvirender, T. The Role of Cognitive Disposition in Deconstructing the Privacy Paradox: A Neuroscience Study. In Proceedings of the AMCIS 2015, *Puerto Rico*, 13-15 August, 2015.
133. Zalmanson, L.; Oestreicher-Singer, G.; Ecker, Y. The Role of Social Cues and Trust in Users' Private Information Disclosure. *MIS Q.* **2021**, *46*, 1109–1134. <https://doi.org/10.25300/MISQ/2022/16288>.
134. European Union. EU Digital COVID Certificate. Available online: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (accessed on 24 April 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Paper – II



Article

How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors

Paspatis Ioannis * and Tsohou Aggeliki

Ionian University, Department of Informatics, Corfu, Greece, 49100; atsohou@ionio.gr

* Correspondence: ipaspatis@ionio.gr; Tel.: +30-26610-87760

Abstract: Several studies have shown that the traditional way of learning is not optimal when we aim to improve ICT users' actual privacy behaviors. In this research, we present a literature review of the theories that are followed in other fields to modify human behavior. Our findings show that cognitive theory and the health belief model present optimistic results. Further, we examined various learning methods, and we concluded that experiential learning is advantageous compared to other methods. In this paper, we aggregate the privacy behavior determinant factors found in the literature and use cognitive theory to synthesize a theoretical framework. The proposed framework can be beneficial to educational policymakers and practitioners in institutions such as public and private schools and universities. Also, our framework provides a fertile ground for more research on experiential privacy learning and privacy behavior enhancement.

Keywords: privacy behavior factors; privacy behavior; cognitive theory; health belief model

1. Introduction

Citation: Paspatis, I.;
Tsohou, A. How to
Influence Privacy
Behavior Using
Cognitive Theory and
Respective Determinant
Factors. *J. Cybersecur.
Priv.* **2023**, *3*, x.
<https://doi.org/10.3390/xxxxx>

Academic Editor(s):
Name

Received: 6 June 2023

Revised: 10 July 2023

Accepted: 13 July 2023

Published: date



Copyright: © 2023 by
the authors. Submitted
for possible open access
publication under the
terms and conditions of
the Creative Commons

Attribution (CC BY)
license
(<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

With the evolvement of technology, such as internet-connected wearables, enhanced reality, mobile devices, and the intrusion of social media in our lives, our individuality is constantly exposed. Data are retrieved from companies and individuals in many ways and sometimes even without our knowledge, for example, from the Internet of Things devices (IoT) [2] or even when we self-expose ourselves to social networks [2,2]. Self-exposed behavior may have a significant negative effect on individuals' lives, and Information and Communications Technology (ICT) users may find themselves as victims of thieves, scams, or impersonation. At the same time, third parties can use personal data in their favor in many ways such as to manipulate voting opinions [2] or manipulate buying behavior through targeted advertising practices [2,2]. Thus, ICT users are vulnerable to privacy breaches, data misuse, and unauthorized access to their personal information.

In the last decade, the research on what influences privacy behavior showed a significant increment. Researchers, software houses, information security providers, and individuals are trying to find ways to enhance ICT users' privacy behaviors. Various studies have shown that ICT users state that they care about their personal data, but they still disclose a vast amount of personal information when using internet-connected devices [2,2]. Many academics recognize this phenomenon as a "privacy paradox" [2,2,2,2]. Several studies have tried to identify the reasons behind ICT users' privacy behaviors, identifying psychological, sociological, and behavioral factors for their actions [2,2,2,2]. Many researchers found various factors that influence privacy behavior, and thus, if we alter these factors we may influence ICT users' privacy behavior actions, such as personal information disclosure, the application of privacy-protective controls, or the configuration of privacy settings.

From the above, we identify a necessity to confront these two issues. First, we need to understand what affects privacy behavior, and second, it will be beneficial to understand how to influence ICT users' protective privacy behaviors. To address the first issue, we conducted

an in-depth literature review on the factors affecting privacy behavior. Our recent research [2] showed that behind ICT users' privacy behaviors, there are eleven dominant factors, including privacy concerns, trust, awareness, and others (further analyzed in Section 5). This research aims to investigate the underlying factors that influence individuals' privacy-conscious actions in the digital realm, as well as to explore effective interventions to promote such actions. In addition, we laid the groundwork for extending our research to the utilization of these factors for enabling privacy-protective behaviors and thus address the second issue. Understanding how to promote human behavior change is crucial for several reasons. First, technological advancements alone cannot ensure adequate privacy protection, as the success of privacy measures ultimately depends on the users' behaviors. Second, a significant number of privacy incidents can be attributed to an individual's lack of awareness, knowledge, or motivation to consciously adopt privacy actions. By investigating how human behavior can be effectively changed, this study can contribute to the development of strategies and interventions that address these underlying factors and thus lead to improved privacy behavior [2,2,2,2]. To address this research gap, this study explores theoretical frameworks, empirical studies, and interventions from related fields such as psychology, sociology, philosophy, and the health field. By drawing upon these interdisciplinary perspectives, our research aims to shed light on the factors influencing privacy behavior, identify effective behavior modification techniques, and propose actionable recommendations for ICT users, service providers, and policymakers. Traditional learning approaches that could be used to promote privacy behaviors, such as lectures, textbooks, and exams have long been the foundation of education systems around the world. However, these approaches have inherent limitations that impede a learner's holistic development. According to many researchers [2,2,2], one of the limitations of traditional learning approaches is passive learning. Traditional learning frequently encourages passive knowledge acquisition, in which students are passive recipients of information rather than active participants in the learning process. Students' engagement, critical thinking, and problem-solving abilities are hampered by this approach. Another limitation is the lack of practical application. Traditional learning methods frequently focus on theoretical concepts that are disconnected from real-world applications. This gap between theory and practice can impede a student's ability to apply classroom knowledge and skills in real-world situations. Further, traditional learning relies heavily on memorization and short-term retention, resulting in limited long-term recall and

understanding. A student's ability to connect concepts and apply knowledge in different contexts is hampered by the emphasis on memorization rather than deep comprehension. Additionally, traditional learning approaches typically take a one-size-fits-all approach, assuming that all students learn in the same way and at the same pace. Individual differences in learning styles, preferences, and strengths are ignored, potentially leading to disengagement and poor learning outcomes. Educators and researchers [2,2,2,2,2,2-2,2,2] have advocated for the incorporation of experiential learning methods to address the limitations of traditional learning approaches. Experiential learning is defined as the process whereby knowledge is created through the transformation of experience [2]. Experiential learning involves learners in hands-on experiences, reflection, and active experimentation, and it provides several advantages. First, experiential learning encourages active participation and personal involvement, allowing students to make direct connections between theoretical concepts and real-life experiences. This participation fosters a deeper understanding as well as a sense of relevance and applicability. Also, experiential learning allows learners to develop practical skills through participation in real-world scenarios, simulations, and problem-solving activities, which improves students' abilities to apply their knowledge and skills in real-world situations, preparing them for real-life challenges. Finally, experiential learning promotes deep comprehension and meaningful learning by actively engaging learners in real-life contexts, resulting in improved retention and the transfer of knowledge and skills to novel situations.

Thus, in this paper, we propose the use of experiential methods and practices to promote privacy-protective behaviors, taking into account the antecedents of privacy behavior. We identify methodologies and practices that are followed in the fields of philosophy, psychology, and sociology to influence someone's behavior using experiential methods. We argue that this can lay the groundwork for empirically examining how to guide ICT users' existing privacy behaviors to become more privacy-protective. To the best of our knowledge, this is the first research that is trying to encapsulate experiential learning methods and target the modification of users' privacy behaviors. In summary, our paper addresses the following research questions:

Research Question 1: what empirical methods and practices have been followed in other fields, such as philosophy or psychology, to influence human behavior via experiential techniques and could be used in the field of information privacy towards enabling privacy-protective behaviors?

Research Question 2: how can we influence privacy behavior determinant factors to guide ICT users' privacy behaviors using experiential methods?

After the introduction, this paper continues with the sampling methodology of the literature review we performed. In section three, we perform a literature review of experiential learning in the fields of philosophy, psychology, health, and sociology. In section four, we provide an adjustment of the definitions we found during the literature review in the field of our expertise, and we provide our conceptual scheme. In section five, we propose an adaptation of the above definitions to our field, and we provide an encapsulation between the theories we capture from our literature review and the privacy behavior factors. In section six, we discuss our findings and our model. Finally, section seven concludes the paper and provides implications, possible solutions, and future research.

2. Literature Review Methodology

2.1. Sampling Methodology

For our search in the literature, we employed a systematic search strategy across multiple academic databases. Since we needed to search in multiple scientific fields, we targeted the most widely used search engines in each field. To identify philosophy-related articles, we used the following search engines: PhilPapers, Jstor, PubMed, and the Stanford Encyclopedia of Philosophy. To find sociology-related articles, we used Sociological Abstracts (www.proquest.com/sociologicalabstracts (accessed on 2 February)), ProQuest Social Science Journals (search.proquest.com/socialsciencejournals (accessed on 3 February 2022)), and SocArXiv (socopen.org accessed on 5 February 2022). To identify psychology-related and health-related articles, we used the search engines PubMed, PsycINFO (www.apa.org/pubs/databases/psycinfo (accessed on 5 March 2022)), and PsycARTICLES (www.apa.org/pubs/databases/psycarticles (accessed on 6 March)). We also included more general databases such as Google Scholar and Scopus. The search was conducted using relevant keywords such as “experiential learning”, “experiential learning methods”, “theory selection for experiential learning and behavior modification”, and “behavior modification methods and theories”. The initial search

yielded a large number of articles, which were then refined based on predefined inclusion and exclusion criteria.

The theory selection (inclusion) procedure entailed a thorough examination of the theories and models identified in the literature. We evaluated each theory's relevance, empirical support, and applicability in the context of behavior modification, behavior enchantment, and how to influence human behavior. The selected theories were chosen based on their potential to provide insights into understanding and modifying human behavior at any age, with a preference for theories that are applied to adults. The reason for this choice is that we primarily aim to validate our framework in future research with adult participants. The theories we chose served as the foundation for our research framework. To identify relevant learning theories, we conducted a thorough review of studies that investigated various approaches to changing human behavior. We considered various learning theories, including experiential learning and persuasive technologies. The theories chosen were chosen based on their potential effectiveness in encouraging people to practice privacy-conscious behavior.

We refrained from imposing any limitations on the chronological range or publication types. Instead, we deemed journal articles and conference articles as suitable sources to yield acceptable outcomes. We used the keywords: experiential learning, experiential education, experiential learning methods in psychology, experiential learning methods in sociology, and experiential learning methods in philosophy. We also included several books that studied experiential methods and experiments that affect learning and education using experiential procedures in the above fields. These books are mostly in physical form and cannot be found online. The theory selection (inclusion) procedure entailed a thorough examination of the theories and models identified in the literature. We evaluated each theory's relevance, empirical support, and applicability in the context of behavior modification, behavior enchantment, and how to influence human behavior. The selected theories were chosen based on their potential to provide insights into understanding and modifying behavior in humans of any age, with a preference for theories that are applied to adults. The reason for these choices is that our initial target group for testing our framework in future research is people aged 18 and up. The theories we chose served as the foundation for our research framework. To identify relevant learning theories, we conducted a thorough review of studies that investigated various approaches to changing human behavior. We considered various learning theories, including experiential learning and persuasive

technologies. The theories chosen were based on their potential effectiveness in encouraging people to practice privacy-conscious behavior.

To identify relevant learning theories, we conducted a comprehensive analysis of studies that investigated different approaches to modifying human behavior. We considered various learning theories, such as experiential learning and persuasive technologies, among others. The selected theories were chosen based on their potential effectiveness in promoting privacy-conscious behavior.

2.2. Exclusion Criteria

Applying the aforementioned methodology outlined above, our initial search yielded a substantial number of 584 outcomes. To refine and narrow down the extensive pool of results, we implemented a rigorous selection process that prioritized articles and books with high citation counts, in addition to publications authored by recognized pioneers within their respective fields. Consequently, our efforts culminated in the identification of 90 distinct and noteworthy papers and books. Nevertheless, a subset of the retrieved articles failed to elucidate any factors associated with experiential learning methodologies. Subsequently, we employed a screening process to eliminate studies that, despite satisfying the search criteria, did not primarily focus on the identification of experiential methods for educational or learning purposes and consequently lacked corresponding outcomes. Consequently, we excluded a total of 41 papers from further analysis, as they did not specifically investigate the subject matter at the core of our study. Following this rigorous procedure, we were left with a final selection of 49 papers and books that specifically examined or identified distinct methods capable of influencing learning or educational procedures.

3. Theoretical Background in Experiential Learning in Other Fields

3.1. The Concept of Behavior in Psychology

This section is a first reference to the basic theories that contributed to the understanding of behavior as reflected in the field of psychology. More specifically, four basic theories are captured:

The neuropsychological theory;

The psychoanalytical theory;

The behavioral theory;

The cognitive theory.

The above theories were not the only ones formulated but were the most basic ones studied in the specific field of psychology.

Neuropsychological Theory: This theory examines only pathological behaviors, which are seen through the cognitive effects of neurological disorders [2,2]. We will not delve into this theory as it relates to ailments of a medical nature.

Psychoanalytical Theory: according to Freud [2,2], human behavior is the result of a person's defense against his instinctual impulses.

Behavioral Theory: A person's behavior consists of the immediate reaction to an environmental stimulus. Stimulus $\rightarrow$ Reaction = Behavior or $S \rightarrow R$ = Behavior. In his research, Pavlov [2] describes that a person's behavior is acquired through classical conditioning, while according to Skinner [2,2], it is through operant conditioning and is modified only if the environmental stimuli are modified. The basic mechanisms of behavior control and modification are reward/reward, fear, and punishment.

Cognitive Theory: It is the evolution of $S \rightarrow R$ behavioral theory. This theory holds that stimuli and reactions mediate cognitive processes that influence behavior. According to Weinman [2], cognitive processes include beliefs, perceptions, and attributions—also called productive causes [2]. According to Koulirakis et al. [2] attribution is defined as the cognitive process that a person constructs to try and explain why an event happened to her. The above contributes together with the environment when making a decision or facing a challenge. Finally, according to Ambrason [2], attributions can be generalized or specialized. Models that attempt to explain how cognitive factors lead to various social behaviors are referred to as socio-cognitive models. Conner [2] and Conner and Norman [2] distinguish two types of socio-cognitive models. The first type includes

the attribution models which refer to people's causal explanations for events related to their health. The second type includes models aimed at predicting people's future behaviors.

In the context of this research, we will not deal with the first two theories as the first concerns behaviors that are due to pathological factors, while the second captures more about the explanation of behavior rather than how it can be modified. Cognitive theory, also known as cognitive psychology, seeks to comprehend how people process information, think, and make decisions. It emphasizes the role of cognitive processes in shaping behavior, such as perception, attention, memory, and problem-solving. According to the theory, people actively interpret and make sense of their surroundings based on their prior knowledge, beliefs, and experiences [2]. The cognitive theory can be applied to understand how individuals perceive and evaluate privacy risks and make decisions about their online privacy in the context of privacy behavior in ICT users. According to the theory, cognitive processes influence people's privacy-related behaviors, including their knowledge and understanding of privacy issues, their perception of risks and benefits, and their attitudes and beliefs about privacy.

One study that exemplifies the application of the cognitive theory in modifying privacy behavior is the work by Ghosh and Singh [2]. They conducted a study to examine cognitive dissonance theory to understand privacy behavior. The researchers discovered that the evaluation of benefits associated with disclosure does not motivate disclosure as strongly as previously believed. Instead, they found that a behavior-based approach, as opposed to an investigation of the attitudes regulating disclosure, yields fresher insights and a more nuanced comprehension of the privacy paradox.

The schematic representation of the behavioral theory and cognitive theory can be seen in Figures 1 and 2.

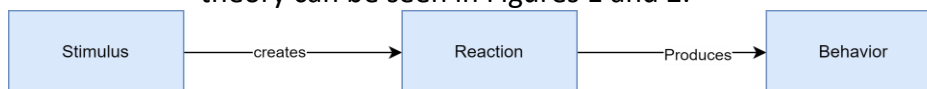


Figure 6. Behavioral theory (based on Overskeid, 2007; Gardner, 1979).

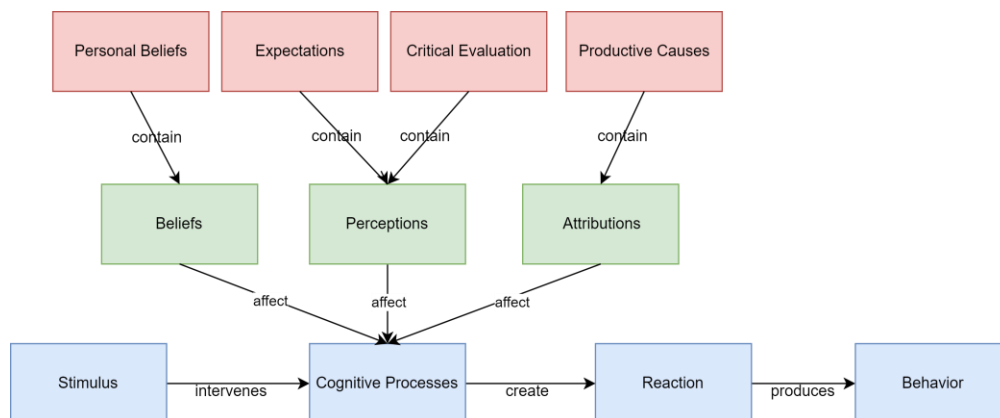


Figure 7. Cognitive theory (based on Weinman, 1990).

An example of cognitive theory can be shown below: John and Alice are looking at the photo uploaded on Instagram by their mutual acquaintances, Tomas and Kathrin, with public access to it. The photo shows the two of them sitting at a park in Karlovy Vary in the Czech Republic. John thinks it is a beautiful photo (cognitive processes: belief and perception), while Alice, who is more privacy-aware, realizes that Kathrin and Tomas are not in their residences; now several people will know about it, and Kathrin and Tomas are exposed to the risk of robbery (cognitive process: attribution: awareness). In this example, the environmental conditions were the same, but the cognitive background of Alice was different. Moreover, we observe that in this example, multiple cognitive processes came into effect. From this point of view, John's beliefs and perceptions made him observe only the romantic part of the photo. On the other hand, Alice's privacy awareness levels activated her cognitive processes differently and made her understand the dangers of that post. The potential expositions in that photo do not stop at what Alice observed. For example, even if the date is not visible, an experienced ICT user could potentially find the date of the photograph from the meta-data of the photograph.

Cognitive psychologists describe two distinct types of cognitive processes. The first type of process is the short-term processes which include expectations, critical evaluation as elements of perceptions, and the productive causes as attributions. The second type is long-term processes that contain the personal beliefs of the person.

According to Bandura [2], expectancy is a process in which the individual discounts a future event. Bandura describes the expectancy process as both a perception process and a belief, depending on the point of view of the event. According to Beck [2], critical evaluation is a perception process and can be used as a diagnostic process in which individuals evaluate what may be happening to them. According to

Rotter [2], productive causes are perceptions that people construct when trying to explain why something happened to them. It is also worth mentioning that according to the social psychologists, Stroebe and Stroebe [2], cognitive processes are essential causes of the manifestation of behavior. Also, cognitive processes are more amenable to modification when they involve cognitive factors such as beliefs rather than factors such as personality. Also, Sheeran and Abraham [2] state that beliefs are stable individual characteristics that shape behavior and are acquired through early socialization without being strictly defined and can vary between individuals of the same social group. Finally, Lewin [2] formulated the value-expectancy model which states that an individual's behavior revolves around two axes: the value that the individual assigns to a specific goal and the individual's assessment of the probability of a specific action to achieve this goal. From all that preceded, we believe that there is a scientific consensus that cognitive theory is the dominant method in the fields of psychology and philosophy, answering Research Question 1. We have to mention that psychology and philosophy were treated as one field until the philosopher Gockel according to Krstic coined the term "psychology" [2].

3.2. The Concept of Behavior in the Health Field

The health field played a significant role in the development of cognitive theory, creating a new path of research mostly because of the close relationship between psychology and psychiatry. Many researchers from the health field tried to adjust the cognitive theory in their field of expertise, most usually called the health belief model. The health model deals with the scientific area of psychology that deals with human behavior in the context of health and illness. Scientists use this model to intervene in problems arising from a chronic or life-threatening disease, but without engaging in a strictly therapeutic process [2,2,2]. Becker et al. [2] added another dimension to the model called "health motivation", which is nothing more than the individual's readiness to care about health issues. The model was formally established with the publication of the research by Becker et al. [2] and was aimed at maintaining health and controlling frailty. The model has been used more than any other social-cognitive model in a range of health behaviors and different target populations [2]. The health belief model is based on two health-oriented axes: Threat Perception and Behavioral Evaluation. The perception of a threat depends on two factors: the subjective sense of vulnerability (perceived susceptibility) and the subjective sense of severity

(perceived severity) [7,8]. The evaluation of the behavior also consists of two sets of beliefs: the subjective feeling about the benefits (perceived benefits) from adopting a behavior targeting better health and the subjective feeling about the obstacles (perceived barriers) from adopting a behavior, i.e., the evaluation of the possible negative consequences associated with the prevention behavior (e.g., side effects.). The health belief model (HBM) is a psychological framework that explains and predicts health-related behaviors in individuals. It implies that beliefs about the severity of a health threat, susceptibility to the threat, the benefits of taking preventive action, and the barriers to such action influence people's actions to protect or improve their health. When applied to the context of privacy behavior in ICT users, the health belief model can be viewed as a framework for understanding individuals' motivations and decision-making processes regarding privacy protection. Individuals are more likely to engage in privacy-enhancing behaviors if they perceive the risks to their privacy as severe and themselves as vulnerable to those risks, according to the model. Furthermore, they are more likely to adopt privacy-conscious behaviors if they believe that the benefits of taking privacy-protective actions outweigh the barriers or costs associated with such actions.

The study by Jensen et al. [7] is an example of using the health belief model in the context of privacy behavior. They looked into the factors that influence people's adoption of privacy-enhancing measures on social networking sites. Individuals who perceived higher levels of privacy risks, believed they were vulnerable to privacy breaches, and perceived more benefits than barriers to taking privacy-protective actions were more likely to engage in privacy-enhancing behaviors, according to the study's findings. The above is reflected in Figure 3.

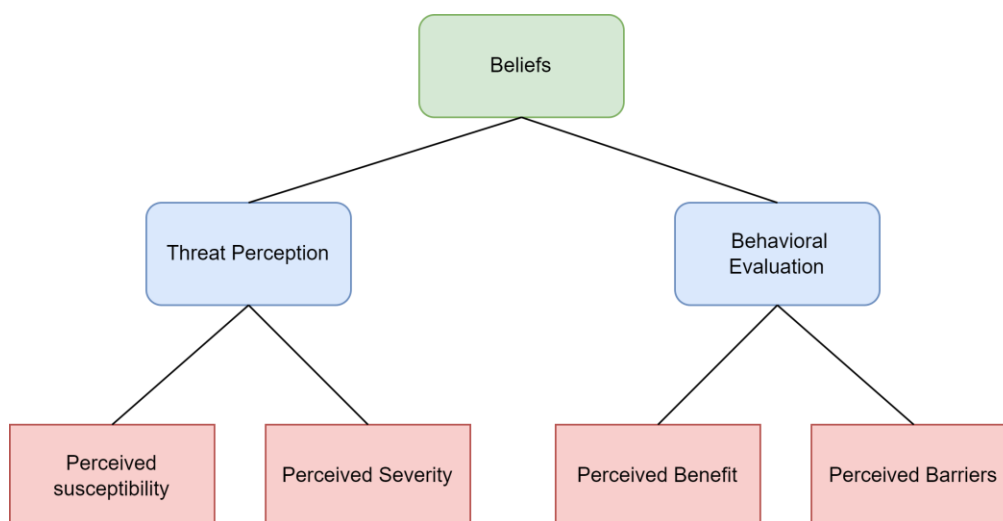


Figure 8. Health belief model based on cognitive theory adjusted to the health field

3.3. Behavior and Experiential Learning

In this section, we present the literature review on the definitions of experiential experience and learning, as they have been defined in the fields of psychology, philosophy, and sociology in the past.

In their book about Aristotle called *Nicomachean Ethics*, Brown and Brown [?] state that according to Aristotle, for the things we must learn before we do them, we learn them by doing them. The experiential experience differs from the didactic experience where the participant has a mostly passive role. Dewey [?], one of the first scholars to deal with the importance of experiences in learning, states that a person learns from their experiences when they are active in them, in light of supporting evidence. In partial agreement with Aristotle, Freire [19] (Figure 4) states that the cycle of learning begins with an experiential event, continues with a reflection on the experience, and leads to action. We argue that this last theory shows common elements with the cognitive theory model we described in Section 3.1 (Figure 2).



Figure 9. Experiential learning process according to Freire (1980).

According to Kolb [?], personality as well as environmental and social factors play a large role in the acquisition of knowledge. He states that to acquire knowledge through experiential learning, the following factors must be present:

The participants must have the will to learn through the experience they lived;

The participants should be able to reproduce the experience;

The participants must have analytical thinking and understand the experience;

The participants have the ability to make decisions and solve problems to create new ideas through the experiences they lived.

Rogers [?] extended Kolb's view, including in the conditions of experiential learning with both the assessment of an acquired experience of the subject himself and of a third party (the subject of experiential learning as an observer).

Boud et al. [?] identifies three stages of the reflective process in the context of experiential learning:

The participant reviews the events and has the ability to study the experience again, calling this review a return to the experience;

The participant recognizes the importance of the experience to third parties, through emotions;

The participant discovers the new dimensions of the experience so that through it, the change in his behavior occurs and creates a new way of thinking and new abilities.

Boud et al. [2] recognize that this is a transformative process, and through experiences, the subject recognizes new tendencies and abilities.

Criticizing Kolb's model, Jarvis [2] agrees that learning arises from experience but does not necessarily involve the activity of processing or conscious reflection, although he emphasizes that awareness allows the individual to change his reactions and beliefs. Therefore, according to Jarvis, experience consists of the integration of an external stimulus into one's store of knowledge. According to Boud et al., [2] as cited in Kokko [2], awareness can lead to an individual's internal commitment to action/reaction as well as the modification of their knowledge. Mezirow [2] states that adults in particular learn more efficiently through reflection on experience and thus experiential learning. By making use of mental habits, meaning-making perspectives, and meaning sets, they become multifaceted, open, and emotionally ready to produce beliefs and opinions that prove capable of justifying the impulse to action. In agreement with the above, scientists in the fields of philosophy, sociology, and psychology also align with the view of Taylor [2]. According to his research, the adoption of opinions and patterns of behavior takes place gradually and mainly experientially, as well as without the awareness of various social and cultural influences and limitations. Experiential learning has also occupied the field of school learning. Other researchers [2,2] have studied the learning processes of teachers and have concluded that teachers as adults are in a daily learning process, focusing on improving their teaching skills and teaching methodologies. Such learning is part of the broader process of self-development and lifelong learning.

As we observed, various scientific fields have been involved with experiential learning for a long time. The first steps of experiential learning came from the ancient times of Aristotle, probably around 335 B.C., when he said the famous phrase "the things we must learn before we do them, we learn them by doing them". Afterward, at the start of the 20th century, we saw the first tries at experiential learning and methods from psychologists and philosophers such as Freud [2], Pavlov [2], Dewey [2], and Kolb [2], and it continues up to the 21st

century, especially from sociologists and philologists such as Kokko [2], Mezirow [2–2], Jarvis [2], and Dacou [2].

By integrating the cognitive theory and the health belief model, researchers and practitioners can gain a comprehensive understanding of individuals' privacy behaviors in the context of ICT use. These theories provide valuable insights into the cognitive processes, beliefs, and motivations that drive privacy-related decision-making and can be used to develop effective strategies for changing someone's privacy behavior.

4. Adaptation of Theoretical Background for the Domain of Privacy Behavior

In this section, we aim to adapt the aforementioned cognitive theory to our field of expertise. Our scope is to adapt the cognitive processes derived from the cognitive theory to the privacy behavior field. Our target is separated into two different axes. Firstly, we will connect, adapt, and classify the cognitive process elements of beliefs, perceptions, and attributions (productive causes) to privacy behavior factors. Secondly, to adapt the cognitive theory as a basic modifier of privacy behavior enhancement using the experiential methods as described in Section 3.3.

With an aim to propose our model, we will create and appropriately define new experiential learning terms that respond to ICT. Moreover, we will try to adapt the terms derived from the behavior and the experiential learning sections and transform them to be a match for our proposed model.

Taking into account the existing literature, we propose the following terms, as shown in the Table 1 while figure 5 presents our conceptual scheme.

Table 4. Terms and definitions.

Term	Definition
Experiential Event	An experiential event is any event experienced by a subject
Experiential Learning	Experiential learning is defined as the process in which one learns or becomes specialized in a task by doing it. By extension, experiential experience is defined as the

	result of experiential learning, such as knowledge and feelings
Event of Privacy Breach	Any data processing that takes place using a service or technology provider (or more) and is contrary to the perception of the data subject when consenting and using this service or technology (we do not mean the violation of the terms of use by the provider). Therefore, the same event can be classified as a violation of privacy, or not, depending on the person and their perception of privacy
Experiential Event of Privacy Breach	Any event of privacy breach in which the subject became aware of that breach. An example of such a breach is when a data subject discloses his location on a social network by posting a photograph and, after appropriate third-party processing of that photograph, the temporal and spatial location of the subject is found, while the data subject was not aware that this is possible.
Experiential Privacy Learning	The process by which the subject analyzes the experiential event and learns from it.
Experiential Experience of Privacy Violation	The outcome for the subject of learning (knowledge, skills, and feelings) about privacy
Privacy Concerns	The user's willingness to share data and how these relationships in turn are affected by inter-individual differences in an individual's regulatory focus, thinking style, and institutional trust [2].
Protective Behavior	A protective behavior enacted by a person to protect them-selves or others from a threat to their health or safety [2].

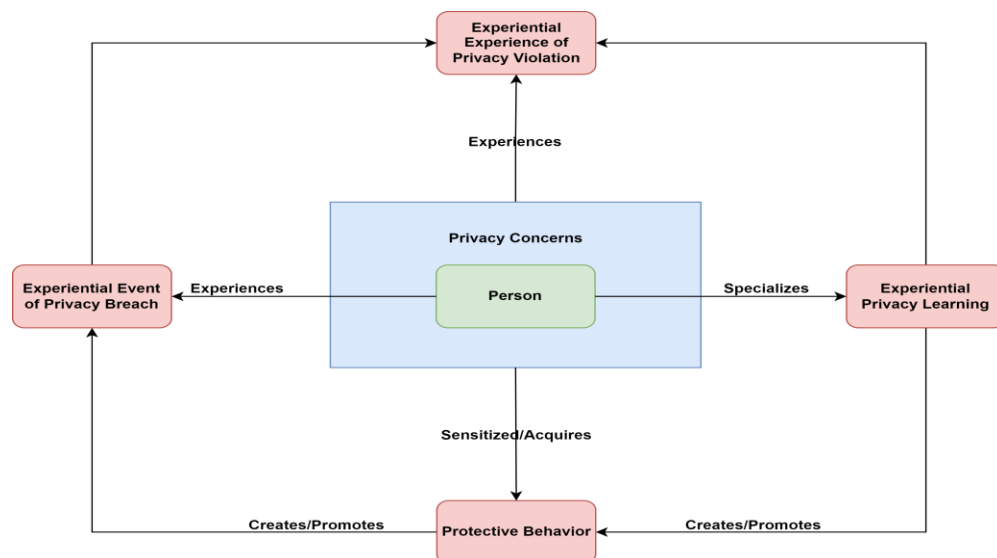


Figure 10. Conceptual scheme.

Practical Case Studies in the Privacy Behavior Field

A case study by Smith et al. [?] examines the implementation of a Privacy Lab at a technology company. The Privacy Lab utilized hands-on workshops, simulated privacy breaches, and had interactive discussions as experiential learning activities. The case study illustrates how employees actively participated in real-world scenarios, such as identifying privacy risks in product development, analyzing data protection measures, and making privacy-aware decisions. Johnson and Anderson [?] discuss privacy training in healthcare settings as an example. The case study focuses on a privacy education program that used experiential learning methods, including role-playing, scenario-based simulations, and peer feedback. The study indicates how healthcare professionals actively applied privacy principles in simulated patient interactions, improving their understanding of privacy regulations and practices. Brown and Green [?] provide an example of a privacy workshop held for K-12 students. To teach students about online privacy and responsible digital behavior, the workshop used experiential learning techniques such as group activities, interactive games, and real-life scenarios. The case study demonstrates how students actively participated in hands-on methods of improving their privacy awareness and developed safe online practices, such as creating privacy settings on social media platforms.

By incorporating these real-life examples and case studies, we provide tangible evidence of the successful implementation of experiential learning in privacy education. These studies demonstrate how

experiential learning activities engage participants, promote practical skills, and foster a more in-depth understanding of privacy concepts and behaviors.

5. Cognitive Theory and Privacy Behavior Factors

If we focus on cognitive theory and the belief model, which we examined in Section 3, we can identify common elements with our previous work [2] of what affects privacy behavior. More specifically, we observed that cognitive processes that affect behavior through experiential methods are affected by three influential axes (hereafter cognitive processes): beliefs, perceptions, and attributions. This offers fertile ground to try to conceptualize the factors that we analyzed in our previous work with the cognitive theory and the belief model. In the next subsection, we will show that every factor we found can be matched with the three elements of the cognitive theory. This match is not exclusively one way, and each factor seems like it can be part of more than one influential axis.

5.1. Conceptualizing Cognitive Theory and Privacy Behavior Factors

5.1.1. Privacy Behavior Factors

In our recent research on how privacy behavior is formulated, we found evidence that privacy behavior is affected by a variety of factors, including individual ones (e.g., demographics) and contextual ones (e.g., financial exchanges). We synthesized a framework that aggregates the scattered factors that have been found to affect privacy behavior. More specifically, we found that there are eleven dominant factors that, under the proper conditions, can influence privacy behavior [2]. We conducted a systematic review of 300+ published papers in high-quality journals such as journals from the Basket of Eight and journals with a citation index, as well as conferences recognized by the Association for Information Systems (AIS). The purpose of the aforementioned papers was to identify the variables that can influence privacy behavior. After conducting an in-depth analysis, we determined that eleven factors or clusters of factors are most likely to influence the privacy behavior of an individual. The factors that we found are demonstrated in Table 2

while the following picture represents our conceptual scheme from our previous research (figure 6).

Table 5. Privacy behavior factors.

Factor	Description
Financial/Non-Financial Exchanges/Benefits/Usefulness	A financial exchange is defined as an action that has an economic benefit as a result. As a non-financial exchange, benefit or usefulness is defined as an action that has a non-economic benefit.
Privacy Risk Perception	Privacy risk perception refers to a person's non-subjective evaluation of the likelihood of a potential privacy incident or event.
Trust/Control/Confidence/Fear	Trust refers to the belief in the reliability or credibility of a person, group, or party. Control refers to the ability of a person to manage situations or personal data. Confidence refers to the belief in a person of their abilities and skills. Fear refers to an emotional response to perceived danger, threat, or uncertainty.
Privacy Concerns	The user's willingness to share data and how these relationships in turn are affected by inter-individual differences in an individual's regulatory focus, thinking style, and institutional trust.
"Needs"/Psychological Engagement/Necessity	Psychological engagement refers to a person's experiences when engaging in an activity or process.
Sensitivity of Information	Sensitivity of information of a person refers to the degree of importance, confidentiality, or information that the person requires not to be public.
Privacy Awareness	Privacy Awareness refers to a person's understanding and recognition of the value and importance of the protection of personal information from disclosure.
Time-lapse	Time-lapse refers to the time between two or more events.
Education/Visualization/Interaction/Experience	Education refers to the process of acquiring knowledge and skills through an educational procedure such as school. Visualization refers to the creation of images or videos in order to represent data or information. Interaction refers

to the exchange of information or sputum response between two or more persons. Experience refers to the accumulation of knowledge and skills through events, incidents, and activities.

Demographics
(age/gender/country, political position, income, etc.)

Demographics refer to the statistical data and characteristics of a population or a group of people

Dimensionality/Complexity of Privacy Decision-making

Dimensionality refers to the number of variables that pull apart a phenomenon.

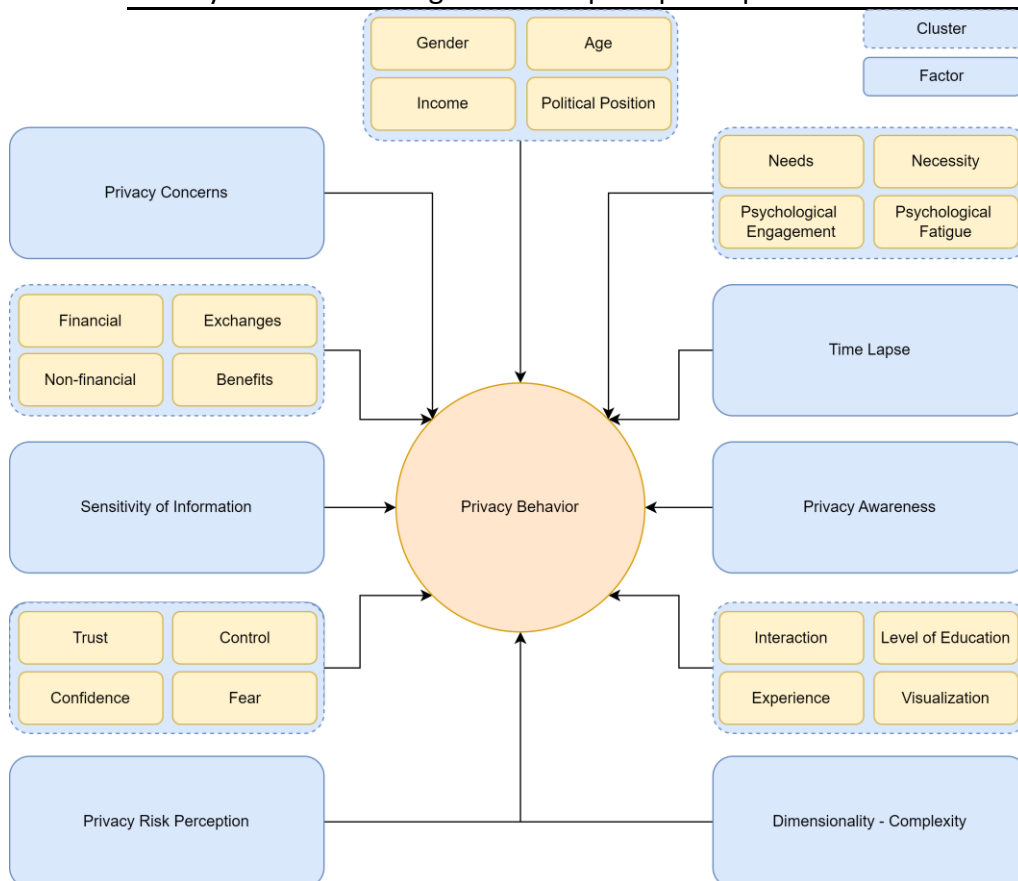


Figure 11. Conceptual scheme obtained using our previous research. In an aim to answer our second research question “How can we influence privacy behavior determinant factors to guide ICT users’ privacy behaviors using experiential methods?” we have first to connect the cognitive theory we analyzed above with our previous research results, which show that privacy behavior factors can influence someone’s privacy behavior. To achieve our goal, we will try to show the connection between the privacy behavior modification factors with the influential axes of the cognitive theory’s cognitive processes.

Before we conceptualize the cognitive theory and privacy behavior factors, we will set the matching criteria.

To set our matching criteria, firstly, we identify the variables we want to match from the fields we discussed that are also the most relevant to Research Question 2: “How can we influence privacy behavior determinant factors to guide ICT users’ privacy behaviors using experiential methods?”

From the privacy behavior field, there is one variable that the privacy behavior factors. On behalf of the cognitive theory model, we recognize the three influential axes that influence the cognitive processes: perceptions, beliefs, and attributions (productive causes). Secondly, we have to determine the method of matching. In academia, several methods have been proposed, including propensity score matching [2] as a means of reducing selection bias in observational studies, covariate matching [2,2], and nearest neighbor matching [2]. The methods are explained as follows:

The propensity score matching method was first proposed by Rosenbaum and Rubin [2] as a means of reducing selection bias in observational studies;

Covariate matching, also known as balance matching, aims to balance the distribution of covariates between the treated and control groups in observational studies to reduce confounding bias;

The nearest neighbor matching method is particularly useful when the number of variables is small. The method can be used in a variety of fields, including epidemiology, economics, and psychology, to estimate the similarities of the observed variables, close relationships of the observed variables, or the outcome of a statistical or medical experiment.

We have excluded the first two methods because they do not apply to our study. The nature of this research is not to observe different groups or persons nor to reduce the confounding bias between groups. We believe that the nearest neighbor method is close to the goals of this study. The dataset we have to match is relatively small while at the same time, this method is commonly used in psychology, philosophy, and sociology studies and experiments.

Based on the aforementioned considerations, we established the following criteria for our analysis:

Criterion 1: Etymological Similarity—this criterion pertains to the impact observed when an element of a cognitive theory exhibits congruence or similarity in meaning to a factor associated with privacy behavior.

Criterion 2: Similar Result or Definition—this criterion addresses the influence observed when an element of a cognitive theory and a

factor related to privacy behavior yield comparable outcomes or share similar definitions.

5.1.2. Beliefs

According to cognitive theory, beliefs affect the cognitive process and have two categories: Threat Perception and Behavioral Evaluation [2,2]. Each category has two subcategories. More specifically, the category Threat Perception includes the subcategories of Perceived and Perceived Susceptibility. The Behavioral Evaluation includes the subcategories of Perceived Benefits and Perceived Barriers. Below, we aim to align the identified privacy factors with the elements of the cognitive theory. According to Paspatis et al., [50], we argue that Financial/Non-financial Exchanges and Benefits are aligned with the subcategories Perceived Benefits and Perceived Barriers [2,2] because they correspond to both criteria 1 and 2. Both Financial/Non-financial Exchanges and Benefits have the same results on privacy behavior, and the subcategories of Behavioral Evaluation have the elements of Perceived Benefit for the Financial/Non-financial Benefits and Perceived Barriers as a similar result of the subfactor usefulness. At the same time, Perceived Benefits are aligned etymologically with the subcategory Financial/Non-financial Benefits. Respectively, the factor of Privacy Awareness matches the subcategory of Perceived Severity. Privacy awareness, as we presented in the photograph example in Section 3.1, can play a significant role in the perceived severity of a person. We argue that privacy-aware persons can better understand a potential danger and minimize the severity of their actions. The cluster of Demographics fits the subcategory of Perceived Susceptibility, which corresponds to criterion 2. This cluster contains elements such as age and gender. Research by Reynolds et al. [2] showed that the susceptibility of a person is affected both by age and gender. More specifically, females tend to post more often and with fewer privacy re-strictions on OSNs than males, while older users claimed to be more concerned with privacy; this is reflected in their posting practices. On the other hand, we believe Sensitivity of Information fulfills only criterion 1 due to the etymological similarity. All of the above is reflected in Figure 7. Table 3 presents our adaptations of privacy behavior factors to the cognitive process beliefs of the cognitive theory.

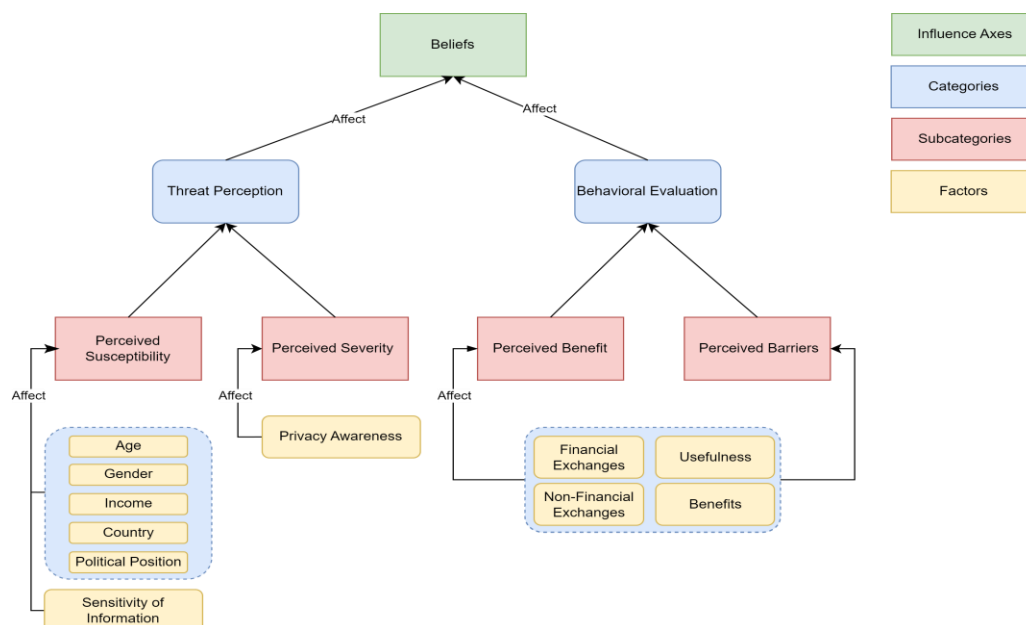


Figure 12. Element beliefs.

Table 6. Encapsulating how privacy behavior factors influence beliefs and thus cognitive processes.

How Privacy Behavior Factors Influence Beliefs and Thus Cognitive Processes		
Privacy Behavior Factor	Belief Element That Is Influenced	Fulfilled Criterion
Both Financial/Non-financial Exchanges and Benefits and Usefulness	Behavioral Evaluation: Perceived Benefits Behavioral Evaluation: Perceived Barriers	Criteria 1 and 2
Demographics	Threat Perception: Perceived Susceptibility	Criterion 2
Sensitivity of Information	Threat Perception: Perceived Susceptibility	Criterion 1
Privacy Awareness	Threat Perception: Perceived Severity	Criterion 2

5.1.3. Perceptions

Respectively, to the previous subsection, the cognitive processes contain two more categories, perceptions and attributions (productive causes). Following the same match criteria as the previous section, we argue that cognitive processes' element "perceptions" can be a match for at least the privacy behavior factors, privacy risk perception, and privacy concerns meeting criterion 2. As we mentioned in Table 1, privacy concerns are the willingness of a person

to share data and how these relationships in turn are affected by inter-individual differences in an individual's regulatory focus, thinking style, and institutional trust. The additional definition in psychology according to Cherry [2] is that perception relies on the cognitive functions we use to process information, such as utilizing memory to recognize the face of a friend or detect a familiar scent. Through the perception process, we can both identify and respond to environmental stimuli. We argue that concerns are philosophically in a close relationship with the cognitive processes' perceptions. Respectively, privacy risk perception seems to meet both the match criteria 1 and 2. Privacy risk perception is a perception relevant to the risk a person may confront while at the same time, the definition of cognitive processes' perception is the process or result of becoming aware [2]. As previously noted, we believe that privacy risk perceptions and the cognitive processes' element of perception are good candidates for a match, so we argue that etymologically is very similar to fulfilling criterion 1. Table 4 presents our adaptations of privacy behavior factors to the cognitive process' perception of the cognitive theory.

Table 7. Encapsulating how privacy behavior factors influence perceptions and thus cognitive processes.

How Privacy Behavior Factors Influence Perceptions and Thus Cognitive Processes		
Privacy Behavior Factor	Element that is influenced	Fulfilled Criterion
Privacy Concerns	Perception	Criterion 2
Privacy Risk Perceptions	Perception	Criteria 1 and 2

5.1.4. Attributions

Following the same matching criteria as above, we argue that the cognitive processes' element of attributions is a match for a variety of factors. As a definition, in social psychology, attribution is the process of inferring the causes of events or behaviors [2]. At the same time, it may describe the characteristics of a person usually without any awareness of any underlying process. On behalf of privacy behavior, we argue that the cluster of "needs, psychological engagement, and necessity" meet the matching criteria for both 1 and 2. Firstly, all of the factors of the cluster are from the field of psychology fulfilling criterion 2. Secondly, by etymology, the factor of psychological engagement fulfills criterion 2. Respectively, awareness is described by both cognitive processes' element of attribution by definition as well as from the part of privacy behavior's factor of privacy awareness. From the above, we argue that privacy awareness and the element of attribution awareness are fulfilling both criteria.

Continuing, we argue that from the side of privacy awareness, the factors of interaction and experience also meet our match criteria. As we mentioned, attribution is the process of inferring the causes of events or behaviors. We argue that both interactions can be the result of an event fulfilling criterion 2. Respectively, attributions may describe the characteristics of a person. We argue that the factor of experience is a characteristic of a person fulfilling criterion 2. Figure 8 presents the cognitive theory with the adapted privacy behavior factors. Table 5 presents our adaptations of privacy behavior factors to the cognitive process of attributions (productive causes) of the cognitive theory.

Table 8. Encapsulating how privacy behavior factors influence attributes (productive causes) and thus cognitive processes.

How Privacy Behavior Factors Influence Attributes (Productive Causes) and Thus Cognitive Processes

Privacy Behavior Factor	Element that is influenced	Fulfilled Criterion
Cluster: “needs, psychological engagement, and necessity”	Attribution	Criteria 1 and 2
Privacy Awareness	Attribution	Criteria 1 and 2
Cluster: Interaction/Experience/Visualization	Attribution	Criterion 2

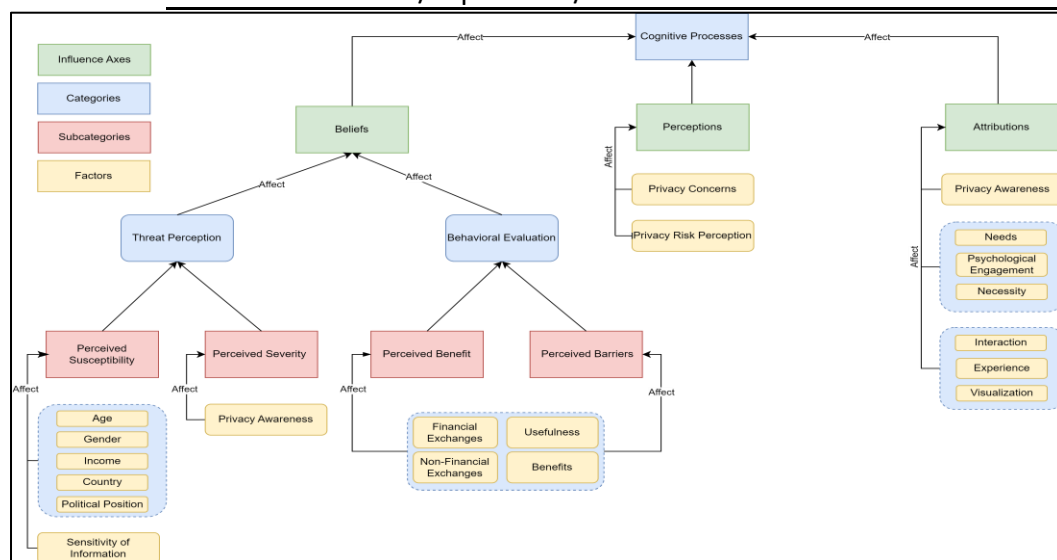


Figure 13. Cognitive theory with adapted privacy behavior factors.

6. Discussion

6.1. General Discussion

In our research, we have shown the use of cognitive theory in the field of information privacy behavior. We performed a literature review regarding relevant works and theories explaining behavioral transformation in the domains of sociology, psychology, philosophy, and health. This analysis demonstrated that significant work related to behavioral transformation was conducted in the field of health. Taking the results of the literature analysis into account, we put our perspective on the cognitive theory and health belief model, by integrating them with privacy behavior determinant factors. Our proposed integrated framework aligns the factors that have been identified to influence privacy behavior with the cognitive theory and health belief model.

Our literature review in Section 3.3 reveals that the experiential learning method is more beneficial for people than traditional learning. Aristotle set the starting line around 349 B.C.. Since then, many philosophers, psychologists, and sociologists were engaged to prove that experiential learning has advantages over the traditional way of learning and education [2,2,2,2,2,2]. In addition, as we described in Sections 3.1 and 3.2, cognitive theory [2] and the health belief model offer a proven approach to transforming someone's behavior [2,2,2]. With our work of conceptualizing privacy behavior determined factors with the cognitive processes, an element of cognitive theory creates a new optimistic frame of the research. With this model, we introduce not only experiential learning in the ICT environment but also which factors we should trigger to succeed in the privacy behavior modification of a person for the change to a more protective one.

6.2. Implications

Our proposed framework's potential implications can be divided into three categories: a) ICT users and individuals, b) organizations, and c) society. Individuals and ICT users can benefit from our proposed framework in multiple ways. ICT users can understand their behavior and can be enabled to make informed privacy decisions. As a result, our work can promote privacy protection skills as well as raise users' awareness of privacy risks associated with ICT usage. Finally, it can assist ICT users to gain better control over their valuable personal

information. Organizations can benefit from this framework by cultivating a privacy-conscious culture among employees and customers (i.e., users of online services). Organizations can improve their data protection practices via experiential learning privacy training, mitigate privacy-related risks, and build stronger relationships with their customers based on trust and respect for privacy. Finally, there are societal benefits to consider. A more privacy-conscious population can help to create a privacy-protective digital ecosystem in which privacy is valued and respected, which could have a positive impact on data protection regulations, privacy laws, and the overall privacy landscape.

Aside from the aforementioned implications, there are numerous research opportunities that arise from our proposed framework. Changes in privacy behavior is a field that still requires extensive research. Researchers may investigate the efficacy of various experiential learning methods, the role of psychological factors in privacy behavior change, and the long-term sustainability of behavior modification interventions. This framework has the potential to broaden current knowledge towards new research paths. For example, it highlights the benefits of broadening our knowledge by taking works in other fields such as psychology, sociology, philosophy, and health into account. Our proposed model provides a comprehensive view of the importance of experiential learning into privacy behavior enhancement while also inspiring further research by addressing the potential benefits and research opportunities and by encouraging interdisciplinary collaborations.

7. Conclusions and Future Work

Privacy behavior is a phenomenon that we have observed for more than 20 years, but it seems that there is more ground to cover to find new and more efficient ways to influence it. The traditional ways of teaching and educating are still present, but it seems they may not be the optimal way for privacy behavior transformation. Many researchers observed in the past that ICT users' privacy behaviors needs improvement [2,2,2], or else we may continue to confront phenomena such as "the privacy paradox" [2,2,2,2]. During our literature review in the fields of sociology, psychology, philosophy, and health, we found that the cognitive theory and the health belief model may offer an alternative method to understand ICT users' privacy behaviors and influence them towards a more protective one. Building on our previous research, on what factors affect privacy

behavior, we provided an integrated framework utilizing the cognitive theory and health belief model. We found connections between the majority of factors and the influential axes of the above theories, proposing a fertile model for more research on experiential privacy learning.

The proposed integrated framework can be used by researchers to design empirical experiments and experiential methods toward finding novel ways to trigger ICT users' protective behaviors. To the best of our knowledge, this is the first research that offers a solid theoretical background for privacy behavioral transformation using the cognitive theory and the health belief model. Our research may be beneficial to the academic community for facilitating privacy learning, for example, for elementary schools, academic institutes, and private schools offering new models of teaching with an aim to improve students' protective privacy behaviors. In addition, it may shift the attention of privacy academics offering new paths of research.

Our findings related to cognitive theory and the connection with our previous research on privacy behavior determinant factors are limited. Therefore, we aim to prove and improve our integrated model via empirical research, which will allow us to refine and propose a solid model for improving ICT users' privacy behaviors. Figure 9 demonstrates a preliminary illustration of our future conceptual framework. The six-phase framework is depicted in this diagram. Phase 1: choosing a multiple-choice questionnaire as a quantitative method to assess participants' current levels of privacy behavior. Phase 2: distribution and completion of the questionnaire by participants. Phase 3: selecting and presenting a small group of people for laboratory application of experiential methodologies. Phase 4: the creation of an experimental environment as well as the analysis and implementation of each selected experiential method. Phase 5: the implementation of the experiential model, cognitive processes, and experiential methods. Finally, Phase 6: the results of the previous phase are presented and discussed. All of the above phases are in an early stage and may change before final implementation. Its phases are divided into several parts depending on the type and duration of the phase.

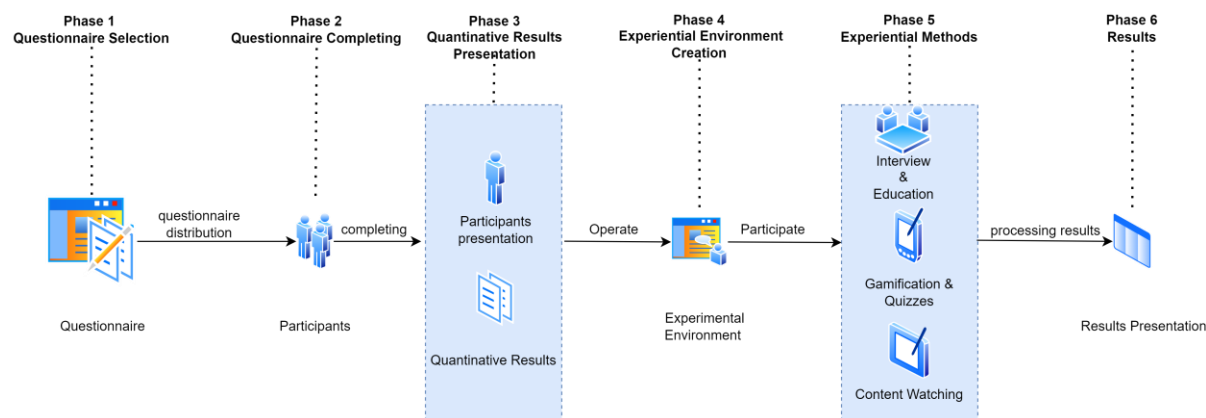


Figure 14. Capture of the experimental phases.

Our future research will be focusing on validating the aforementioned proposed framework. Specifically, we will employ the proposed framework and the aforementioned dominant privacy behavior factors during Phase 5 through empirical experiments, interviews, and assessments. Our experiments will take part in simulated as well as non-simulated environments, both online and on site, creating a favorable environment to be used in the future without any geographical restrictions.

This research received no funding.

Author Contributions: Conceptualization, Ioannis Paspatis. and Aggeliki Tsohou.; methodology Ioannis Paspatis.; formal analysis, Aggeliki Tsohou.; investigation, Ioannis Paspatis.; writing—original draft preparation, Ioannis Paspatis; writing—review and editing, Ioannis Paspatis and Aggeliki Tsohou.; visualization, Ioannis Paspatis.; supervision, Aggeliki Tsohou. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding; APC was funded by 100% discount from the Journal of Cybersecurity and Privacy.

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Menard, P.; Bott, G. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Comput. Secur.* 2020, 95, 101856.
- Shane-Simpson, C.; Manago, A.; Gaggi, N.; Gillespie-Lynch, K. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Comput. Hum. Behav.* 2018, 86, 276–288. <https://doi.org/10.1016/j.chb.2018.04.041>.
- Dhir, A.; Kaur, P.; Lonka, K.; Nieminen, M. Why do adolescents untag photos on Facebook? *Comput. Hum. Behavior.* 2016, 55, 1106–1115.

-
- Hinds, J.; Williams, E.; Joinson, A. It wouldn't happen to me: Privacy concerns and perspectives following the Cambridge Analytica scandal. *Int. J. Hum. Comput. Stud.* 2020, 143, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>.
 - Mathews-Hunt, K. CookieConsumer: Tracking online behavioural advertising in Australia. *Comput. Law Secur. Rev.* 2016, 32, 55–90.
 - Palos-Sanchez, P.; Saura, J.R.; Martin-Velicia, F. A study of the effects of programmatic advertising on users' concerns about privacy overtime. *J. Bus. Res.* 2019, 96, 61–72.
 - Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* 2017, 64, 122–134. ISSN 0167-4048. <https://doi.org/10.1016/j.cose.2015.07.002>.
 - Hallam, C.; Zanella, G. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput. Hum. Behav.* 2017, 68, 217–227.
 - Li, H.; Luo, X.; Zhang, J.; Xu, H. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Inf. Manag.* 2017, 54, 1012–1022.
 - Gerber, N.; Gerber, P.; Volkamer, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Comput. Secur.* 2018, 77, 226–261.
 - Paspatis, I.; Tsohou, A.; Kokolakis, S. How is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors. *Multimodal Technologies and Information (MTI)*. 2023, submitted.
 - Angst, C.M.; Agarwal, R. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Q.* 2009, 33, 339–370.
 - Acquisti, A.; Grossklags, J. Privacy and rationality in individual decision making. *IEEE Secur. Priv.* 2005, 3, 26–33.
 - Tsai, J.Y.; Kelley, P.G. Who's viewed you? The impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Boston, MA, USA, 4–9 April 2009; ACM: New York, NY, USA, 2014; pp. 2005–2008.
 - Johnson, D.G. Human-Computer Interaction: Psychology as A Science of Design. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, 3rd ed.; Jacko, J., Ed.; CRC Press: Boca Raton, FL, USA, 2013; pp. 3–18.
 - Conner, M.; Norman P (1993). Pros and cons of social cognition models in health behaviour, in *Health Psychology*. Update Volume 14, pages 24-31, 1993, https://fhs.thums.ac.ir/sites/fhs/files/user31/P_R_E_D_I_C_T_I_N_G.pdf (accessed on 30 May 2023).
 - Conner, M.; Norman, P. *Predicting Health Behaviour. Research and Practice with Social Cognition Models*; Open University Press: Buckingham, UK, 1996; pp. 1–22.
 - Jarvis, P. *Adult Education & Lifelong Learning*; RoutledgeFalmer: London, UK, 2004.
 - Dewey, J. *Experience and Education*; Macmillan: New York, NY, USA, 1938.
 - Freire, P. *Teachers as Cultural Workers—Letters to Those Who Dare to Teach*; Boulder, Westview Press, 100 pp., ISBN 0 8133. 2304-5 1998.
 - Kolb, D.A. *Experiential Learning: Experience as the Source of Learning and Developmen*. Pearson Education LTD. United States of America. ISBN-10: 0-13-389240-9; 1984.
 - Rogers, A. *Adult education*. Metaichmio Publications, Vol. 1 ISBN: 978-960-566-840-2. 1999.
 - Kokko, A. *Adult Education Methodology: Theoretical Framework and Learning Conditions*. Volume A. Patras: EAP. 2005.
 - Mezirow, J. *Transformative Dimensions of Adult Learning*; Jossey-Bass: San Fransisco, CA, USA, 1991.
 - Mezirow, J. Transformative learning and social action: A response to Inglis. *Adult Educ. Q.* 1998, 49, 70–72. American association for adult and continuing education: Sage publications.
 - Mezirow, J. On critical reflection. *Adult Educ. Q.* 1998, 48, 185–198. American association for adult and continuing education: Sage publications.
 - Mezirow, J. *Transformative learning*. Metaichmio Publications, Vol.1 ISBN: 978-960-455-226-9.2006..
 - Taylor, W.E. *The Theory and Practice of Transformative Learning: A Critical Re-View*. ERIC Clearinghouse on Adult, Career, and Vocational Education; The Ohio State University: Columbus, OH, USA, 1998.
 - Dacou, E. Educational Biography influences and determines the career path of adults. The case of educational institutions. *Hellenic Open University*. 2018. Available online: <https://apothesis.eap.gr/handle/repo/39397> (accessed on 29 January 2020).

-
- Gluck, M.A.; Mercado, E.; Myers, C.E. *Learning and Memory: From Brain to Behavior*; Worth Publishers: New York, NY, USA, 2016; p. 57. ISBN 978-1-319-15405-9.
 - Posner, M.I.; DiGirolamo, G.J. Cognitive neuroscience: Origins and promise. *Psycho-Log. Bulletin*. **2000**, *126*, 873–889. <https://doi.org/10.1037/0033-2909.126.6.873>.
 - Overskeid, G. Looking for Skinner and finding Freud. *Am. Psychol.* **2007**, *62*, 590–595. <https://doi.org/10.1037/0003-066X.62.6.590>.
 - Gardner Behaviorism and dynamic psychology: Skinner and Freud. *Psychoana-Lytic Rev.* **1979**, *66*, 253–262.
 - Pavlov, I.P. *Conditioned Reflexes: An Investigation of the Physiological Activity of the Cerebral Cortex*; Translated and edited by Anrep, G.V.; Oxford University Press: London, UK, 1927.
 - Weinman, J. Health Psychology: Progress, Perspectives, and Prospects, Current Developments in Health Psychology; Hardwood Academic Publishers: London, UK, 1990; pp. 9–33.
 - Koulirakis, Metalinou, Pantzou. *Sociological and Psychological Approach to Hospitals and Health Services*; Hellenic Open University Publications: Pátra, Greece, 1995.
 - Abramson, L.Y.; Seligman, M.E.; Teasdale, J.D. Learned helplessness in humans: Critique and reformulation. *J. Abnorm. Psychol.* **1978**, *87*, 49–74.
 - Cherry, K. What is Cognitive Psychology? The Science of How We Think. 2022. Available online: <https://www.verywellmind.com/cognitive-psychology-4157181> (accessed on 28 May 2023).
 - Ghosh, I. & Singh, V., (2017). Using cognitive dissonance theory to understand privacy behavior. Proceedings of the Association for Information Science and Technology. 54. 679-681. 10.1002/pra2.2017.14505401114.
 - Bandura. Self-efficacy: Toward a unifying theory of behavioural change. *Psychol. Rev.* **1977**, *84*, 191–215. DOI: [https://doi.org/10.1016/0146-6402\(78\)90002-4](https://doi.org/10.1016/0146-6402(78)90002-4).
 - Beck, A.T. *Cognitive Therapy and the Emotional Disorders*; International Universities Press: New York, NY, USA, 1976.
 - Rotter, J. B. Generalized expectancies for internal and external control of reinforcement. *Psychol. Monogr. Gen. Appl.* **1966**, *80*, 1.
 - Stroebe, W. *Social Psychology and Health*; Open University Press: Buckingham, UK, 1995.
 - Abraham, C.; Sheeran, P. The Health Belief Model in Conner and Norman, Predicting Health Behaviour. Research and Practice with Social Cognition Models; Open University Press: Buckingham, UK, 1995; p. 23-61.
 - Lewin. *Field Theory in Social Science*; Harper: New York, NY, USA, 1951.
 - Krstic. Journal of the Psychological Institute of the University of Zagreb, Zagreb, Croatia, 1964; pp. 7–13.
 - Hochbaum, G.M. Public Participation in Medical Screening Programs: A Socio-Psychological Study, Public Health Service; United States Government Printing Office: Washington, DC, USA, 1958.
 - Rosenstock, I. M. Historical origins of the health belief model. *Health Educ. Monographs*. **1974**, *2*, 328–335.
 - Becker, M.H.; Maiman, L.A.; Kirscht, J.P.; Haefner, D.P.; Drachman, R.H. The health belief model in the prediction of dietary compliance: A field experiment. *J. Health Soc. Behaviour*, Vol. 18, No. 4 (Dec., 1977), pp. 348-366 1977.
 - Anagnostopoulos, F.; and Papadatou, D. *Psychology in the Field of Health*; Ellinika Grammata Publications: Athens, Greece, 1995.
 - Jensen, C.; Potts, C.; Jensen, C.D. Privacy practices of Internet users: Self-report versus observed behavior. *Int. J. Hum. -Comput. Stud.* **2017**, *98*, 82–91.
 - Brown, R.; Brown L. *The Nicomachean Ethics*. Oxford; Oxford University Press: New York, NY, USA, 2009.
 - Boud, D.; Keohg, R.; Walker, D. *Reflection: Turning Experience Into Learning*; Kogan Press: New York, NY, USA, 2002.
 - Mavrogiorgos. Teacher Training: Other – Rivalry. Nicosia. https://www.pi.ac.cy/pi/files/keea/synedria/synedrio_pi_pdf_tel/7_Mavrogiorgos.pdf (Accessed 28 May 2023); 2009.
 - Freud, S. *Massen Psychologie und Inch Analyse*; Internationaler Psychoanalytischer Verlag G. M. B. H., Wien, Austria; 1921.
 - Koester, N.; Cichy, P.; Antons, D.; Salge, T.O. Perceived privacy risk in the Internet of Things: Determinants, consequences, and contingencies in the case of connected cars. *Electron. Mark.* **2022**, *32*, 2333–2355. <https://doi.org/10.1007/s12525-022-00522-6>.
 - West R. and Michie S. Embedding Covid-safe behaviours into everyday life through an enhanced risk management approach. <https://www.qeios.com/read/SPL9QE> (Accessed on 28 May 2023).

-
- Smith, J.; Johnson, A.; Davis, R. Privacy Lab: A Case Study of Experiential Learning in Privacy Education. *J. Priv. Educ.* **2018**, *12*, 145–162.
 - Johnson, M.; Anderson, L. Enhancing Privacy Education in Healthcare: A Case Study of Experiential Learning Approaches. *Health Inform. J.* **2019**, *25*, 1766–1782.
 - Brown, E.; Green, H. Engaging Students in Privacy Education: A Case Study of Experiential Learning in K-12 Settings. *J. Digit. Citizsh.* **2020**, *4*, 78–94.
 - Rosenbaum, P.R.; Rubin, D.B. Reducing bias in observational studies using subclassification on the propensity score. *J. Am. Stat. Association.* **1984**, *79*, 516–524.
 - Rubin, D.B. Estimating causal effects of treatments in randomized and nonrandomized studies. *J. Educ. Psychology* **1974**, *66*, 688–701.
 - Rubin, D.B. Estimating causal effects from large data sets using propensity scores. *Ann. Intern. Medicine.* **1997**, *127*, 757–763.
 - Holmes, C.C.; Adams, N.M. Likelihood Inference in Nearest-Neighbour Classification Models. *Biometrika* **2003**, *90*, 99–112. <https://doi.org/10.2307/30042022>.
 - Reynolds, B.; Venkatanathan, J.; Goncalves, J.; Kostakos, V. Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. In *Human-Computer Interaction—INTERACT 2011: 13th IFIP TC 13 International Conference, Lisbon, Portugal, 5–9 September 2011, Proceedings, Part III 13*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 204–215. https://doi.org/10.1007/978-3-642-23765-2_14.
 - Cherry, K. What Is Perception? Recognizing Environmental Stimuli Through the Five Senses. 2023. Available online: <https://www.verywellmind.com/perception-and-the-perceptual-process-2795839> (accessed on 30 May 2023).
 - Cherry, K. What Is Attribution in Social Psychology? 2022. Available online: <https://www.verywellmind.com/attribution-social-psychology-2795898> (accessed on 28 May 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Paper – III



+Article

Experiential Transformation in privacy behavior. A new framework for privacy behavior enhancement.

Ioannis Paspatis ^{1*} and Aggeliki Tsohou ¹

Citation: To be added by editorial staff during production.

Academic Editor: Firstname
Lastname

Received: date

Revised: date

Accepted: date

Published: date



Copyright: © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

¹ Ionian University, Department of Informatics, Corfu, Greece, 49100. 1; ipaspatis@ionio.gr; atsohou@ionio.gr

* Correspondence: ipaspatis@ionio.gr; Tel.: +30-26610-87760.

Abstract: Multiple researches have demonstrated that the conventional method of learning is suboptimal when our goal is to enhance individuals' genuine privacy behavior. This study introduces a framework for transforming privacy behavior, with the objective of enhancing individuals' privacy practices to a higher level of confidentiality. We performed an experiment on a limited number of persons to validate the efficacy of our suggested transformation framework. This framework combined determining aspects of privacy behavior with experiential behavior modification methodologies such as neutral stimuli (e.g. Cognitive Behavioral Transformation - CBTx), practical assessments and motivational interviews from other disciplines. While these methods have proven effective in fields like psychology and sociology, they have not yet been applied to the realm of Information Computer and Technology (ICT). In this study, we have effectively demonstrated the efficacy of the proposed framework through a five-phase experiment. The suggested framework has the potential to be advantageous for educational institutions, including both public and private schools as well as universities to construct new frameworks or develop new methodologies regarding individuals' privacy behavior transformation to a more protective one. Furthermore, our framework offers a conducive environment for further investigation into privacy behavior transformation methodologies.

Keywords: privacy behavior; privacy behavior transformation; privacy attitude, privacy behavior transformation framework.

1. Introduction

The recent advances in technology, such as internet-connected wearables, augmented reality, mobile devices, and the widespread presence of social media in our everyday lives, our singularity and individuality are constantly being put on display for the world to see [1]. Data can be obtained from individuals as well as businesses in a variety of different methods, and sometimes it happens even without our knowledge [2]. One way this can happen is via the gadgets that are connected to the Internet of Things (IoT) [3], and another is when we voluntarily expose ourselves on social networking sites such as posting a personal photo or other personal information. The provision of such advanced information services has triggered researchers to examine the phenomenon of privacy behavior. Privacy Behavior actions include personal information disclosure or the application of privacy-protective controls, or the configuration of privacy settings [4].

During the past ten years, there has been a discernible rise in the amount of studies conducted on understanding the factors that influence individuals' privacy behavior [5-9]. Researchers, software companies, companies that provide information security, and individuals are interested in findings ways

to improve the privacy behavior of information and communication technologies' (ICT) users. Despite the fact that many ICT users claim to be concerned about their privacy, research from a number of different studies has revealed that the same individuals nonetheless reveal a significant amount of personal information online. The term "privacy paradox" was coined to describe this situation by a number of scholars [5-8]. Self-disclosure of information may have negative consequences on our lives, such as becoming a victim of identity theft, impersonation, etc. Moreover, third parties may exploit this information for their own benefit, such as targeted advertising practices [10,11] or even affecting people's voting opinion [12].

A number of studies have been conducted in an effort to determine the elements that contribute to the psychological, sociological, and behavioral motivations of ICT users' privacy-related actions [5,6]. Numerous scholars have identified a range of factors that may have an impact on privacy behavior [7,8,13]. Consequently, by influencing these factors, it may be possible to influence ICT users' privacy behavior, including their tendency to disclose personal information, employ privacy-protective measures, or adjust privacy settings [7,8]. Although there exist many scattered privacy behavior models, literature misses an integrated framework that may effectively facilitate such change. In order to address this gap, in this paper we integrate existing privacy behavior determinants and we rely on experiential behavior transformation theories, so as to develop a novel experiential privacy behavior transformation framework towards enabling ICT users' privacy protective behavior. In summary, our paper addresses the following research questions:

Research Question 1: Can an individual's privacy behavior be transformed through experiential methods?

Research Question 2: Which experience method is more effective in transforming an individual's privacy behavior?

To address the above research questions, in this paper we suggest and validate the effectiveness of a novel privacy behavior transformation framework. This framework and its validation are consisted of an experiment that includes a variety of methods such as conducting questionnaires, interviews and applying behavioral transformation methodologies (such as experiential methodologies) as are described to the following sections. These theories and methods are based on concrete scientific theories and methods from other disciplines such as the cognitive behavior transformation methods.

After the introduction, this paper continues with the literature review on privacy behavior theories and privacy behavior determinant factors. In section 3, we investigate the theoretical background in experiential theories. In section 4, we propose our experiential privacy behavior transformation framework while in section 5 we provide our methodology to empirically test the proposed framework. In section 6 we present the results of our empirically tests. Finally, Section 7 concludes the paper and provides implications and future research.

2. Literature review

2.1 Privacy Behavior Theories

Two primary theories had been used for understanding privacy behavior, including the "privacy calculus theory" and the "privacy paradox." The "privacy calculus theory" suggests that individuals engage in a rational evaluation of costs and benefits when making decisions regarding their privacy [14]. Put simply, individuals assess the potential advantages of revealing their personal information in comparison to the potential drawbacks, such as the possibility of identity theft or discriminatory treatment. "The Privacy Paradox theory" refers to the discrepancy between people's stated privacy concerns and their actual privacy behavior [5]. For example, people may say that they care about their privacy, but they may still disclose a lot of personal information online.

Additionally, we encountered references to other theories, namely the "theory of privacy as a resource" and the "theory of privacy as a right". The perspective known as the "theory of privacy as a resource" posits that privacy is a valuable asset that may be leveraged to attain many objectives, including but not limited to social standing and financial benefits. As an illustration, individuals may have a propensity to divulge their personal information as a result of incentives, such as price reductions or complimentary merchandise. The perspective known as the "theory of privacy as a right" posits that privacy is an inherent and essential entitlement of individuals, which ought to be safeguarded against encroachments by both governmental and corporate entities. Many countries have vote laws to guard this right by suggesting directives such as OECD Privacy Guidelines or implementing laws such as the General Data Protection Regulation (GDPR) which is the regulation on data protection and privacy in the European Union [15], the corresponding Brazilian law [16] called General Data Protection Law Lei Geral de Proteção de Dados (LGDP), the Personal Information Protection Act (PIPA) in Canada [17] and Personal Data Protection Act (PDPA) in Singapore [18].

Each of these theories possesses distinct advantages and limitations. The privacy calculus theory provides a valuable framework for comprehending the various determinants that shape individuals' privacy-related choices. However, it falls short in acknowledging the emotional and social dimensions of privacy. The concept of the privacy paradox serves as a valuable framework for comprehending the incongruity between individuals' privacy-related behaviors and their expressed worries. However, it falls short in elucidating the underlying reasons for this disparity. Theoretical frameworks that conceptualize privacy as a resource offer insight into individuals' motivations for divulging personal information. However, these frameworks fail to fully acknowledge the inherent value of privacy as an independent and significant entity. Theoretical frameworks concerning privacy as a fundamental right play a crucial role in safeguarding privacy against encroachments. However, these

theories offer limited assistance in navigating the delicate equilibrium between privacy and other societal objectives, such as security or efficiency.

2.2 Privacy Behavior Determinant Factors

Previous studies have explored the determinants of privacy behavior, often employing pertinent theoretical frameworks, such as Protection Motivation Theory [19]. Other studies have investigated the variables that influence individuals' privacy behavior and developed relevant research models.

Many studies propose that gender significantly influences privacy behavior [20-24]. Their research indicated that gender significantly influences the extent to which individuals disclose personal information on the internet, with age being a contributing factor. As an illustration, women usually display a higher frequency of posting on their preferred social network and impose less limitations on privacy compared to men. The aforementioned studies are also incorporated into the research conducted by Paspatis et al. [13], who consolidated all of the factors determining privacy behavior into a single study. Other studies verify that age is also a contributing factor [8,20,21,25,26]. For example, it has been shown that as they grow older, adolescent males prefer to decrease the amount of information they share on online social networks (OSNs) and remove tags from their earlier photographs [27]. Further, relevant works have asserted that the perception of privacy risks [27-29] and their privacy concerns [30-37] also have a noteworthy impact on privacy-related behaviors. Another factor that appears to influence privacy behavior is the potential financial benefits or exchanges that individuals can obtain through the sharing of their personal data with providers. Previous research shows that individuals who state that they wish to protect their personal data, are willing to disclose personal information in contrast to those statements in case of financial or other non-financial exchanges. [30,38,39,25,40,41,33]. Financial and non-financial transactions (such as a monetary transaction involving personal data disclosure is the provision of a 10-euro advance or additionally, the usage of a mobile application game that advertises to be free of advertisements but necessitates the reveal of personal data) have the potential to influence individuals to overcome their concerns and willingly disclose their personal information to third parties, as well as agree to the terms and conditions presented to them [42,38,43,44,31,41,45]. Literature has also demonstrated that privacy behavior is influenced by the necessary disclosure of information to complete tasks or fulfill practical needs. For example, users are requested to present identification documents to an aviation company when traveling [46,30] or to provide medical records, such as a COVID vaccination certificate, for medical purposes [47]. The same may happen for psychological needs, such as psychological charging [46,48,35], such as when downloading a mobile application for entertainment purposes [49]. Furthermore, socialization needs (e.g., social media) may also drive personal information disclosure [34,35]. Other studies have examined the impact of education [50, 45], the

allocation of time for making privacy behavior choices [51, 52], and the use of visualization techniques [36, 51, 53] on privacy behavior.

Further to these works, previous research has attempted to aggregate the identified factors that affect privacy behavior in the literature [13, 54]. Factors that were found to determine privacy behavior include privacy concerns, privacy awareness, trust, demographics, and others. Additionally, previous research showed that some factors seem to affect privacy behavior more than others [13] while some factors affect privacy behavior directly or indirectly or with positive or negative way.

3. Theoretical Background

Experiential learning is an educational methodology that places significant emphasis on the value of acquiring knowledge through firsthand experiences, active involvement in practical tasks, and subsequent contemplation and analysis of those experiences [55]. The methodology suggests that individuals are more likely to gain knowledge, skills, and understanding in a more effective manner when they actively participate in and contemplate real-world events, as opposed to acquiring information passively inside the confines of a conventional classroom environment. Many researchers from the past until very recent claim that experiential learning is advantageous than traditional didactic approach [56-65]. According to Kolb [55] and Rogers [59] a person in order to learn through experience the following factors must be present:

- The participants must have the will to learn through the experience they lived;
- The participants should be able to reproduce the experience;
- The participants must have analytical thinking and understand the experience;
- The participants have the ability to make decisions and solve problems to create new ideas through the experiences they lived.

In addition, Boud [66] identifies the below three stages of reflective process in the context of experiential learning and recognize that this is a transformative process and the subjects can acquire new tendencies and abilities:

- The participant reviews the events and has the ability to study the experience again, calling this review a return to the experience;
- The participant recognizes the importance of the experience to third parties, through emotions;
- The participant discovers the new dimensions of the experience so that through it, the change in his behavior occurs and creates a new way of thinking and new abilities.

Researchers from a wide array of scientific domains, such as psychology, sociology, philosophy, and health sciences, have embarked on extensive investigations to explore the intricacies of behavior and experiential learning. Their studies have encompassed various experiential learning strategies, which have provided valuable insights into how individuals acquire knowledge and skills through direct experience. These studies have typically employed various experiential learning approaches, encompassing visual and audio stimuli such as the ringing of a bell (term in psychology classical conditioning), practical assessments (term in psychology operant conditioning), and motivational interviewing.

3.1 Neural and Neutral Stimulation

Neural stimulation, in the context of neuroscience and physiology, refers to the process of applying a stimulus to excite or activate neural tissue (neurons) in the nervous system [67]. The utilization of this form of stimulation is frequently employed in scientific investigations to examine neurological processes, explore the impacts of particular stimuli on neurons, or as a therapeutic modality within the domains of neurology and psychiatry. Neural stimulation encompasses various techniques, including electrical stimulation, magnetic stimulation, and optogenetics (neural stimulation). The latter use light as a means to activate genetically modified neurons. [67]. Numerous empirical studies have been undertaken in the field of psychology pertaining to the phenomenon of behavior transformation. Pavlov's classical conditioning experiment is widely recognized as one of the most renowned experiments in the field. [68]. Through his empirical investigations involving canines, the researcher successfully established a conditioned response in the subjects by pairing a neutral stimulus, namely a bell, with the presentation of food. Consequently, the dogs exhibited salivation alone in reaction to the bell, devoid of any food-related stimuli. Bandura conducted an additional behavioral trial. [69]. In his research, commonly referred to as "the Bobo Doll experiment," Bandura [69] demonstrated that youngsters who observed an adult engaging in hostile conduct towards the doll were more inclined to replicate the same aggressive behavior. Through this experiment, the researcher elucidated the notion of observational learning and its role in acquiring behavior through the process of observing others. Ainsworth's study [70] on attachment styles in infants explored the manner in which infants reacted to separations and reunions with their caregivers, within the framework of the same theoretical construct. This experiment facilitated the comprehension of how various parenting behaviors might influence the behavioral style of a child. The results highlighted the importance of a stable bond between newborns and caregivers in promoting positive emotional growth. In a separate study, Watson and Rayner [71] conducted an experiment to illustrate the potential of an auditory stimulus, specifically a terrifying noise, as a catalyst for behavioral modification. Their findings emphasize the capacity for behavioral change through environmental stimuli. Asch experiment [72] additionally employed an optical manipulation

to alter the observed behavior of participants. The study aimed to examine the degree to which individuals would comply to the opinion of a group, even when it contradicted their own personal judgment. The study involved the presentation of a basic perceptual task to the participants, which required them to assess line lengths. The participants were situated in an environment where they were exposed to confederates who intentionally provided inaccurate responses. The findings unveiled the significant impact of social conformity on individual decision-making, providing insight into the intricacies of human behavior in social settings. In the same context, Becker's [73] research delved into the labeling theory, which posits that individuals tend to engage in deviant behavior when they are officially or socially classified as deviant by authorities or society. This particular viewpoint centers on the influence of social reactions on human conduct.

3.2 Practical Assessments

Practical assessments encompass evaluation methodologies or exercises that necessitate individuals to exhibit their knowledge, skills, and competences through tangible tasks, real-life applications, or hands-on activities. The purpose of these assessments is to evaluate an individual's capacity to apply theoretical knowledge in real-world scenarios, effectively solve issues, and successfully execute tasks that are pertinent to a specific field or subject. [74]. Numerous strategies have been suggested within the realm of Information and Communication Technology (ICT) to alter privacy-related behaviors. These approaches encompass gamification techniques, privacy quizzes [75], and privacy simulators [76]. Practical evaluations adhere to Aristotle's renowned statement, which posits that the acquisition of skills is achieved via the active engagement in the respective activities. The concept of gamification for privacy behavior entails the incorporation of game-like components, such as incentives, obstacles, and rivalry, with the aim of motivating individuals to embrace and sustain privacy-oriented conduct in their digital engagements and online undertakings [75]. The process entails the utilization of game design principles to effectively engage and inspire users in making well-informed decisions pertaining to the safeguarding of their personal information, cybersecurity procedures, and compliance with privacy rules and regulations. In recent years, numerous approaches have been proposed or adopted. Mavroidi et al. [78] assert the possibility of gamification as a means to safeguard user privacy. The authors posit that the implementation of gamification holds potential in the realm of privacy education, as it may effectively inform users about privacy concerns, motivate them to adopt privacy-conscious behaviors, and enhance the appeal of privacy-protective features. In a separate instance, scholars conducted a study examining the utilization of game-based learning (GBL) in the context of information security (IS) and privacy education and awareness [79]. The authors suggest that game-based learning (GBL) possesses the capacity to serve as a viable method for instructing information systems (IS) and privacy principles, owing to its ability to captivate learners, foster interactivity, and stimulate motivation. Respectively, the work of Drozd and Kirrane also

supported these evidences [80]. In a separate study, the authors assert that game-based learning is a proficient method for educating individuals in technological domains, while also providing ample learning prospects for diverse target populations. The researchers asserted that the utilization of gamification in virtual reality escape rooms has the potential to enhance users' awareness of privacy matters [81]. On the contrary, gamification can also be utilized for evil purposes. Several studies suggest that the implementation of gamification carries inherent risks to user privacy. These risks include the possible exploitation of users' privacy, unauthorized collection of personal data, and the tracking of their online activities without their explicit authorization [82]. In an additional study [83] researchers discovered that individuals utilizing gamified services have a higher propensity to disclose personal information compared to those utilizing non-gamified services. The authors believe that the reason behind this phenomenon is the potential for gamification to induce cognitive absorption, thereby hindering users' capacity to make logical judgments regarding privacy.

Additional strategies that have been employed to alter privacy-related behaviors include the utilization of privacy simulators and privacy quizzes. Privacy simulators are software tools or systems that have been specifically designed to replicate and represent different facets of data privacy. These simulators are commonly used for teaching, testing, or research reasons. Simulators are utilized to generate synthetic data or scenarios that replicate real-world privacy difficulties, enabling users to enhance their comprehension and assessment of privacy threats, compliance with data protection legislation, and the efficacy of privacy-enhancing methods. As an illustration, Bum et al. [76] devised a simulator aimed at enhancing individuals' awareness of privacy matters and facilitating their comprehension of the privacy consequences associated with their online behaviors. In a separate study, the researchers developed a simulator for mobile security and privacy. This simulator allows for the simulation of mobile entities and their surrounding environment, facilitating the investigation of security and privacy concerns [84]. The authors asserted that simulation can be employed to assess privacy dangers and countermeasures using numerical analysis and visualization, enabling a more comprehensive understanding of the ramifications and privacy threats faced by users. Privacy quizzes are interactive evaluations or surveys created to check an individual's comprehension and familiarity with concepts, principles, legislation, and optimal approaches pertaining to privacy. The quizzes commonly have a range of question formats, including multiple-choice, true/false, and open-ended, which encompass diverse dimensions of data privacy and security. Privacy quizzes are frequently employed as pedagogical instruments, instructional modules, or consciousness-raising initiatives to enable individuals and entities to assess their proficiency in matters of privacy and discern domains that necessitate enhancement. In their study, Leenen and van Vuuren [75] asserted that privacy quizzes serve as a means to encourage secure online conduct and represent an efficient and cost-effective approach in aiding the military community in the prevention and detection of online threats.

3.3 Motivational Interviewing

Motivational Interviewing (MI) is a counseling technique and communication method that prioritizes assisting individuals in examining and resolving their conflicting feelings regarding modifying their behavior. This approach demonstrates notable efficacy within circumstances characterized by persons who exhibit resistance or reluctance to modify their behaviors, such as addiction treatment, healthcare, and mental health counseling. Motivational interviewing (MI) is a therapeutic approach that encompasses the utilization of active listening, empathy, and non-confrontational questioning techniques. These strategies are employed to facilitate individuals in recognizing their own motives and aspirations for personal transformation, hence enhancing their preparedness to initiate behavioral change [85]. Motivational interviewing (MI) can be integrated with other behavioral modification techniques, such as cognitive-behavioral therapy (CBT), in order to enhance the efficacy of interventions aimed at promoting behavior change [86]. The aforementioned methodologies are commonly employed in the disciplines of psychology and sociology to effectively tackle a range of behavioral issues, including but not limited to anxiety disorders and eating disorders. [86]. In recently, there has been an emergence of a novel variant of cognitive behavioral therapy known as cognitive behavioral transformation (CBTx), which has begun to be employed in practice. Cognitive Behavioral Therapy (CBT) places emphasis on facilitating individuals in the process of modifying their fundamental beliefs and assumptions. CBTx operates under the premise that our fundamental ideas and assumptions regarding ourselves, the world, and others exert a significant influence on our cognitive processes, emotional experiences, and behavioral patterns. The existing body of literature on CBTx is still minimal. However, certain tests undertaken with CBTx have reported positive outcomes in terms of attitude, well-being, and learning. [87-89].

3.4 Choice of research method

As we demonstrated in this section, experiential methods offer more benefits than traditional learning and education [55-58]. Based on the fact that the cognitive model was created by the field of psychology, this field considers the monitoring of the individual's phlegmatic response such as facial expressions and emotion recognition and the recording of the individual's personal narratives to be extremely essential [90]. A person who is able to verbally or physically convey an emotion may have trouble expressing it in writing or require assistance or a reward from the researcher [91-94]. At this juncture, the researcher records both the participant's possible written or verbal response to a question as well as their physical reaction. This response may be identical to the participant's or completely different. During the literature review of the fields of the sciences of psychology,

philosophy, and sociology, the methods that were followed by the vast majority were field research and analysis based on qualitative methods, as each individual may exhibit a completely different behavior than another individual despite having the same or similar characteristics [55-57, 61-64]. Numerous factors, such as socio-cultural approaches, social milieu, previous experiences, economic status, etc., can influence a person's behavior, so demographic characteristics are not the only focus in the field of psychology. We chose the qualitative research methodology for the aforementioned reasons and because the premise of the experiment is the proof of experiential methods of learning and education against the dominant model.

4. The proposed experiential privacy behavior transformation framework

Section 3 has elucidated that behavior can be modified by many methods and stimuli. In the realm of psychological experimentation, researchers frequently employ neutral stimuli, such as noises and visual effects. Conversely, within the fields of sociology, health, and psychology, motivational interviews are commonly utilized in conjunction with Cognitive Behavioral Therapy (CBT) and CBT-based theories. In contrast, within the field of information technology, practical methods such as practical assessments and gamification approaches are predominantly employed for the purpose of transforming privacy behavior. In this section, we present our framework for transforming privacy behavior, based on the literature review and the theoretical background presented above.

As stated in the literature review, prior studies have endeavored to consolidate the factors that are mentioned in existing literature as determinants of privacy behavior [13, 54]. In these works, the researchers examined the relationship between determinant elements of privacy behavior, such as fear and financial-non financial exchanges, and the influential axes of the cognitive theory, namely beliefs, perceptions, and attributions. Further, as described in Section 3, experiential learning approaches include visual and audio stimuli, practical assessments and motivational interviewing. Therefore, our framework will encompass neutral stimuli, practical assessments and motivational interviewing with regards to their efficiency to transform individuals' privacy behavior.

We define two types of neutral stimuli, namely short-length visual content and long-length visual content regarding privacy behavior. We define three types of practical evaluations: a) privacy behavior quizzes, b) privacy behavior simulators, and c) privacy behavior gamification methods. We consider motivational interviews to assess privacy outcomes related to meta-data mobile phone monitoring and google account monitoring from the side of privacy related incidents. The aforementioned concepts are depicted in Figure 1.

Due to the fact that in addition to experientialism, our model also incorporates training on increasing the perception of risks and questions on the results of our experiment's questions, a qualitative method rather than a quantitative one was chosen for the experiment. The experimental design is also a consideration when selecting a qualitative technique. Due to the fact that the individuals will be monitored with our own apparatus, it was necessary to have physical access to them. In a later phase of the experiment, each participant will undergo an interview and training phase at the same time as they progress through the experience's stages.

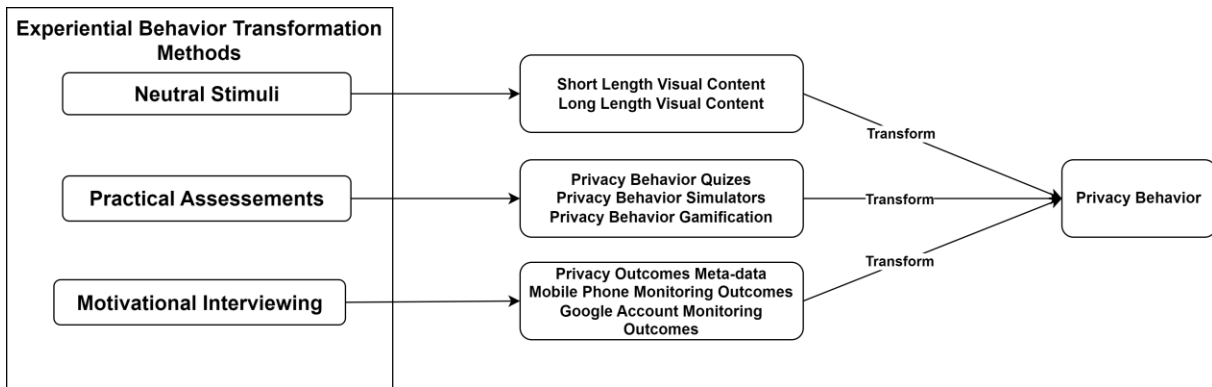


Figure 15. Experiential privacy behavior transformation framework.

For the design of the empirical research, we will adopt observation and behavior techniques witnessed in psychology and sociology. As mentioned in section 3, these techniques are conducted qualitatively by employing narrative interviews and field research. The primary reason for this choice is that the researcher aims to observe the participant's reaction and response. In relevant empirical studies the researcher places participants in dilemma situations and observes the initial reaction to chain questions and how behavior changes over time.

5. Methodology to Empirically Test the Proposed Framework

In this section we present the validation methodology of our framework, which comprises five phases. We describe and analyze every phase of the methodology to validate the proposed behavioral transformation framework, including the respective scope and target per phase.

We adopted a multiple stratification methodology to empirically test our proposed framework. As demonstrated in Paspatis et al. [13], privacy behavior is influenced by a variety of factors. Similarly, Paspatis and Tsohou [54] show that the cognitive processes of privacy behavior are influenced by three cognitive axes of influence, with each axis being influenced by a distinct set of factors, which are sometimes present in two or three axes.

Our methodology to test our framework is divided into five phases as described below:

- Phase 1: Creation of qualitative questionnaire with multiple-choice and open-type questions to assess users' privacy behavior
- Phase 2: Implementation of privacy behavior measurement using the methods derived from phase 1 in a small, closed group of up to 10 individuals.
- Phase 3: Creation of the experimental environment per experiential method (i.e., neutral stimuli, practical assessments, motivational interviews).
- Phase 4: Implementation of the experiential experiment aiming towards privacy behavior transformation
- Phase 5: Analysis of results with regards to the success of behavioral transformation

The above phases are illustrated in the figure below (figure 2).

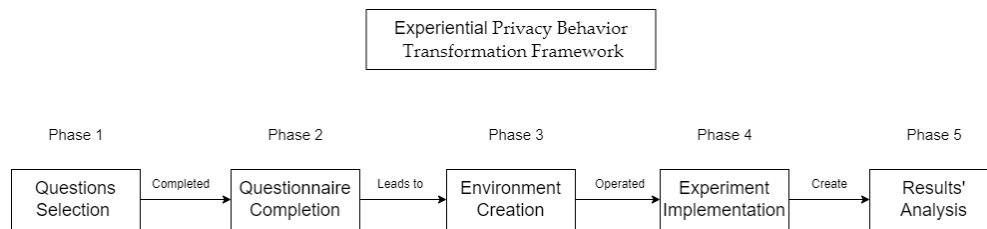


Figure 16. Capture of experimental phases

5.1 Participants' selection criteria and profile

People from our broader social milieu and outside our sphere of influence were chosen for the experiment. In order to enlist the volunteers, we conducted a thorough search throughout our wider surroundings. The selection criteria primarily consisted of three factors: unfamiliarity with the participants to prevent any bias, no personal connections such as family, academic affiliation, or university enrollment to maintain impartiality, and being an adult to meet the requirements for signing the consent form to participate in the experiment. The majority of the participants were recruited using the "friends of a friend" tactic. Individuals were selected using a stratified method. Specifically, we selected participants from as wide a range of age, gender, educational level, and occupation. We made a deliberate effort to ensure an equal representation of both genders, with participants having varied occupations. Additionally, each participant had a minimum age difference of 5 years from others, regardless of gender. The objective of the stratification method was to assess the effectiveness of the framework in all

conceivable combinations. Although more than 20 individuals initially expressed interest, some withdrew due to privacy concerns after receiving additional information. When we informed the participants about the duration of the experiment and the amount of effort required some of them revoke their willingness to participate.

Every participant signed an analytical consent form in order to engage in the study. In addition to the consent form, all participants received additional information regarding the experiment, which may not have been extensively covered in the consent form. This information included an analytical overview of the experiment as well as any anticipated advantages for the participants, researchers, and society. The consent form and the experiment adhered to the ethical standards of our institution and followed Cope's best practices [92]. Initial interest was expressed by 22 individuals, 9 women and 13 males. After withdrawals and exclusions, four women and five men were ultimately chosen. The participants' age ranged from 26 to 62, with a mean of 40.89 years, a median of 36 years, and a standard deviation of 11.33 years. Despite the large age range of 26 to 62 years, the sample's mean value was relatively close to the sample's mean, as indicated by the standard deviation. We can conclude from the above that our sample is representative of this value range. Four people had a university education, two women and two men, of which two had a master's degree; three people had a technological education, two women and one man, of which two had a master's degree; and two people had a complete secondary education, one woman and one man, of which one has a qualification. Three participants held bachelor's or master's degrees in information technology. Participants' profile is presented in table 1.

Table 9. Profile of participants

Participant Number	Index	Gender	Age	Education	Occupation
Participant -1	CD	W	47	University Education	Philologist
Participant -2	PE	M	36	University Education	Police officer
Participant -3	NB	M	46	University Education	Military
Participant -4	DS	W	50	University Education	IT
Participant -5	PM	M	62	University Education	Refrigerant
Participant -6	PW	W	36	Technological Education	Technologist
Participant -7	AA	M	36	Technological Education	Technologist
Participant -8	AE	W	29	High School	Employee
Participant -9	TE	M	26	High School	Employee

Total: 9		AVG = 40.9y	MD = 36y	SD = 11.33
----------	--	-------------	----------	------------

5.2 Phase 1. Creation of qualitative questionnaire to assess users' privacy behavior

In this phase, a qualitative questionnaire was created to assess participants' current privacy behavior. The purpose of this questionnaire is to assess the current (pre-study) privacy behavior of the participants who will be involved in the experiment. The participants were asked to complete again the same questionnaire after the experimental process, so that we can compare the pre- and post-evaluations. The questions of the questionnaire are presented as Appendix A2.

Each question was selected after comprehensive research in academic journals such as the basket of eight and google scholar search engines. The questionnaire inquiries were derived from a collection of articles on privacy-related behavior. Regarding the questionnaire, each question may appear in more than one of the selected questionnaires. Each question may not be presented verbatim, but its core meaning or purpose remains the same as other questions with similar wording. In addition, each question was selected so that it could be used as a variable in our conceptual model for further analysis, while also being associated with at least one of the influencing factors of privacy behavior identified in our previous research [13]. Additionally, each selected question was modified to be asked as open question due to our qualitative process but it is also could be rated on a 5-point Likert scale ranging from "Very often" to "rarely." Thus, if a question was in 7-point Likert form then the two extreme values on a 7-point Likert scale were merged with the preceding value. For instance, "Too often" and "Very often" have been merged into "Very often."

Further, we matched each question with at least one influencing factor of privacy behavior as they emerged from the work of Paspatis et al. [13]. For the sake of convenience each factor matched to an acronym as they are appearing to table 2. As matching criteria, we used the "nearest neighbor" methodology as they emerged from our previous research [54]. The nearest neighbor matching method is especially advantageous when the number of variables is limited. This method is applicable in various domains including as epidemiology, economics, and psychology. It is used to assess the similarities between observed variables, the close correlations among observed variables, or the outcome of a statistical or medical experiment [93].

The below table 2 demonstrates the acronyms of its affected factor or cluster of factors while table 3 demonstrates the questions and the number of the articles that these were engaged as well as the affected factor(s).

Table 10. Privacy Behavior Factors obtained by Paspatis et al., (2023)

Factor or Cluster	Acronym
Financial Exchanges/benefits/usefulness	FEBU
Privacy Risk Perception	PRP
Trust / Control/confidence/fear	TCCF
Privacy Concerns	PC
“Needs”/ psychological engagement / necessity	NPEN
Sensitivity of information	SOI
Privacy Awareness	PA
Time lapse	TL
Education/Visualization/Interaction/ Experience	EVIE
Demographics	DE
Dimensionality/Complexity of a privacy decision making	DC

Table 11. Questionnaire to assess users' privacy behavior

Activated Factor	Question	Number of Articles
PA	Q1: How often do you check the privacy settings on your social media accounts?	5
TCCF, PRP, PC	Q2: How often you felt like your privacy was violated online?	5
PA	Q3: How often do you read the privacy policies or terms of service for the websites or apps you use?	5
PA, PC	Q4: Have you ever declined to use a service or app because of privacy concerns? If so, can you describe the situation (open)?	5
PA, PC	Q5: How often do you use different passwords for different accounts? How do you keep track of them (open)?	4
TCCF	Q6: Have you ever been a victim of identity theft or online fraud? How did that experience affect your privacy behaviors (open)?	4
PRP, PA	Q7: How much personal information do you share online? Can you describe the reason (open)?	5
PA	Q8: How often do you take steps to protect your online privacy? Do you use ad-blockers or other tools and which (open)?	4
PRP, TCCF	Q9: Did you know companies collecting and using your personal data for targeted advertising?	5
PC	Q10: Do you have any concerns about government surveillance or monitoring of your online activities?	3

5.3 Phase 2. Implementation of privacy behavior measurement

To conduct the qualitative questionnaire, we used mixed methods. Due to some participants' educational level and/or computer skills familiarity four of the questionnaires were completed with the help of the researcher on a physical meeting in most cases; when this is not possible due to distance or time limitations the meeting was conducted online. Prior to distributing the questionnaire, we notified the participants that all their personal data and identifiers will be anonymized. The purpose of this option is to convince respondents that they cannot be identified so that they will answer the questions more truthfully. Murdoch [95] found that people who assume they cannot isolate themselves from the results of a survey are approximately nine percent more likely to participate and to provide the most accurate response possible. Thus, for the same reason we did not reveal how many people participated.

5.4 Phase 3. Creation of the experimental environment per experiential method

We devoted a big effort to create an experimental environment to cover both our specifications but also create a nice and full anonymized experience for the participants of the experiment. We emphasized on making the participants feel comfortable and secure about their privacy and their personal data. We were also transparent for our methodology to mitigate any of their privacy concerns. Due to page limitations, we will not go in detail about our infrastructure. In summary, our experimental environment is consisted of the following components key components:

- One central and 9 client gmail accounts (IonianUniversityLab@gmail.com, ionianuniversitylabvictim1-9@gmail.com,
- virtual machines,
- multiple streaming platform accounts accounts with legal, secure and anonymized way,
- and finally, other applications (e.g., Family Link, Viber, Streaming Platform App etc.).

The Gmail accounts were used with the build-in app “find my device” and were remotely installed to participants' phones (more information to the next subsection) along with other necessary applications such as family link and Viber. To establish a secure, anonymous, and legally compliant visual content environment, we implemented a privacy protocol that incorporates several levels to enhance privacy. These layers include a VPN browser plugin,

temporary email services, and crypto-cards. The aforementioned approach was implemented to guarantee anonymity for both us and the participants. Conversely, the goal of the streaming platform service is to offer a lawful means for our participants to access privacy-related content we selected. The multi-layer anonymity procedure we followed is pictured to the following figure 3.

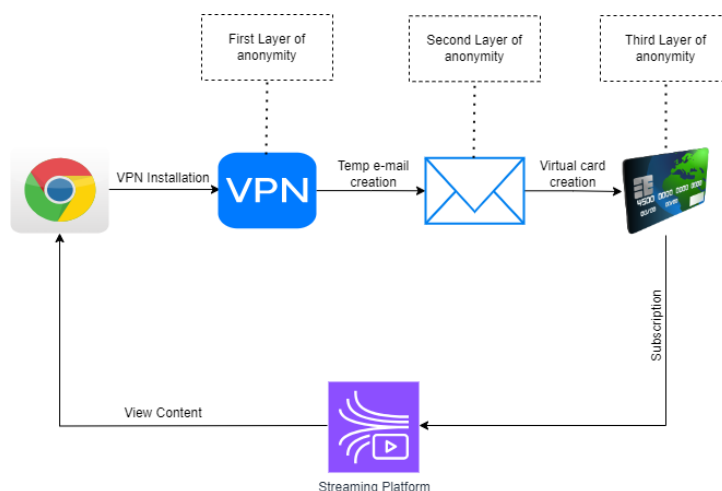


Figure 17. The multi-layer anonymity procedure

5.5 Phase 4. Implementation of the experiential experiment aiming towards privacy behavior transformation

As we analyzed in section 3 and 4, privacy behavior can be transformed mainly using three methods (content viewing, practical assessments and one-to-one motivational interviews), with neutral or visual stimulus, by practicing and by external motivation speeches such as motivational interviews. In our experiment, we included all three methods in order to test our framework.

In the following we describe the three experiential procedures that we followed. During the experimental period we gave to the participants a two-sim card mobile android phone. The participants used the one sim slot for the sim-card that belong to us and the second sim slot could be used for own sim-card, if selected. We opted for this choice to avoid making them uncomfortable by carrying two smartphones (own and experiment) and because we expect that this would allow them to use the experimental phone to the maximum. All participants were part of all three experiential procedures, content viewing, practical assessments and one-to-one motivational interview. We provide more details about the experimental procedures in Appendix C. Due to the lack of multiple experimental mobile devices and sim cards, we included the participants sequentially and not in parallel (so that the same phones could be used by several participants).

After the execution of the two of the experiential procedures (content watching and practical assessments) we gather all the information in order to construct the material for the motivational interview. Motivational interview is our final part of the experiential methods that the participants taking part.

5.6 Phase 5. Results analysis and framework validation

This phase includes the analysis of the experiment data to investigate if behavioral transformation was successful.

First, we re-executed the questionnaire of phase 1 and compared the data with the ones from phase 4, per participant, to assess if self-reported behavioral transformation was successful. In this step we gathered the results of the first questionnaire and we compared them with their last answers in order to calculate if their privacy self-reported behavior changed and how much is changed. To calculate the difference, we weight the responses from the first and second questionnaires into 5-point Likert-type scores and perform two-stage ANOVAs [96] as well as Cronbach's A-tests [97].

Second, to assess participants' actual privacy behavior transformation we asked participants to be re-monitored but for a smaller period of 10 days. This way, we can collect information about actual privacy behavior and compare with the data that we collected during phase 4, so as to assess if actual privacy behavior was transformed. The decision to reduce the re-monitoring stage to 10-day duration instead of 30 days was taken due to resource constraints. As previously stated in section 5.5, multiple participants utilized the same mobile phones due to a scarcity of available experimental devices. In order to expedite the re-monitoring process, we decided to reduce the duration from 30 days to 10 days. The re-monitoring was conducted utilizing identical procedure, tools and equipment as the initial 30-day period.

For the sake of completeness in Appendix C we provide all the content and the items we used in our framework.

6. Results

This section provides the results of our empirical study.

6.1 Pre-Study privacy behavior assessment

We utilized Google Forms to create and disseminate questionnaire A1. The selection was made based on the speed at which a form could be generated, the simplicity of distributing it, and the ease of processing the data. As previously stated, 9 people participated. The questionnaire was distributed to our participants through various channels, including email, a

hyperlink, and direct messages on the social media platforms Facebook (Meta) and Viber. Hence, we notified the participants that they are required to finalize the questionnaire within a period of 10 days. Participants who were unfamiliar with the Google Forms platform or lacked the necessary technological skills were provided assistance by scheduling an appointment with our team. At last, all nine participants have successfully submitted the questionnaire.

The results were initially examined using a two-factor quantitative ANOVA approach without replication. We choose the ANOVA approach due to its recommendation for situations where there are several factors that influence an independent variable. As we have seen in Chapter 2, there are a total of eleven determine factors in our instance. Furthermore, ANOVA is suggested for assessing multiphase techniques, as we will perform in our specific situation. The Cronbach's Alpha technique was utilized to assess the validity of the questionnaire. Due to the limited number of participants ($n=9$), this approach was used as it is considered the most straightforward technique for testing a questionnaire. Furthermore, as the objective of this questionnaire is not to extract or elucidate any phenomenon, but rather to compare the outcomes prior to and following the experiential transformation, we have concluded that more intricate quantitative analysis methodologies are unnecessary. However, the results are primarily presented for the sake of comprehensiveness and also for potential statistical analysis in the future, either by the current researchers or other scholars. Regarding the descriptive results, it was evident that all participants consistently exhibited risky privacy behavior across all questions, with an average score of 4.09. This suggests for example that privacy settings are seldom or rarely modified, or that the participants have a low level of privacy-conscious behavior. Table 4 presents the overall and individual question averages. Concerning the implementation of the ANOVA, it is evident that the participants' responses to each query do not exhibit a statistically significant disparity ($F = 1.19$, $P\text{-value} = 0.31$, $p=0.5$), despite a considerable likelihood of inaccuracy. On the other hand, each person shows a pretty little difference for each question ($F = 3.57 > F\text{ critical } 2.07$, $P\text{-Value} = 0.001$, $p = 0.05$). The ANOVA analysis outcomes are presented in Table5 5. Cronbach's application demonstrated a performance validity of 0.71961223 (table 6). The questionnaire responses are considered adequate and reliable, as demonstrated in Tables 4-6.

Table 12. Participants' answers

<i>Participant</i>	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Avg
Participant 1	5	5	4	5	5	5	5	4	5	5	4.80
Participant 2	4	5	4	5	4	4	5	4	5	4	4.40
Participant 3	5	5	4	5	5	5	5	4	5	5	4.80
Participant 4	2	4	4	5	4	2	4	4	5	4	3.80
Participant 5	5	4	4	5	3	5	4	4	5	3	4.20
Participant 6	5	3	3	5	5	5	3	3	5	5	4.20
Participant 7	4	3	5	4	4	4	3	5	4	4	4.00
Participant 8	4	5	2	4	3	4	5	2	4	3	3.60

Participant 9	3	5	1	1	5	3	5	1	1	5	3.00
Total Average	4.11	4.33	3.44	4.33	4.22	4.11	4.33	3.44	4.33	4.22	4.09

Table 13. ANOVA's summary table.

ANOVA						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Rows	26.48889	8	3.311111	3.566489	0.001557	2.069832
Columns	9.955556	9	1.106173	1.191489	0.313744	2.012705
Error	66.84444	72	0.928395			
Total	103.2889	89				

Table 14. Cronbach's Alpha Internal consistency matrix

Cronbach's Alpha	Internal consistency
$0.9 \leq \alpha$	Excellent
$0.8 \leq \alpha < 0.9$	Good
$0.7 \leq \alpha < 0.8$	Acceptable
$0.6 \leq \alpha < 0.7$	Questionable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable
Participants' Score:	0.71961223

6.2 Monitoring Results

During the initial phase, participants were provided with a phone that was accepting two SIM cards simultaneously. As previously said, we closely observed the participants using various methods for a duration of 30 days. Throughout this duration, we effectively observed and tracked all individuals involved. To obtain the mobility and location data of each participant and effectively analyze them, we retrieve all the accessible information. To accomplish this, we initially attempted to utilize the Google Takeout service. However, we encountered various problematic issues, such as the inability to pick certain date and time ranges. To address the issue mentioned above, we employed a bespoke Python script that leveraged the cookies of the participants. Through the surveillance of Viber's desktop sqlite database, in conjunction with findmydevice, we have effectively obtained data on participants' daily routines, including their place of residence, workplace, preferred WiFi hotspots, and real-time position tracking. We effectively

utilized the GPX file data from sports apps like Strava and Endomondo to extract information about participants' hobbies, preferred sports locations, and GPS data. It should be noted that GPX file data is accessible to anybody on the mentioned platforms, provided that the platform user has not protected it by modifying the privacy settings. It is important to note that none of the participants chose to uninstall any pre-installed applications, despite being informed of their ability to do so. We will utilize some of the aforementioned processed data as proof and as a means to enhance awareness during the Motivational Interviews in the experiential procedure-3.

6.3 Experiential Procedures

6.3.1 Experiential Procedure – 1. Content viewing

Throughout the phone-monitoring period, all participants were required to access the privacy behavior content that we had provided on the chosen streaming platform and other media platforms. In order to ensure the viewing of content, we closely watched the content history area of each platform. Based on the information provided, we can confirm that all participants were exposed to the instructed content. However, it is not possible to verify this with certainty, as the participants may have initiated the media content and subsequently discontinued their engagement. In order to enhance obedience, we incorporated additional content-related questions into the motivational interview process.

6.3.2. Experiential Procedure – 2. Practical Assessments

At this point, the participants were required to select and utilize at least one item from each category, including privacy-related tests, privacy emulators, and privacy-related games. In addition, they were required to upload a minimum of one photograph to their chosen social media platform. In order to assure compliance, the participants were required to provide their personal scores for each practical assessment tool they selected. Each participant could select multiple tools from each category, but just one tool should be chosen as the minimum requirement. The privacy-related meta-data, if available, will be utilized in the Motivational Interview Procedure. The time frame to complete all of the aforementioned tasks was identical to the previously mentioned 30-day period.

6.3.3 Experiential Procedure – 3. Motivational Interviews.

In this section, we initially provided our monitoring findings to each participant individually, as indicated in section 4. The objective of this activity is to demonstrate the extent of personal information that may be obtained by an application developer, company, or individual using a seemingly harmless program, such as a free flashlight app from a marketplace. By presenting individuals with the data collected by monitoring their phone activities, we aimed to trigger the most influential causes for behavioral change, such as fear and concerns about privacy. As stated in the literature review section, if we elicit the instinct of fear in humans by visual stimuli, it will lead to a significant and lasting change in their behavior. Following their findings presentation, the procedure proceeds with a qualitative and open-ended questionnaire designed to provide further insight into their emotional state regarding their privacy. The objective of this questionnaire is to ascertain individuals' perspectives on their emotions over the disclosure of personal information and whether they require or desire our assistance in safeguarding it. For example, Question 3 asks (we): "Did you know that a service or an app such as google timeline could monitor your daily movement? How you feel about it? That lead to the answer: Participant-PE: "Firstly, I never knew the existence of this app. Firstly I heard about it through this experiment. I felt like a victim of monitoring of some company. The details about my daily movement such as going to get by girls from daycare scared me about my safety and the safety of my family" Question (we): What would you like to do? PE: "Can I disable this function? If I disable it my phone will continue to be functional?" (We): "Sure you can deactivate it. Let me show it to you". The protocol of the motivational theory stipulates that, in this final phase, all inquiries or responses to the participant should be presented in a positive manner, without judgment or negativity. The questions of the motivational interview technique are presented in appendix B1. The questions, as well as the subsequent follow-up questions, can vary depending on the participant's answers and subsequent inquiries.

6.4 Questionnaire re-execution

In order to assess any potential changes in participants' self-reported privacy behavior, we requested them to once again complete the phase-2 questionnaire (A1). The objective of this action was to obtain the updated values following the completion of all the experimental procedures. Following this phase, the two questionnaires were compared using two different methods. Firstly, through descriptive analysis, we analyze and process the averages of each question individually. We conducted a comparative analysis of each participant's responses, both on a question-by-question basis and in terms of the overall average. Furthermore, we employed a paired T-test on each item to determine the statistical significance of the observed differences. Based on the findings, we may deduce that the self-

reported privacy behavior of each participant has shown improvement in nearly all of the questions. The T-tests we conducted demonstrated that the p-values for each question were significantly below 0.05, indicating a substantial and meaningful change in behavior. Therefore, it is important to note that participants with higher levels of education had lower changes in behavior. Additionally, it is possible that having a degree in the IT field influenced the results. Due to the limited size of the group, it is difficult to determine with certainty if a degree, particularly in IT, had a significant impact on the observed behavioral changes. The table below displays the participants' replies to A1, together with the p-value obtained from the T-test conducted comparing the two questionnaires. The table 7 below displays the outcomes of the questionnaire that was re-administered.

Table 15. Participants's answers on A1 re-execution.

Part/a nt	Q'1	Q'2	Q'3	Q'4	Q'5	Q'6	Q'7	Q'8	Q'9	Q'1 0
Part/p ant 1	3	3	4	4	3	3	3	3	4	3
Partici pant 2	2	3	3	4	3	3	3	3	4	3
Partici pant 3	2	2	4	2	3	3	3	3	3	3
Partici pant 4	2	2	3	2	2	2	4	4	3	3
Partici pant 5	3	2	3	4	2	3	3	3	3	2
Partici pant 6	2	2	2	3	2	2	3	3	4	3
Partici pant 7	2	2	3	2	1	2	2	3	4	3
Partici pant 8	1	2	2	2	3	2	3	2	3	2
Partici pant 9	1	5	1	1	2	2	3	1	1	2
p- value	0.00 013	0.00 058	0.02 220	0.00 105	0.00 066	0.00 042	0.00 171	0.02 220	0.00 275	0.00 020

6.5. Framework Validation (monitoring re-execution)

Shortly after concluding the experiential techniques, we requested the participants to undergo mobile monitoring, similar to phase-2, but for a duration of 10 days. The objective of this action was to verify the effectiveness of our framework, not only through participants' self-reported privacy behavior, but also through their actual privacy behavior. Once again, the participants did not receive the phone and the SIM card simultaneously due to the limited availability of phones and SIM cards. As a result, several individuals received the equipment a few days after their prior monitoring, while others had to wait for a longer duration, up to 4 months after the experimental procedures concluded. Initially, we were concerned that some participants could revert to their previous privacy-related behaviors, but this did not actually occur. Out of the nine participants, six of them disabled location permissions for most of the apps, including Google services and Viber. Among these six participants, two of them specifically inquired about how to disable these permissions. Out of the 9 participants, 8 uninstalled the lens application that we had previously installed and had both location and actual location rights enabled. All individuals refrained from posting any images on the social networks they utilized during the initial monitoring period. Ultimately, none of the participants were able to successfully uninstall the family connection app, likely due to the software's intentional design to resist removal and the requirement of sophisticated technical expertise for such an activity.

6.6 Final Results

Based on the information provided, we conclude that the experiment was successful for most of the participants. The privacy behavior of all participants appears to have undergone a significant transformation towards increased privacy protection, at least from the conclusion of the experimental procedures until a period of four months thereafter, answering research question 1. Not all participants exhibited the same level of transformation in their privacy behavior, and we are now unable to provide a complete explanation for this phenomenon. Furthermore, we did not anticipate this outcome. Several factors can influence the extent to which participants' privacy behavior changes, including their demographic background and their level of IT education. We deliberately selected participants spanning a wide age range (26-62 years old) and varying educational levels, ranging from high school to individuals with a master's degree, to assess the effectiveness of the framework in transforming privacy behavior regardless of one's academic background. Based on the conversations in the motivating interview and the qualitative questionnaire responses (open-ended answers), we have determined that participants found visual stimulations (experiential procedure-1) to be more effective in transforming their privacy behavior, answering research question 2. Consistently, participants indicated that their

monitored findings, along with the motivating interview's positive discourse, aided their comprehension of their prior privacy behavior level. The majority of the participants regarded the results of procedure-3 to be enlightening. However, without external assistance, it would be challenging for them to initially recognize the extent of their personal information exposure and the necessary precautions they should take to safeguard themselves. Ultimately, participants deemed the practical assessments to be beneficial although occasionally tedious. They provided assistance in determining their present level of privacy and recommended changes to enhance their protection, albeit in a less inspiring manner compared to the other two procedures.

7. Conclusions

The investigation of individuals' privacy behavior and their corresponding activities has been a phenomenon that we have been studying for over 20 years. However, in academia, the prevailing methods to shape an individual's private behavior primarily consist of conventional teaching approaches, despite the fact that most persons still rely on this method for learning or may not receive any education on this issue at all. Our research did not uncover any evidence of a privacy behavior transformation framework being used in primary or high schools. However, such frameworks are predominantly found in higher education, particularly in academic syllabi that are IT-focused. In contrast, disciplines like sociology and psychology have extensively conducted research and experiments to modify individuals' behavior.

The integrated privacy behavior transformation framework we propose draws upon theories and experiences from the disciplines listed above. By leveraging our prior research on factors influencing privacy behavior and conducting an extensive literature analysis on behavior modification theories in other domains, we have successfully crafted a robust framework for transforming privacy behavior. To assess and confirm the effectiveness of our framework, we carried out a controlled experiment, which provided validation for our framework. To the best of our knowledge, this is the initial comprehensive framework that aims to modify an individual's privacy behavior using proven experiential methods.

This framework could prove advantageous to the academic community by facilitating the learning of privacy behavior alteration from individuals' early age and continuing even after they have completed their educational journey. Our framework can be utilized by elementary schools, academic institutes, and private schools to enhance students' adherence to protective privacy behavior. Furthermore, it has the potential to redirect the focus of privacy scholars onto novel avenues of investigation.

The scope of our findings regarding the changing of privacy behavior by experiential aspects is restricted. The experiment was conducted with restricted resources and within a small group of individuals. Hence, our objective is to enhance our framework by identifying its vulnerabilities and subsequently refining them. Our future research will focus on evaluating our

framework in more detail and detail and with a larger group of participants, exploring improved approaches to promote individuals' privacy behavior while reducing our intrusion. This includes investigating alternate methods to phone surveillance that we previously employed by a less privacy-intrusive one.

References

1. Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Adam Thierer, *The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation*, 21. <http://dx.doi.org/10.2139/ssrn.2494382>.
2. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, 80, 1-50.
3. Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security*, 95, 101856. <https://doi.org/10.1016/j.cose.2020.101856>.
4. Tsohou, A., & Kosta, E. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. *Computer law & security review*, 33(4), 434-457. <https://doi.org/10.1016/j.clsr.2017.03.027>.
5. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64, 122-134. <https://doi.org/10.1016/j.cose.2015.07.002>.
6. Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217-227. <https://doi.org/10.1016/j.chb.2016.11.033>.
7. Li, H., Luo, X. R., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & management*, 54(8), 1012-1022. <https://doi.org/10.1016/j.im.2017.02.005>.
8. Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, 77, 226-261. <https://doi.org/10.1016/j.cose.2018.04.002>.
9. Bless, C., Dötlinger, L., Kaltschmid, M., Reiter, M., Kurteva, A., Roa-Valverde, A. J., & Fensel, A. (2021). Raising awareness of data sharing consent through knowledge graph visualisation. In *Further with Knowledge Graphs* (Vol. 53, pp. 44-57). <https://doi.org/10.3233/SSW210034>.
10. Mathews-Hunt, K. (2016). CookieConsumer: Tracking online behavioural advertising in Australia. *Computer Law & Security Review*, 32(1), 55-90. <https://doi.org/10.1016/j.clsr.2015.12.006>.
11. Palos-Sanchez, P., Saura, J. R., & Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research*, 96, 61-72. <https://doi.org/10.1016/j.jbusres.2018.10.059>.
12. Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>.
13. Paspatis, I., Tsohou, A., & Kokolakis, S. (2023). How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors. *Multimodal Technologies and Interaction*, 7(8), 76. <https://doi.org/10.3390/mti7080076>.
14. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389-402. <https://doi.org/10.1057/palgrave.ejis.3000590>.
15. The General Data Protection Regulation (GDPR). Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> . (Accessed on 23 January 2024).

16. Lei Geral de Proteção de Dados (LGDP). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm . (Accessed on 23 January 2024).
17. Personal Information Protection Act (PIPA). Available at: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01 . (Accessed on 23 January 2024).
18. Personal Data Protection Act (PDPA). Available at: <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> . (Accessed on 23 January 2024).
19. Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). Plenum Press. ISBN: 0-306-45443-2 (Hardcover).
20. Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, 55(4), 948-956. <https://doi.org/10.1016/j.dss.2013.01.004> .
21. Hofstra, B., Corten, R., & Van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, 60, 611-621. <https://doi.org/10.1016/j.chb.2016.02.091>.
22. Jiang, J. (2018). Social Login Acceptance: A DIF Study of Differential Factors. In PACIS (p. 20). Volume 20. Available online: <https://aisel.aisnet.org/pacis2018/20> (Accessed on 1 May 2023).
23. Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in) equality in the Internet. *Computers in Human Behavior*, 50, 252-258. <https://doi.org/10.1016/j.chb.2015.04.011> .
24. Reynolds, B., Venkatanathan, J., Gonçalves, J., & Kostakos, V. (2011). Sharing ephemeral information in online social networks: privacy perceptions and behaviours. In *Human-Computer Interaction-INTERACT 2011: 13th IFIP TC 13 International Conference, Lisbon, Portugal, September 5-9, 2011, Proceedings, Part III 13* (pp. 204-215). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-23765-2_14 .
25. Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior*, 76, 149-163. <https://doi.org/10.1016/j.chb.2017.07.015> .
26. Li, C., & Chau, P. Y. (2019). Leveraging communication tools to reduce consumers' privacy concern in the on-demand services: An extended SOR Model of perceived control and structural assurance. *PACIS 2019 Proceedings*. Volume 48. <https://aisel.aisnet.org/pacis2019/48> (Accessed on 5 April 2023).
27. Dhir, A., Kaur, P., Lonka, K., & Nieminen, M. (2016). Why do adolescents untag photos on Facebook?. *Computers in Human Behavior*, 55, 1106-1115. <https://doi.org/10.1016/j.chb.2015.11.017>.
28. Yu, L., Li, H., He, W., Wang, F. K., & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51, 102015. <https://doi.org/10.1016/j.ijinfomgt.2019.09.011> .
29. Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in human behavior*, 86, 276-288. <https://doi.org/10.1016/j.chb.2018.04.041>.
30. Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, 54, 102122. <https://doi.org/10.1016/j.ijinfomgt.2020.102122> .
31. Wilson, D. W., Schuetzler, R. M., Dorn, B., & Proudfoot, J. G. (2015). When disclosure is involuntary: Empowering users with control to reduce concerns. Volume 17, Dr. C.C. and Mabel L. Criss Library. Available online: <https://digitalcommons.unomaha.edu/isqafacproc/17> (Accessed on 1 May 2023).
32. Ioannou, A., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society*, 67, 101774. <https://doi.org/10.1016/j.techsoc.2021.101774>.
33. Nikkhah, H. R., & Sabherwal, R. (2017). Mobile cloud-computing applications: A privacy cost-benefit model. In *Proceedings of the Americas Conference on Information Systems, Boston, MA, USA, 10-12 August 2017*. <https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/11> .
34. Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 33(3), 472-480.. <https://doi.org/10.1016/j.giq.2016.06.004> .
35. Jordaan, Y., & Van Heerden, G. (2017). Online privacy-related predictors of Facebook usage intensity. *Computers in Human Behavior*, 70, 90-96. <https://doi.org/10.1016/j.chb.2016.12.048> .
36. Fox, G., Tonge, C., Lynn, T., & Mooney, J. (2018). Communicating compliance: developing a GDPR privacy label. *AMCIS 2018 Proceedings*. 30. <https://aisel.aisnet.org/amcis2018/Security/Presentations/30> .

37. Risius, M., Baumann, A., & Krasnova, H. (2020). Developing a new paradigm: introducing the intention-behaviour gap to the privacy paradox phenomenon. In Proceedings of the Twenty-Eighth European Conference on Information Systems (ECIS2020) 15-17 June 2020, virtual conference, Marrakesh, Morocco, 2020. https://aisel.aisnet.org/ecis2020_rp/150.
38. Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107, 106260. <https://doi.org/10.1016/j.chb.2020.106260>.
39. Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications*, 13(5), 305-319. <https://doi.org/10.1016/j.eelerap.2014.06.007>.
40. Zhang, Y., He, W., & Peng, L. (2022). How perceived pressure affects users' social media fatigue behavior: a case on WeChat. *Journal of Computer Information Systems*, 62(2), 337-348. <https://doi.org/10.1080/08874417.2020.1824596>.
41. Mager, S., & Kranz, J. (2021). "Consent Notices and the Willingness-to-Sell Observational Data: Evidence from User Reactions in the Field" (2021). ECIS 2021 Research Papers. 89. https://aisel.aisnet.org/ecis2021_rp/89.
42. Hew, J. J., Tan, G. W. H., Lin, B., & Ooi, K. B. (2017). Generating travel-related contents through mobile social tourism: does privacy paradox persist?. *Telematics and Informatics*, 34(7), 914-935. <https://doi.org/10.1016/j.tele.2017.04.001>.
43. Xu, H., Parks, R., Chu, C. H., & Zhang, X. L. (2010). Information disclosure and online social networks: From the case of Facebook news feed controversy to a theoretical understanding. In Proceedings of the 16th Americas Conference on Information Systems 2010 (AMCIS 2010) 12-15 August, 2010, Lima, Peru; Volume 7, p. 503. <https://aisel.aisnet.org/amcis2010/503>.
44. Gómez-Barroso, J. L. (2018). Experiments on personal information disclosure: Past and future avenues. *Telematics and Informatics*, 35(5), 1473-1490. <https://doi.org/10.1016/j.tele.2018.03.017>.
45. Schomakers, E. M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity—insights from Germany. *International Journal of Information Management*, 46, 142-150. <https://doi.org/10.1016/j.ijinfomgt.2018.11.018>.
46. Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51. <https://doi.org/10.1016/j.chb.2017.12.001>.
47. European Union. EU Digital COVID Certificate. Available online: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (Accessed on 24 April 2023).
48. Kraus, L., Wechsung, I., & Möller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, 34, 34-45. <https://doi.org/10.1016/j.jisa.2016.10.002>.
49. Schreiber, T., Deuker, A., Albers, A., & Neves, M. (2013). The Privacy Trade-Off: App Usage on OSN. In Proceedings of the AMCIS 2013, 15-17 August 2013, Chicago, Illinois, USA (Accessed on 24 April 2023).
50. Chou, H. L., Liu, Y. L., & Chou, C. (2019). Privacy behavior profiles of underage Facebook users. *Computers & Education*, 128, 473-485.
51. Keith, M., Ngo, N., & Babb, J. The effects of consumer self-regulation on information disclosure over mobile devices" (2014). AMCIS 2014 Proceedings. 8.. In Proceedings of the International Conference on Interaction Sciences, Savannah, Georgia, USA, 7-9 August, 2014. <https://aisel.aisnet.org/amcis2014/MobileComputing/GeneralPresentations/8> (Accessed on 24 April 2023).
52. Renaud, K., & Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies*, 120, 22-35.
53. Paspatis, I., Tsohou, A., & Kokolakis, S. AppAware: A policy visualization model for mobile applications. *Inf. Comput. Secur.* 2020, 28, 116-132. <https://doi.org/10.1108/ICS-04-2019-0049>.
54. Paspatis, I., & Tsohou, A. (2023). How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. *Journal of Cybersecurity and Privacy*, 3(3), 396-415. <https://doi.org/10.3390/jcp3030020>.
55. Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development*. FT press. ISBN-10: 0-13-389240-9; 1984.
56. Jarvis, P. (2004). *Adult Education and Lifelong Learning: Theory and Practice* (3rd ed.). Routledge.. <https://doi.org/10.4324/9780203561560>.
57. Dewey, J. *Experience and Education*; Macmillan: New York, NY, USA, 1938. <https://doi.org/10.1080/00131728609335764>.

58. Freire, P. *Teachers as Cultural Workers—Letters to Those Who Dare to Teach*; Westview Press: Boulder, CO, USA, 1998; p. 100, ISBN 978-0-8133-4329-7.
59. Rogers, A. *Adult Education*; Metaichmio Publications: Athens, Greece, 1999; Volume 1, ISBN 978-960-566-840-2.
60. Kokko, A. *Adult Education Methodology: Theoretical Framework and Learning Conditions*; Patras EAP: Patras, Greece, 2005; Volume A.
61. Mezirow, J. *Transformative Dimensions of Adult Learning*; Jossey-Bass: San Francisco, CA 94104-1310, USA, 1991. ISBN: ISBN-1-55542-339-6.
62. Mezirow, J. Transformative learning and social action: A response to Inglis. *Adult Educ. Q.* 1998, 49, 70–72. <https://doi.org/10.1177/074171369804900109>.
63. Mezirow, J. On critical reflection. *Adult Educ. Q.* 1998, 48, 185–198, American association for adult and continuing education: Sage publications. <https://doi.org/10.1177/1534484315622735>.
64. Mezirow, J. *Transformative Learning*; Metaichmio Publications: Athens, Greece, 2006; Volume 1, ISBN 978-960-455-226-9.
65. Taylor, W.E. *The Theory and Practice of Transformative Learning: A Critical Review*. ERIC Clearinghouse on Adult, Career, and Vocational Education; The Ohio State University: Columbus, OH, USA, 1998. Available at: <https://eric.ed.gov/?id=ED423422> (Accessed on 31 January 2024).
66. Boud, D., Keogh, R., & Walker, D. *Reflection: Turning Experience into Learning*; Kogan Press: New York, NY, USA, 2002. ISBN: 9781315059051.
67. Tass, P. A. (2003). A model of desynchronizing deep brain stimulation with a demand-controlled coordinated reset of neural subpopulations. *Biological cybernetics*, 89(2), 81–88. <https://doi.org/10.1007/s00422-003-0425-7>.
68. Pavlov, I. P. (1949). Conditioned Responses. In W. Dennis (Ed.), *Readings in general psychology* (pp. 249–267). Prentice-Hall, Inc. <https://doi.org/10.1037/11352-036>.
69. Bandura, A. (1962). Social Learning through Imitation. In M. R. Jones (Ed.), *Nebraska Symposium on Motivation* (pp. 211–269). Lincoln, NE: University of Nebraska Press. Vol.9, No.7. July 12, 2018.
70. Ainsworth, M. D. S., Blehar, M. C., Waters, E., & Wall, S. (1978). Patterns of attachment: A psychological study of the strange situation. Hillsdale, NJ: Erlbaum. Available at: <https://psycnet.apa.org/record/1980-50809-000> (Accessed on 8 September 2023).
71. Watson, J. B., & Rayner, R. (1920). Conditioned emotional reactions. *Journal of Experimental Psychology*, 3(1), 1–14. <https://doi.org/10.1037/h0069608>. Available at: <https://psycnet.apa.org/record/2006-01667-001> (Accessed on 8 September 2023).
72. Asch, S. E. (1951). Effects of group pressure upon the modification and distortion of judgments. In H. Guetzkow (Ed.), *Groups, leadership, and men* (pp. 177–190). Carnegie Press. Available at: <https://psycnet.apa.org/record/1952-00803-001>. (Accessed on 8 September 2023).
73. Becker, H. S. (1963). *Outsiders: Studies in the sociology of deviance*. Free Press. Available at: <https://psycnet.apa.org/record/1965-08393-000>. (Accessed on 8 September 2023).
74. Gipps, C. (2011). *Beyond Testing (Classic Edition): Towards a theory of educational assessment*. Routledge. <https://doi.org/10.4324/9780203182437>.
75. Leenen, L., & van Vuuren, J. J. (2019, February). Framework for the cultivation of a military cybersecurity culture. In 14th International Conference on Cyber Warfare and Security (ICCWS 2019) (pp. 212–220). Available at: <http://www.cair.org.za/sites/default/files/2020-02/>. Framework for the cultivation of a Military Cybersecurity Culture FinalJan2019.pdf (Accessed on 8 September 2023).
76. Bum Mook Oh,, HeeYoon Byun, & Arvindram Krishnamoorthy. Privacy Issues on Social Media: A Tool for Raising Privacy Awareness on Social Media. Available at: <https://www.ideals.illinois.edu/items/106341/bitstreams/346901/object?dl=1> (Accessed on 8 September 2023).
77. Deterding, S., Sicart, M., Nacke, L., O'Hara, K., & Dixon, D. (2011). Gamification. using game-design elements in non-gaming contexts. In CHI'11 extended abstracts on human factors in computing systems (pp. 2425–2428). <https://doi.org/10.1145/1979742.1979575>.
78. Mavroeidi, A. G., Kitsiou, A., & Kalloniatis, C. (2020). The role of gamification in privacy protection and user engagement. *Security and Privacy From a Legal, Ethical, and Technical Perspective*, 79. DOI: 10.5772/intechopen.91159.
79. Karagiannis, S., Papaioannou, T., Magkos, E., & Tsohou, A. (2020, November). Game-based information security/privacy education and awareness: theory and practice. In *European, Mediterranean, and Middle Eastern Conference on Information Systems* (pp. 509–525). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-63396-7_34.

80. Drozd, O., & Kirrane, S. (2020). Privacy CURE: consent comprehension made easy. In ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35 (pp. 124–139). Springer International Publishing. https://doi.org/10.1007/978-3-030-58201-2_9.
81. Maragoudaki Sofia-Niovi & Kalloniatis Christos. 2022. Virtual Reality as a mean for increasing privacy awareness: The escape room example. In 26th Pan-Hellenic Conference on Informatics (PCI 2022), November 25–27, 2022, Athens, Greece. ACM, New York, NY, USA, 9 Pages. <https://doi.org/10.1145/3575879.3576002>.
82. Mavroeidi, A. G., Kitsiou, A., Kalloniatis, C., & Gritzalis, S. (2019). Gamification vs. privacy: Identifying and analysing the major concerns. *Future Internet*, 11(3), 67.
83. Mavroeidi, A. G., Kitsiou, A., & Kalloniatis, C. (2021). Gamification: A necessary element for designing privacy training programs. DOI: 10.5772/intechopen.97420.
84. Henne, B., Szongott, C., & Smith, M. (2011, September). Towards a mobile security & privacy simulator. In 2011 IEEE Conference on Open Systems (pp. 95–100). IEEE. Available at: <https://ieeexplore.ieee.org/abstract/document/6079294> (Accessed on 8 September 2023).
85. Miller, W. R., & Rollnick, S. (2012). *Motivational interviewing: Helping people change*. Guilford press. ISBN: 978-1-60918-227-4 (Hardcover); 978-1-4625-0757-3
86. Naar, S., & Safren, S. A. (2017). *Motivational interviewing and CBT: Combining strategies for maximum effectiveness*. Guilford Press. Available at: <https://psycnet.apa.org/record/2017-26282-000> (Accessed on 8 September 2023).
87. Towne, K., Campagna, M., Spohn, R., & Richey, A. (2023). “Put it in your toolbox”: How vocational programs support formerly incarcerated persons through reentry. *Crime & Delinquency*, 69(2), 316–341. Available at: <https://journals.sagepub.com/doi/full/10.1177/00111287221098581> (Accessed on 8 September 2023).
88. Liping, C. U. I., Kun, H. U., Haoce, H. U. A. N. G., Ning, D. E. N. G., Jia, W. E. N., Lisen, Y. A. N. G., & Yuexia, Z. H. A. O. (2022). Effect of Cognitive-behavioral Change Model-based Online Health Education in Hypertension Management. *Chinese General Practice*, 25(16). DOI: 10.12114/j.issn.1007-9572.2022.0052.
89. Dali, K., & Hohmann, G. (2023). Preserving the Wonder of Stories: The Role of Reflection in Reading Education in Library and Information Science Programs. *Journal of Education for Library and Information Science*, 64(2), 206–229. <https://doi.org/10.3138/jelis-2022-0014>.
90. Dols, J. M. F., & Russell, J. A. (Eds.). (2017). Natural facial expression: A view from psychological constructionism and pragmatics. In J.-M. Fernández-Dols & J. A. Russell (Eds.), *The science of facial expression* (pp. 457–475). Oxford University Press. ISBN: 978-0-19-061350-1.
91. De Berardis, D., Fornaro, M., & Orsolini, L. (2020). “No Words for Feelings, Yet!” Exploring Alexithymia, Disorder of Affect Regulation, and the “Mind-Body” Connection. *Frontiers in Psychiatry*, 11, 593462. <https://doi.org/10.3389/fpsy.2020.593462>.
92. COPE Core practices. Available at: <https://publicationethics.org/core-practices> (Accessed on 23 January 2024).
93. Holmes, C.C.; Adams, N.M. Likelihood Inference in Nearest-Neighbour Classification Models. *Biometrika* 2003, 90, 99–112. <https://doi.org/10.2307/30042022>.
94. Rufer, M., Hand, I., Braatz, A., Alsleben, H., Fricke, S., & Peter, H. (2004). A prospective study of alexithymia in obsessive-compulsive patients treated with multimodal cognitive-behavioral therapy. *Psychotherapy and psychosomatics*, 73(2), 101–106. <https://doi.org/10.1159/000075541>.
95. Murdoch, M., Simon, A. B., Polusny, M. A., Bangerter, A. K., Grill, J. P., Noorbaloochi, S., & Partin, M. R. (2014). Impact of different privacy conditions and incentives on survey response rate, participant representativeness, and disclosure of sensitive information: a randomized controlled trial. *BMC Med Res Methodol* 14, 90 (2014). <https://doi.org/10.1186/1471-2288-14-90>.
96. Fisher, R. A. (1970). *Statistical methods for research workers*. In *Breakthroughs in statistics: Methodology and distribution* (pp. 66–70). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4612-4380-9_6.
97. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *psychometrika*, 16(3), 297–334. DOI: <https://doi.org/10.1007/BF02310555>.
98. Paspatis, I., Tsohou, A., & Kokolakis, S. (2017). Mobile application privacy risks: Viber users’ de-anonymization using public data. *MCIS 2017 Proceedings*. 32. <https://aisel.aisnet.org/mcis2017/32>. Crossref on Appendix-D.

Appendix A – Questionnaire (ENG)

1. [PA]How often do you check the privacy settings on your social media accounts?

2. [TCCF,PRP,PC] How often you felt like your privacy was violated online?
3. [PA]How often do you read the privacy policies or terms of service for the websites or apps you use?
4. [PA,PC] Have you ever declined to use a service or app because of privacy concerns? If so, can you describe the situation (open)?
5. [PA,PC] Do you use different passwords for different accounts? How do you keep track of them(open)?
6. [TCFF] Have you ever been a victim of identity theft or online fraud? How did that experience affect your privacy behaviors (open)?
7. [PRP,PA] How much personal information do you share online? Can you describe the reason (open)?
8. [PA] How often do you take steps to protect your online pri-vacy? Do you use ad-blockers or other tools and which (open)?
9. [PRP,TCFF] Did you know companies collecting and using your personal data for targeted advertising?
10. [PC] Do you have any concerns about government surveillance or monitoring of your online activities?

Appendix B - English (Interview Questions)

Questions based on experiment (likert 1-5) of qualitative.

- 1) [TCCF, PC, PA, EVIE] Interview and simultaneous demonstration of her/her personalized image as well as data we have recovered, habits, etc. How do you feel about this?
- 2) [PA,PC,EVIE] Did you know that a lens app could access your daily location?
- 3) [TCCF,PC,PA,EVE]How do you feel about this? H8b triggering fear, privacy risk concerns, privacy awareness through visualization
Did you know that automatically or automatically someone or a company could create your daily patterns such as waking up in the morning, what you go to or leave your job, or when and where you train?
- 2) [PA,TCCF] How do you feel about this?
- 3) [PA,PRP] Did you know that through your posted photos you could find the time and place they were taken or other data?
- 4) [TCCF, PRP, PC]How do you feel about it?
- 5) [PA,PRP]Do you think you should disable Google timeline, strava, viber? (photo from viber/sqlite/strava)
- 6) [EVIE] Will you do it or will you ask for help with it?
- 7) [EVIE]Do you know how to remove permissions from apps?
- 8) [PA,PC,PRP]Will you search and remove permissions from apps?
- 9) [PA,PC,PRP]Will you continue to post photos on social networks?
- 10) [PA,PC,PRP]Do you feel upset that a company or even a developer can create patterns of your daily life?

Appendix C – Experiment content and items

Table 16. Visual Content and Stimulations

Activated Factor(s)	Movie/Series Name	Short Description	Purpose and Target
PRP, TCCF, PA, EVIE	The Great Hack	The Cambridge Analytica scandal is examined through the roles of several affected persons.	Awareness of the handling of personal data by social platforms. Decreased trust in social networks.

PRP, TTCF, PA, EVIE	The Social Dilemma	Explores the dangerous human impact of social networking, with tech experts sounding the alarm on their own creations.	Awareness of the handling of personal data by social platforms. Decreased trust in social networks.
FEBU, TCCF, NPEN, EVIE	Black Mirror: Nosedive	A woman desperate to boost her social media score hits the jackpot when she's invited to a swanky wedding, but the trip doesn't go as planned.	Social media awareness. Indication of compulsive behavior
TCCF, NPEN, PA, TL	Black Mirror: Smithereens	A cab driver with an agenda becomes the centre of attention on a day that rapidly spirals out of control.	Awareness of social networks and risks of compulsive behavior

Table 17. Short videos items

Activated Factor(s)	Video Name	Short Description	Purpose and Target
PA, EVIE	"How to Protect Your Privacy Online" by Techquickie	This video covers the basics of online privacy and offers practical tips for staying safe on the internet.	Social media privacy awareness enhancer.
PA, TCCF, PC, EVIE	Data Protection and Privacy.	(animated). Increasingly, an ever-wider range of economic, political and social activities are moving online, encompassing various kinds of information and communications technologies (ICTs). The evolving ICT use is having a transformational impact on the way business is done, and the way people interact among themselves, as well as with government, enterprises and other stakeholders.	Personal Data protection privacy awareness, data control enhancer regarding companies, government etc.

PA, TCCF, EVIE	"Why Privacy Matters".	When it comes to online privacy, many who skip over the subject have said: "I have nothing to hide, so I'm okay." It's a response to which some experts in the field of privacy point out, even if you're alone in your home, would you be okay with someone watching through your window and taking notes on everything you do the entire day? Because that is essentially what's happening online right now, and it's legal.	Arise privacy awareness through control and fear
PA, TCCF, EVIE	Protecting Personal Privacy.	(animated) This animated video explains how your exposed personal data can get you in trouble.	Arise privacy awareness, enhance privacy concerns and privacy risk perception through control and fear.
PA, PC, EVIE	Why Care About Internet Privacy?	(animated) Whenever you browse the Internet, websites are collecting information about you and using it to fuel their businesses. They use your information to display relevant ads, to sell you products you might be interested in, and more. If you're okay with companies collecting your information, that's fine. If you're not, there are steps you can take to lessen the risk.	Increase privacy awareness and privacy concerns
PA, PC, EVIE	Privacy Matters.	(animated). This video shows how private data exposition can hurt your job position.	Increase privacy awareness and privacy concerns
PA, PC, EVIE	Online Privacy for Kids - Internet Safety and	(animated). Social media is a great tool to communicate with our family and friends but it's important to be mindful of what we post,	Increase privacy awareness and privacy concerns on kids

	Security for Kids.	where we post it and who we share it with. In this educational video we're going to give you advice on how to protect our online privacy. We should be careful with what we share, even more so if it's personal information that we wouldn't like other people to know about. Sharing is a responsibility.	
PA, PC, EVIE	Online safety Staying safe online.	(animated). Learn how to stay safe and act responsibly when using the internet in school and at home.	Increase privacy awareness and privacy concerns on kids
PA, PC, EVIE	Cyber Security for kids Internet Safety Tips for Kids.	This video talks about the importance of password, protecting personal information, limiting screen time etc.	Increase privacy awareness and privacy concerns on kids
PA, PC, PRP, EVIE	NetSafe Episode 11: Protect Your Personal Information.	This video explains why keeping personal information private is so important, and it offers tips on how to do it.	Increase privacy awareness and privacy concerns through show the privacy risks
PA, TCCF, EVIE	"Social Media Privacy: How to Be Safe" by Norton	This video provides tips for protecting your privacy on social media platforms.	Increase privacy awareness and control.
PA, EVIE	"Privacy Matters" by Mozilla	This video highlights the importance of privacy and provides tips for protecting your online privacy	Increase privacy awareness and confidence through education
PA, PC, EVIE	"The Cost of Privacy" by Vox	This video explores the trade-offs between privacy and convenience in our digital lives.	Increase privacy awareness and privacy concerns

Table 18. Practical Assessments items

Activated Factor(s)	Simulator Name	Short Description
PA, TCCF, EVIE	Privacy Choices	https://www.telus.com/en/wise/parents/privacy-quiz
PA, EVIE	Privasim	Privasim is a simulator game where you play as an app company, collect users, mine data, and sell data to get rich. Avoid cyber attacks, fight legal battles and get Influencers to join your app. https://privasim.itch.io/privacysimulator
PA, PC, EVIE	Data Detox Kit	Take control of your digital privacy, security, and wellbeing, learn about tackling misinformation, control your health data, find resources for youth and families, and browse our Alternative App Centre and workshop materials. Meet our partners to get a glimpse into the global movement of the Data Detox Kit. https://datadetoxkit.org/en/home
PA, PC, EVIE	The Realistic Facebook Privacy Simulator	https://www.tomscott.com/usvsth3m/realistic-facebook-privacy-simulator/
PA, EVIE	Privacy Scores	Learn about your privacy settings and how they compare to others. It can also help you to identify areas where you can improve your privacy settings.

Table 19. Gamification items

Game Name	Short Description
Privacy Badger	This is a browser extension game that teaches users how to protect their online privacy by blocking ads and trackers
Data Dealer	This is a web-based game that simulates the buying and selling of personal data. Players learn about data privacy issues and how to protect their information
The Glass Room	This is a physical exhibition that can be turned into a game. Visitors learn about data privacy and security by engaging with interactive exhibits
Keep Calm and Log On	This is a card game that teaches players how to protect their online privacy by recognizing different threats and taking appropriate measures
Cryptoy	This is a mobile game that teaches players about encryption and digital security by challenging them to solve puzzles

Table 20. Privacy behavior quizzes items

Quiz Name	Short Description
Online Privacy Quiz	This quiz, created by the Electronic Frontier Foundation (EFF), tests your knowledge of online privacy issues and helps you learn how to protect your personal information online.
Privacy IQ Quiz	This quiz, created by the Privacy Rights Clearinghouse, tests your knowledge of privacy laws and practices in the United States.
Data Privacy Quiz	This quiz, created by the National Cyber Security Alliance (NCSA), tests your knowledge of data privacy and security best practices.
Facebook Privacy Quiz	This quiz, created by Facebook, helps you understand how to manage your privacy settings on the social media platform
Google Privacy Quiz	This quiz, created by Google, tests your knowledge of how Google collects and uses your data.

Appendix-D – Experimental Environment Setup

- Google's accounts and tools

We constructed our experimental environment during the environment setup phase. Specifically, we created a central Gmail account (IonianUniversityLab@gmail.com) to which all other accounts will be linked. Then, we created participant accounts (ionianuniversity-labvictim1-9@gmail.com, figure 20) and tested per device that we can through the embedded application by typing per account the address <https://www.google.com/android/find/> in a browser to confirm that we can pinpoint the exact location of the device and whether it is moving, the wifi network it is connected to (ssid), and whether it is currently charging (battery level 100%). The purpose of creating these accounts is to demonstrate to the participants, via Google Timeline, that each of their movement activities can be recorded, allowing for the creation of personalized patterns, such as when they leave or return home each day, if they use wifi or mobile data, etc. As demonstrated in our previous research [98], all of these data can be extracted by any mobile application that is installed on our device and has access to the corresponding rights. As a reminder, the respective application's installation file (manifest apk package) is sufficient. To ensure participants' privacy and security every data will be collected in a separate virtual machine per participant as it is pictured in figure 9. Each virtual machine for the safety and privacy of the participants will be safely deleted upon the publication of the experiment.

Two lines of code within the manifest file, for instance, are sufficient for an application to access our website (figure X).

```
<manifest ... >
  <!-- Always include this permission -->
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />

  <!-- Include only if your app benefits from precise location access. -->
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
</manifest>
```

Figure 18. Android's manifest example file.

- Create VPN accounts (1-click vpn)

We used a free browsing anonymizer to create streaming platform's accounts without the risk of being detected by creating multiple accounts from the same IP address. Specifically, we installed a virtual private network add-on (extension/add-on) from the browser's official app store in the browser of our choosing. We chose 1clickVPN because it has an ideal rating (5 stars) and is compatible with more than 26,000 browsers.

- Streaming Platform Account Creation

To facilitate legal monitoring of our content, we've employed a low- to no-cost strategy. First, we generated temporary email identifiers for each topic. With VPN enabled and the Asia region selected, we conducted a search for a free trial offer for an unspecified period of time and discovered numerous 30-day trials. Asia was selected because, based on our inquiry, it appeared to offer the most affordable prices compared to the other options. After creating the profile, we were required to provide a credit or debit card for continued service use. For this reason, we placed 5 euros onto a virtual prepaid crypto card (virtual prepaid crypto card) in a foreign service of our choosing. The selection of a virtual card in a foreign service was made as an additional measure of anonymity, as this particular service states that it does not share personal information with third parties (<https://www.blockchain.com/card>), despite the fact that identification was not required. Notably, while multiple accounts were established, the same prepaid cryptocurrency card sufficed for each. Finally, we opted for the most affordable platform access method. Also, there was no issue with the language selection, so we chose a profile in its Greek version to ensure there were no issues locating the content or with the supported subtitles.

- Virtual Machines Creation

To ensure maximum monitoring isolation, ensure participants' privacy and secure their data an equal number of virtual machines were constructed. Oracle Virtual Box was chosen to construct and utilize virtual machines because it is free and open source. Windows 10 Student Edition was selected as the operating system, which is provided for free for 30 days, with the only limitation being a subtly displayed prompt to activate it. The primary factors (except enhancing participants' privacy) for utilizing virtual machines were as follows. Each Viber for PC application can have a sim card attached, making the surveillance of Viber's internal database (SQLite) simpler and more isolated. Using VMs allows us to simultaneously monitor and execute SQL scripts on all experiment participants. The purpose of using Viber for PC and its built-in platform is explained in the following section. Each virtual machine was configured with 2 10th-generation Intel i7 cores, 4GB RAM, and 20GB SSD on a 32GB RAM system. The reason for the low computing power requirements was that only the most essential software would be installed, and in order to extricate the data, a large number of VMs would need to be open in parallel, so we avoided a more expensive solution.

- Viber και SQLite.

The objective of this application is to extract as much information as possible about the participants' actual behavior. According to our previous research [98], if an advanced user and developer installs both Viber for Desktop and the SQLite Browser for direct access to the local database of his Viber account (SQLite DB), he is presented with a set of options. First, as soon as the application synchronizes with his Google or iOS account, he can automatically view and modify a set of data through the SQLite browser. For instance, it can determine how many of its contacts have Viber installed (ViberContact = 1), if they have uploaded a photo to their profile (DownloadID = "not null"), and their last login date in unix date and time format, as well as perform various types of SQL queries. Our research at the time demonstrated that, with proper management and methodology (figure 5,6), it is possible to identify a group of unknown individuals with a success rate of greater than 85 percent. The purpose of this application is to transform all collected data into relevant information. In the same study [98], we demonstrated that the methodology we developed enabled us to reveal various behavioral patterns of the research participants at the time, such as the time of morning awakening and evening sleep, arrival at work, and a different pattern of behavior during the weekends (figures 7,8).

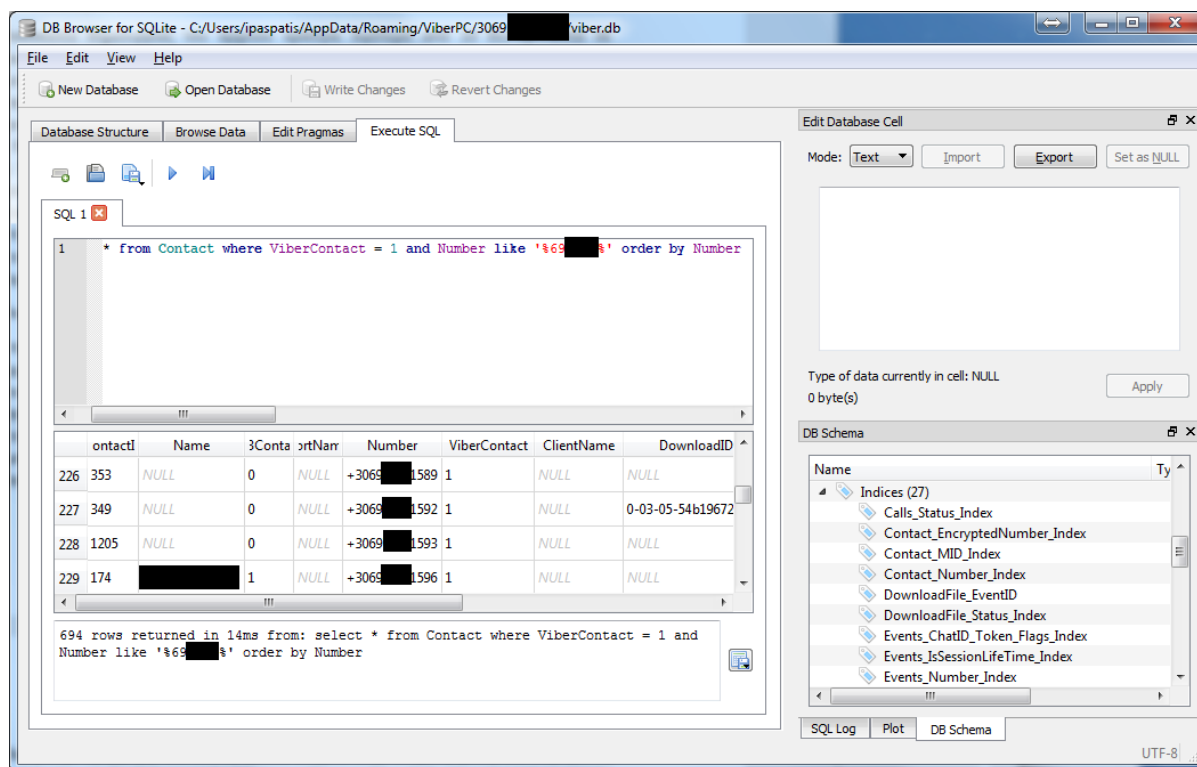


Figure 19. Viber's SQLite Database derived from Paspatis et al., [98] research.

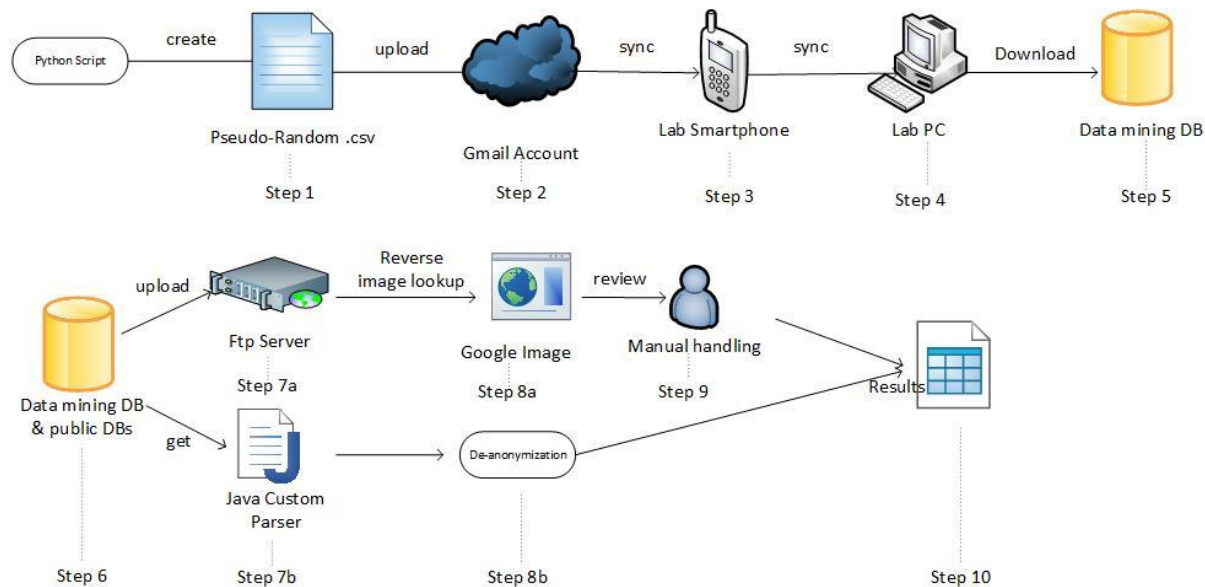
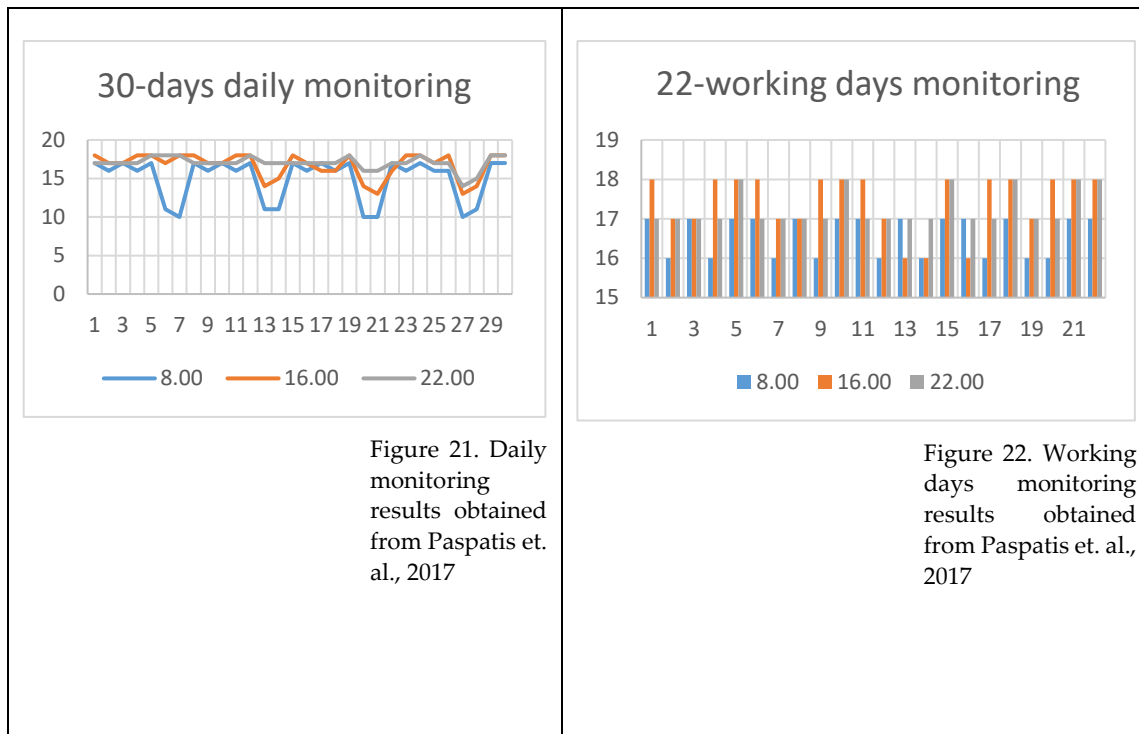


Figure 20. Paspatis et al., [98] de-anonymization methodology.



Experimental Framework Tools

As we mentioned multiple free to use software tools selected to utilize through the experiment. Each tool is described in the following table 13 while figure 9 includes the experimental from the virtual machines perspective.

Table 21. Experimental Environment tools

Application / Software	Connected Software	Target
Virtual Machine	Google Account	Google Account Management
	Viber For Desktop	Viber Account Management
	Streaming Platform Account	Content Tracking Control
Google Account	Family Link	Location finding, pattern formation
	Find my phone	Location finding, pattern formation
	Timeline	Participant movement tracking
	YouTube progress	Content Monitoring Validation
Viber For Desktop	SQLite DB Browser	Finding patterns and participant information
Streaming Platform Account	Streaming Platform	Content Monitoring Validation

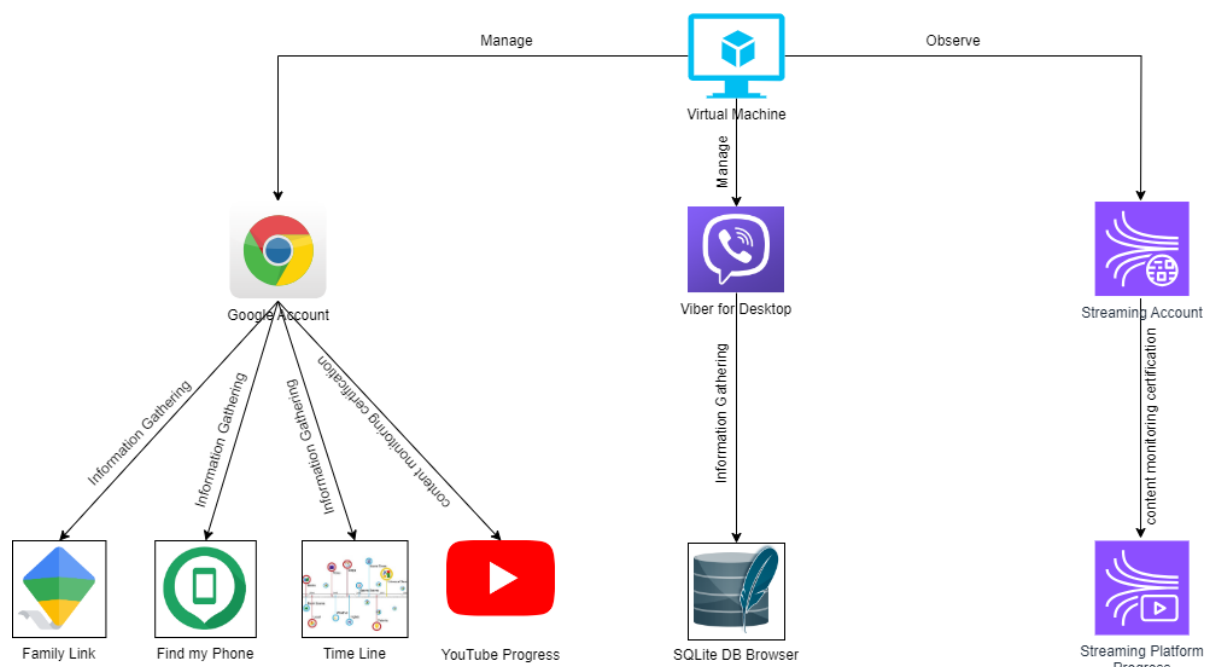


Figure 23. Environment setup representation

- Limitations and Challenges

Throughout the preparation and execution of our experiment, we faced many obstacles and constraints arising from the chosen tools. An initial constraint we faced was the inability to monitor many SIM cards on a single virtual machine using "Viber for Desktop" and "SQLite Browser". Although employing the Windows switch account feature may resolve the current problem, it would thereafter prevent us from concurrently monitoring several databases or extracting data from their databases simultaneously using SQL queries. To address this issue, we established many instances of virtual machines and successfully resolved it. This resulted in a RAM allocation problem, as each Virtual Machine required a minimum of 4 GB of RAM, totaling 32 GB for the entire infrastructure. In order to resolve this problem, we opted to replace the selected version of Windows with a lightweight variant known as Tiny11, which required less than half the amount of RAM compared to our initial choice of operating system. Another problem we faced was the lack of support in Google Timeline for extracting a specific time period. Instead, it simply allows for downloading all of the recorded historical data. We experimented with various browser add-ons in an attempt to overcome the issue, but we could not get the anticipated outcomes. Consequently, we developed a bespoke Python script that temporarily resolved the issue, but requiring us to modify the code slightly and rerun the script whenever we needed new data. This involves basic programming proficiency, but we should strive for a long-term solution that does not necessitate the aforementioned skills. Regarding the ethical surveillance aspect, we plan to exclude it from our architecture as it evolves. In the meanwhile, we intend to collect data solely using SQL queries and programming scripts. Subsequently, the obtained data can be processed using K-anonymity techniques to reduce the disclosure of personal information, street names, and specific locations, even to the research team.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Part 3 – Support Papers

Paper – IV

Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2017 Proceedings

Mediterranean Conference on Information Systems
(MCIS)

Mobile application privacy risks: Viber users' de-anonymization using public data

Research full-length paper

Track 10- Trust, Security and Privacy Track

Paspatis, Ioannis, Ionian University, Corfu, GR, c16pasp@ionio.gr

Tsohou, Aggeliki, Ionian University, Corfu, GR, atsohou@ionio.gr

Kokolakis, Spyros, University of Aegean, Samos, GR, sak@aegean.gr

Abstract

Mobile application developers define the terms of use for the applications they develop, which users may accept or declined during installation. Application developers on the one hand seek to gain access to as many user information as possible, while users on the other hand seem to lack awareness and comprehension of privacy policies. This allows application developers to store an enormous number of personal data, sometimes even irrelevant to the application's function. It's also common that users choose not to alter the default settings, even when such an option is provided. In combination, the above conditions jeopardize users' rights to privacy. In this research, we examined the Viber application to demonstrate how effortless it is to discover the identity of unknown Viber users. We chose a pseudorandom sample of 2000 cellular telephone numbers and examined if we could reveal their

personal information. We designed an empirical study that compares the reported behavior with the actual behavior of Viber's users. The results of this study show that users' anonymity and privacy is easily deprived and information is exposed to a knowledgeable seeker. We provide guidelines addressed to both mobile application users and developers to increase privacy awareness and prevent privacy violations.

Key words: Viber, privacy, awareness, anonymity, privacy deprivation, public data, mobile apps.

1. Introduction

The massive increase of smartphone use has created new opportunities in the telecommunications' field. Multiple instant messaging applications like Viber, WhatsApp and Facebook Messenger are being downloaded, installed, and used daily to enhance human communication, making these apps an important part of almost anyone's social life. According to the surveys by Statista (Statista, 2017a; 2017b; 2017c) in 2017's first quarter, there were 1.2 billion WhatsApp and Facebook Messenger and 891 million Viber's unique users. Such mobile applications (hereafter mobile apps) have evolved from being a simple instant messaging service to a multi-use social networking tool. Apart from Instant Messaging, they provide voice messaging, file and photos sharing, location tracking, voice calls and many more features. Mobile app developers (hereafter app developers) are responsible for the mobile app's permission set. This allows app developers to collect a vast amount of information on users, such as mobile numbers, locations, contact lists, profile pictures, or other users' private information and to use them at will or opportunity, including selling data to third parties.

Recent studies have concluded that users consent to the mobile app's permission set, as a mandatory step in the downloading process, without actually reading the privacy policy. The result is the misinformed exposure of their personal data. McDonald and Cranor (2009) illustrated that such privacy policies are far too long and complicated for the users to spend their time reading them. Giovani and Pashley (2007) state that even though users are informed about the possible consequences of a leakage of personal data and the imminent dangers involved, they don't change their security settings in their social networks and they keep on using them as usual, although they know how to change them. According to Tow et al. (2008), users are not well informed and, therefore, not aware of their personal data exposure, or they feel it is unlikely that such a privacy

incident could harm them. So, users are unaware of the risks they are facing, such as identity forge, stealing, impersonation and many others, as they lack the knowledge required to evaluate these risks (Pitkanen & Tuunainen, 2012).

Our aim is to demonstrate how effortless it is to discover the identity of an unknown app user by only processing self-exposed public data and to offer guidelines for mobile app users and developers. We revealed users' personal information such as their real name, address and other personal data. It is crucial to show that even without any prior information we can extract automatically information on one's private habits, such as the time they wake-up or when they switch on and off their mobile phone. More importantly, we can do this for a large number of people, and not only for targeted individuals. The purpose of such a demonstration is to enhance privacy awareness of mobile app users and to inform them about the risks involved in disclosing their public data, so that they would change the privacy settings on their mobile apps and stop blindly accepting privacy policies.

In order to examine our claim that users' identity can be revealed by publicly available data, we conducted an empirical experiment using the popular instant messaging mobile app Viber. We chose a set of 2000 pseudo-random cellphone dummy numbers and we automatically discovered which of them have the Viber app installed. We had a prior knowledge that these cellphone numbers were active in the recent past. The de-anonymization process was successful for 75% of our test sample. In most cases, we disclosed the full name of the subject and his/her address. This study is the first, to the best of the authors' knowledge, to show that this kind of information can be gathered in a large scale without targeting specific subjects. Buchenscheit et al. (2014) have similarly studied WhatsApp mobile app and concluded through an experiment that it is possible to infer users' habits. Although the study of Buchenscheit et al. (2014) reveals several privacy related inferences, it does not show that users' identities can also be revealed, which we do in this paper.

The paper is structured as follows. In section two we present the related work. Section three presents the methodology we followed and the preparation we made in order to accomplish our data mining aims and create meaningful statistic data. In section four, we present our de-anonymization results, our statistical analysis and our empirical questionnaire results (see Appendix). Section five presents the contribution of the paper and a guide for best practices to reduce private data leak. Finally, section six concludes the paper.

2. Related Work

In order to examine scholar disquisition associated to our research objective, we reviewed the following literature areas: (a) general literature on personal data disclosure, (b) users' privacy awareness, and (c) mobile apps' features and vulnerabilities. At section 2.3, we specifically examined the Androids OS security characteristics and features. We chose to study Android OS because it allows users to change the security settings (Benenson & Reinfelder, 2013). On the other hand, IOS uses an App review process system when a new app is uploaded to its App Store, whilst users cannot change any security settings or review the permission set before installation.

2.1 Personal Data Disclosure

The invasion and violation of one's privacy and personality includes unauthorized collection, publishing and/or posting of personal data through the Internet and any other use of personal information without the prior consent of the data subject (Wang et al., 1998). The collection, sale and/or exchange of personal data between companies or individuals has become a common practice (Gillmor, 1998) as the Internet has made it easy to collect and store large volumes of personal information (Caruso, 1998). According to a 2002 survey (Rust et al., 2002) it has become impossible for consumers to carry out almost any electronic transaction without revealing some sort of personal information. Several online companies are operating on collecting and using such personal data (Fletcher, 2003). Users show an increased concern when their data are collected and disclosed on the web (Global Internet User Survey, 2012; TRUSTe, 2014). Several researchers have set out indicators on consumers' concerns when the handling of their personal information is involved (Sheehan and Hoy, 2000; Dinev and Hart, 2004; Bellman et al., 2004). Users' awareness on data collection, misuse of data, experience in internet use, social profile and consumers' level of education are some of these indicators.

2.2 Users' privacy awareness and the cost of reading privacy policies

McDonald and Cranor (2008) examined the reasons why users' do not read the privacy policies, as well as time and financial costs of reading them. They investigated 75 of the most popular websites, and they

reveal that a user would need about 10 minutes to read one privacy policy, at an average read rate of 250 words/minute. Also, they concluded that an average user should read at least 1354 privacy policies per year, where 412 of them should be read while at work hours (McDonald and Cranor, 2008). Based on the above, they conclude that a user would have to spend 40 minutes per day for just reading policies, while the average user is browsing the internet for approximately 72 minutes per day. Translating this into financial cost would mean about 3500 dollars per year for a user, while at a national level (in the U.S., where the research was conducted) this would be 781 billion per year. Capistrano and Chena (2015) showed that the specificity of the privacy policy has a significant effect on consumers' perceptions of its importance in deciding to share personal information. The key factor for their decision was the length of the privacy policy as primary reason as well as the visibility of its.

Govani and Pashley (2007) focused on the privacy awareness of university students in relation to the Facebook social network. According to their findings the majority of students are aware of the potential impact from the leakage of personal data as well as the imminent danger of impersonation or monitoring. Although they are aware of their options to limit the leakage of personal data, they do not take any action. This is in line with the findings of Tow et al. (2008) that users are either not fully aware of the privacy incidents or feel that the likelihood of privacy violation is too small to happen. Similar results have been shown by Gross and Acquisti (2005). Their findings stated that the risk of personal exposure or identity theft and other negative effects is proportional to the amount of information a user exposes. Almuhimedi et al. (2014) concluded that most users are unaware that their personal data are collected by mobile apps and also that their location can be exposed by these data. In addition, they suggested the use of an app permission manager such as AppOps, an embedded app manager in Android 4.2. The permission manager will notify users with privacy nudges in case an app starts to use a permission that can expose their personal information. Similar privacy nudges are present iOS 6 and after, where users receive popup warnings about usage of some data types and are asked for informed consent (Benenson and Reinfelder, 2013). As conclusion of the above, is proved that the users' low awareness can lead to privacy risk incidents or increase the chance for them to be happen. Researchers also concluded that users avoid reading privacy policies due to their extended length or the time need it for it.

Mobile apps' features and vulnerabilities

The Mobile Device Safety Management with Android operating system is implemented with a multisite security system (Boksasp et al., 2012). This Safety Management System includes: (a) app's permission management system (permission set), (b) sandboxing, (c) unique certification signing for every developer, (d) remote kill switch for detected malfunctioning apps, (e) core file system protection in read only mode, (f) google bouncer as anti-virus, and (g) third-party antiviruses. These security characteristics tend to protect only the device and not user's data. According to a Pew Research Center survey (2012), 82.56% of the app's that are available for downloading in app markets are requiring the permission "Full network access", while 23.75% of apps are requiring the permission "Precise Location GPS and network based Permission". These permissions are giving the opportunity to an app developer to disclose users' real location. Combined with the fact that most users install at least 10 apps on their mobile device (Olmstead & Atkinson, 2015), it creates favorable conditions for revealing users' location. Rakib and Ho (2011) concluded that service providers should consider users' privacy concerns before they use capabilities such as location detection or personal-data detection. Buchenscheit et al. (2014) have studied WhatsApp mobile app and found, through an experiment, that it is possible to infer users' habits. Several researchers have shown that many users not pay attention to the permissions are granting to an app upon installation (Felt et al., 2012; Kelley et al., 2012). The researchers also, concluded that the technical language in which they are written is not easy to understand. Benenson and Reinfelder (2012) showed that Android users would be better informed about possible risks in case they notice and can understand the permissions. The same researchers concluded that although the Android's permissions visibility and cryptic language is difficult to understand, they seem to work in raising awareness at least with more technically savvy users. Appelman et al. (2011) conducted a research regarding Viber's communication security. Some of their findings were: Viber's database is unencrypted and easy accessible, it is possible to bypass the official registration process and one could forge a person's Viber account, data messages are probably sending scrambled and not encrypted.

Users' low privacy awareness and the difficulties they face on reading privacy policies, as mentioned in chapters 2.1 and 2.2, combined with the mobile devices' security management system, create appropriate conditions for the non-consented disclosure of personal information. In our experiment, we show that it is possible to disclose users' personal information, such as real name and surname, profile photos

and address without any prior knowledge of their identities. This study is the first, to the best of the authors' knowledge, where these vulnerabilities of the security management system are explored with actual personal information for empirical investigation.

3. Preparation and methodology

Viber's users are nearly 900 million as of March 2017. This makes Viber a perfect candidate to conduct our research. There are three core characteristics of this app that are essential to note. Firstly, when a user installs Viber, her cell phone number is sent to Viber's servers by default. Also, as feature, the contact list of the new user's device is parsed, and every Viber's user who is registered at this contact list is automatically informed about the new user enrolment. Secondly, there is a practical difficulty for a user to exit the mobile app. Even if the user presses the exit button from the app's menu, the app will continue running in the background as a service. Lastly, the mobile app allows a massive import of contact data in Viber's contact list without any confirmation from the other users. This feature was exploited in our research.

3.1 System Preparation

To create a controlled setting for our experiment, we created a virtual machine with Microsoft Windows 10 and we installed our toolset. Our toolset is composed by Viber for Desktop, DB Browser for SQLite for the mobiles' database handling, Python for our scripts and Netbeans for Java to create our crawlers. The virtual machine is equipped with an Intel i7 6700, 16 GB of RAM and 250 GB SSD SATA 3 disk. Also, a sim card was purchased for the testing device to activate the "Viber for Desktop" application.

3.2 Methodology of data mining

To start our data mining we first wrote an 8-line python script with which we created a 2000-line dummy csv file. The file was grafted as follows: name as dummyName[serial number], surname as dummySurname[serial number], cellphone number as +3069xxxx[serial number]. Then, we created a new Gmail account and we imported our dummy csv file as real contacts. Next, we installed Viber for cellphones and we added the Gmail account we

created. The cellphone numbers were pseudorandom numbers. We had prior knowledge that these phone numbers were employees' phone numbers of a telecommunication company that stopped functioning since 2013. In sequence, the Viber app started to synchronize our dummy dataset with real Viber accounts. After this step, we can see in our testing device which contacts have an account on Viber. This was performed by opening the viber.db with the SQLite app and running the SQL query "select * from Contact where ViberContact = 1 and order by Number". The result includes the contacts who have a Viber account (ViberContact = 1), a possible name and a possible profile picture (DownloadID not null) (Figure 1). These data were exported to a csv file for later processing.

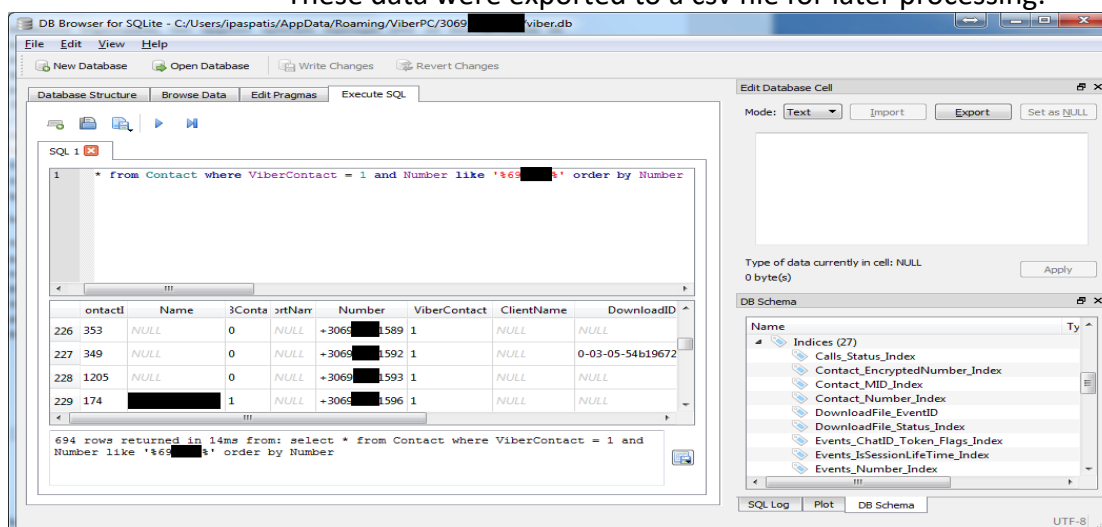


Figure 24: Screenshot from SQLite during datamining

4. Methodology of the de-anonymization of the test sample

With the intention to de-anonymize our data set we used two methods. In the first method, we used three public and free databases, Greekphones, Sync.me and TrueCaller. These databases contain freely given personal data from various sources, such as public data records or personal data that were disclosed on social networks such as Facebook, LinkedIn and Twitter (Loie Favre, 2014). We should notice that Sync.me is also using another method to collect data. When Sync.me is installed in a cellphone it uploads all phone numbers that are stored in the device's contact list or in the Gmail account contact list (Heather Clancy, 2013). For the database "Greekphones"

we created a custom-made crawler based on java and the jsoup library. Our crawler automatically parses the Name and Surname, the address, the postal code and, in some cases, the occupation of a given set of Greek phone numbers. The other two databases use the captcha authentication system and limit the time of use. For this reason, we conducted a semi-automatic parse: (a) we connected to these two databases through the Tor network, in order to override the limited times of use, (b) we authenticated manually at least one time, and (c) we used a custom-made java program to find if a given number that wasn't identified with our first crawler, exists in the other two databases. In case of a query limit lockout, we created a new Tor identity and re-authenticated through captcha. For our second method, we used the google reverse image lookup. We created an ftp server and uploaded the profile pictures we discovered during our data mining exploration. After, we created a java program for data handling and used Google reverse image API as an imported library. The program tried to identify a person using the hyperlink profile image provided by our ftp server. If there were similar pictures, then a web browser would open a webpage with these similar pictures for manual identification. Unfortunately, Google has discontinued officially supporting this API (Google, 2011) and since November 2016 it prevents the automatic parse of the findings in aim to promote its new Google Custom Search API. This API limits the searches to 100 per day and, then, charges each search based on the number of results (Google, 2016). If a person used the same profile picture in one or more social networks, then we were able to discover the name of that person.

We distinguish two types of de-anonymization. First, full de-anonymization (or de-anonymization) is considered when we disclose at least the name and the surname of an entity simultaneously. Second, semi de-anonymization occurs when we disclose the name or the surname or a nickname for an entity.

Both data mining and the de-anonymization can be viewed in greater detail in figure 2. We separated figure 2 in ten steps as follow:

Step 1: we created a pseudo-random .csv with a simple python script

Step 2: we uploaded the .csv file to a gmail account

Step 3: In this step the gmail contacts synchronized with our lab smartphone

Step 4: we synchronized the smartphone with our lab pc

Step 5: we mined the data from the sqlite DB using DB browser and simple sql scripts

Step 6: we prepared our databases for handling

Step 7a-8a: we uploaded the viber images that we mined from step 5 to an ftp server in order to do our reverse image lookup

Step 7b-8b: we used our java custom parser to get public information (name, surname, address) about our dataset's subjects

Step 9: we reviewed our results from step 8a and manually we removed the inconvenient data.

Step10: we merged our results to a datasheet file and we conducted our statistical analysis.

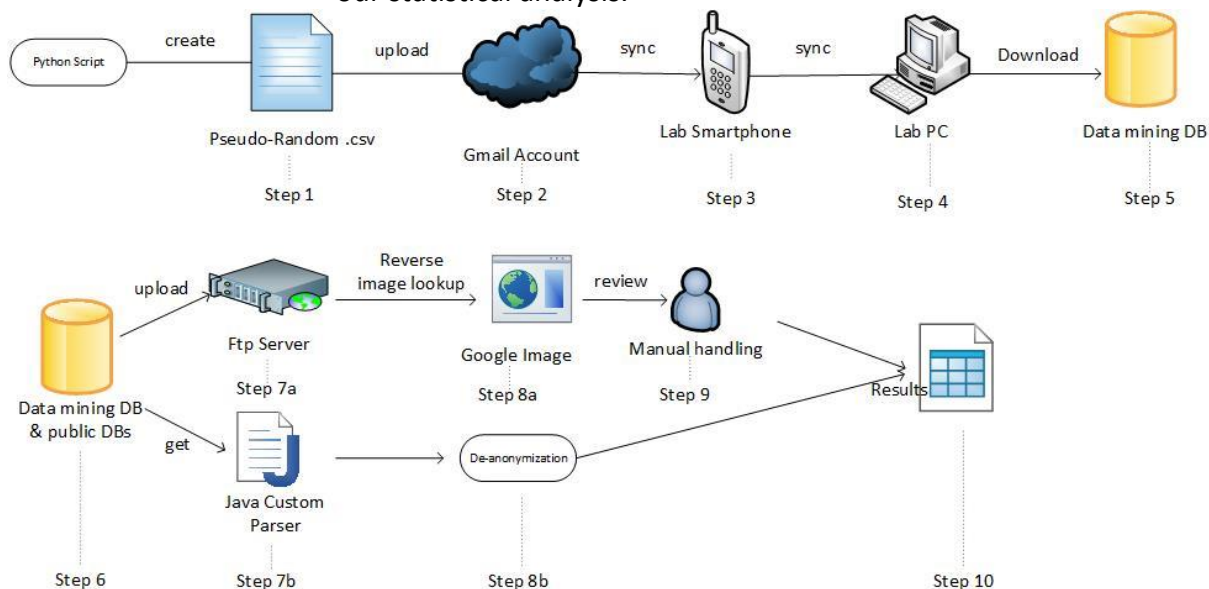


Figure 2: Steps of data de-anonymization

5. Methodology of Privacy Awareness Exploration

Within our research we also investigated the privacy awareness level of Viber users regarding the mobile app's privacy settings. For this reason, we designed an empirical study that compares the reported behavior with the actual behavior of Viber users. We followed the approach of convenience sampling and invited participants who were accessible to the researchers. All participants were holders of a computer science diploma. Our sample included 20 individuals, who are users of the Viber mobile app and agreed to participate, being aware of the monitoring processes that we followed.

In order to monitor actual behavior, we included the 20 users in the dataset for 30 consecutive days. The purpose of the survey was to

investigate if the Viber's users are aware regarding the features of Viber, such as the possibility of personal data and habits exposure. Also, to explore if they were aware of the potential risks of the blind consent to the privacy policies. The purpose of the monitoring was to determine if we could expose through Viber some of our subjects' habits, such as the time they turn on/off their device or other habits. The monitoring was taking place three times a day at 8.00am, 4.00pm and 10.00pm.

In order to record reported behavior, we distributed a questionnaire that we designed using Google Forms due to its characteristics (e.g., speed of processing the results, security and ease of use). The questionnaire was distributed online via e-mail to our sample. The survey was running for 30 days and all participants replied to the questionnaire.

6. Results and Statistical analysis

6.1 De-anonymization results

After we recovered the accumulated data, we had appropriate and sufficient data to proceed to statistical analysis. From the total of 2000 pseudo-random cellphone numbers it emerged that 682 subscribers have installed Viber for mobile (34%). From the 682 entities, the 316 entities (46.3%) have uploaded a profile picture. From the entities that have uploaded a profile picture we have de-anonymized or semi de-anonymized 258 of them (82%) while from the entities that hadn't upload a profile picture we have de-anonymize or semi de-anonymize 291 of them (80%). In total, from both categories we have de-anonymize or semi de-anonymize 549 entities. To conclude, we have fully de-anonymized 475 entities (75%). In table 1 we present our results in greater detail.

Description	Sample analysis
Entities with Viber installed (n=2000)	682 (34%)
Entities with profile picture (n=682)	316 (46%)
De-anonymized entities with profile picture (n=316)	258(82%)
Full de-anonymized entities with profile picture (n=258)	220 (82%)
Semi de-anonymized entities with profile picture (n=258)	38 (18%)
De-anonymized entities without profile picture (n=366)	291 (80%)
De-anonymized entities without profile picture (n=291)	255 (88%)

Semi de-anonymized entities without profile picture (n=291)	36 (12%)
De-anonymized entities with or without profile picture (n=549)	475 (87%)
Semi de-anonymized entities with or without profile picture (n=549)	74 (13%)
De-anonymized entities in total (n=682)	549 (80%)
Fail to de-anonymize entities (n=682)	133 (20%)

Table 1. Results of the sample de-anonymization process

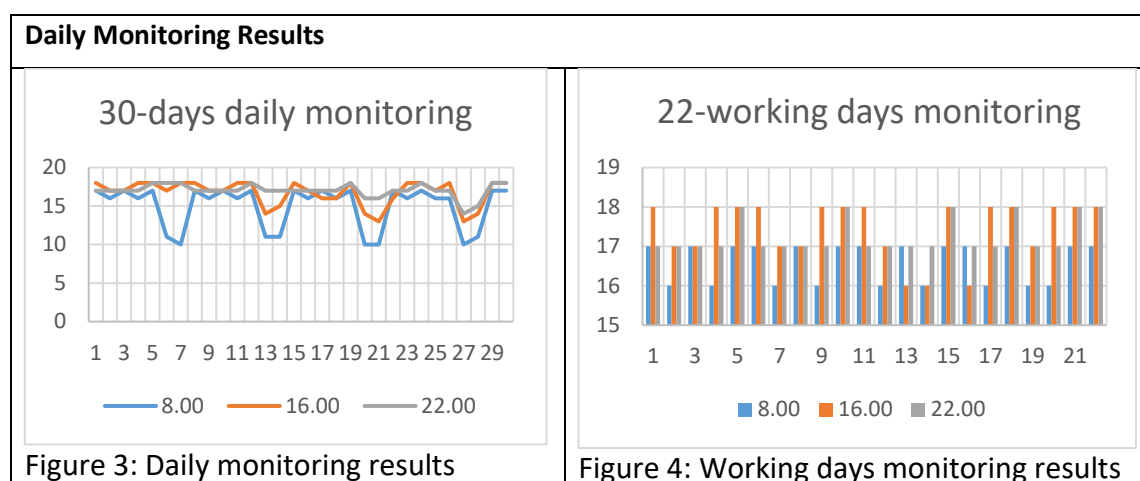
6.2 Empirical questionnaire results

Our findings from the online questionnaire reveal that Viber users have a low level of privacy awareness regarding the possibility of personal data exposure and habits' inference, as well as the potential risks of the blind consent to Viber's privacy policy. From the perspective of privacy awareness, our findings showed that all our subjects - except one - never changed their profile picture (95%). 90% of our subjects answered that they didn't read, or didn't remember if they read, the privacy policy before installing Viber. 85% stated that even if they had read it, they weren't sure if they would have understood it. 90% stated that they didn't know that the data they publish on Viber is considered as public data. The same percentage stated that they didn't know that Viber, according to its privacy policy, can share users' public data with other cooperating social networks, like Facebook or Twitter. 50% stated that they find it at least difficult to change Viber's privacy settings. 65% of our subjects stated that they didn't know it's possible to identify someone through reverse image lookup, while 75% answered they didn't know that it was possible for someone to be de-anonymized via her phone number. 60% stated that they didn't know that through Viber they could be a target of spam messages or phishing attacks nor that they could be a target of physical or electronic monitoring. Nevertheless, 35% would suggest to a friend to install Viber, while 60% will continue to use it.

6.3 Daily Monitoring Results

From our daily monitoring of the 20 subjects, the following findings were obtained: The 74.9% of our participants had been connected to Viber at 8.00 am (+/- 2 hours) at all days. The percentage increased during working days at 82.9% (+/- 2 hours). From this, we conclude that most our subjects preferred to connect to Viber from their work space. At 4.00 pm and 10.00 pm the percentage of connected subjects

was approximately at 87% the most of the days. From a privacy perspective, we can conclude that our subjects are more vulnerable to spam messages or unwanted advertising phone calls within this time. Our findings are analyzed in greater detail in the following figures (3, 4). Also, we monitored their profile pictures changes. Only one of the subjects changed his/her profile picture (5%). From the side of privacy this is positive. If the de-anonymization process fails to identify a person through reverse image lookup in first place, it is less probable that (s)he will be identified with this process in the future.



From our findings, we conclude that computer science knowledge is not sufficient to enhance individual privacy awareness. Most our subjects didn't read Viber's privacy policy. Even if they had read it they fear that they wouldn't understand it. The fact that almost all our subjects did not know that the data they share with Viber is considered to be public data demonstrates a basic lack of privacy awareness with regard to personal data. Finally, since they do not change their privacy settings, they can be an easy target for many potential threats, such as spam messaging or monitoring.

7. Contribution and guidelines

7.1 Contribution to the Research community

The importance of users' awareness has been pointed out by the literature review in section 2 and by our experimental and survey results. We proved that even without any prior information about the records of our pseudo-random dataset, we could de-anonymize 75% of our subjects, revealing their names, surnames and/or home addresses. It is important to consider that interested companies (e.g.,

advertisers or public data handlers) perform such de-anonymization and the derived information is a useful tool for their practices. When it comes to the user's privacy, it appears to be difficult for the average user to keep their personal data from becoming public due to lack of awareness. Therefore, this exposes them to various types of threats, such as physical and electronic monitoring, hacking or spam messaging. The above threats can be abridged by increasing user's privacy awareness, in conjunction with the development of appropriate mobile programming protocols for the developers.

7.2 Guidelines for the Privacy Regulation

Authorities regarding mobile app developers

Our research has demonstrated the ease of acquiring personal data using mobile app characteristics. Our experiment would not have been possible if some personal data processing principles had been followed by the mobile app. We suggest that the personal data protection authorities consider our findings and enforce a set of principles for mobile developing companies and mobile app developers, in order to protect the mobile app users:

Any mobile application should request the users' consent whenever someone tries to add them to their contact list. Even if some mobile apps use implicit consent, we argue that explicit consent is imperative for the provision of this right by a user. Therefore, the default setting for a given user should be to disable the automatic connection with others, and it be at the discretion of users to enable the feature.

When the mobile app settings allow the user to expose personal data, such as profile pictures or names, the default settings should disable the exposure and it should be at the users' discretion to activate it.

When the mobile app collects information that may allow the exposure of personal habits (e.g., state the device, turned on or off) the default settings should disable the collection of such data and be activated only after users' explicit consent. The users should be warned about the potential risks they may face.

7.3 Guidelines for mobile app users

From our experiment results it is shown that it is possible to expose users' personal data or habits regarding the features of a mobile app. Our experiment wouldn't have succeed if an informed user had disabled some of these characteristics. Below we provide guidelines that will help users to protect their data.

To mobile app users we recommend:

Always read the privacy policy before accepting it. It may contain valuable information about your personal data handling.

Read the mobile app permissions that are granted during the installation. Disable the permissions you consider as dangerous even if this limits the mobile app's functionality (this feature is available only from Android version 7 and on).

Check the mobile app's privacy settings before you use it or add your personal information. They may contain features that may expose your personal data, such as usual or temporary location, name, etc.

We recommend to never upload a real profile picture. It can be used to de-anonymize you or to link your entity to the social networks you may use.

If there is a setting that prevents someone to add you to a social network without your consent, consider to enable it. Since many personal data crawlers use auto-join features to profile you, your authorization to such an act, can be proved useful to keep your information private.

Conclusions

In this paper, we have proved that it is possible to de-anonymize Viber users without any prior knowledge about their identity. We selected a pseudorandom sample of phone numbers and successfully de-anonymized 75% of 682 Viber users by acquiring and disclosing their real name, surname and address. Our experiment was successful due to some low security characteristics of Viber, that have been reported also by Appelmann et al. (2011). We have applied software tools for the data mining process, using only freeware tools and software we developed ourselves and de-anonymize our dataset with custom made crawlers in conjunction with three, free to use, online phone databases. From the above, we conclude how important is to raise users' awareness for privacy implications in Viber and other mobile apps in order to protect their personal data.

We investigated the privacy awareness level of Viber users regarding the general features of Viber app that could expose their personal data, as well as the importance of reading the privacy policies. Our exploratory survey included 20 Viber users as participants, all of them holding a computer science diploma. The results verified our initial conjecture about the low level of privacy awareness regarding the general features of Viber that could expose their personal data and put themselves in potential risk. Indeed, most of the participants were not aware that they could be identified with the use of online databases, that their personal habits could be monitored or that their private data is considered as public data after they disclose them, voluntarily on mobile applications. Despite the high level of computer science education of the participants, they weren't tempted to read

Viber's privacy policy or alter Viber's privacy settings. Our results emphasize the need to raise privacy awareness of Viber users and of mobile applications, in general.

Based on our findings, we provided general guidelines for the personal data regulation authorities and more specific recommendations for the profession of mobile apps developers, all of which aim to protect the personal data of mobile apps users by default. We also offered specific guidelines to mobile apps users with the main intention to help them protect their personal data, especially since misuse of their data could put them at risk.

Appendix

A. Demographics

1. Gender?

Male\Female

2. What is your age?

17 or younger\18-20\21-29\30-39\40-49\50-59\60+

3. What is the highest level of school you have completed or the highest degree you have received?

Less than high school degree\High school degree or equivalent (e.g., GED)\Some college but no degree\Associate degree\Bachelor degree\Masters degree\P.H.D. Graduate degree

4. Do you have an account on a social networking website (like Facebook or Twitter)?

Yes\No\Maybe

5. About how many contacts do you currently have on social networking websites?

0-100\100-500\500+\I have no social network profile

6. About how many of your "friends" on social networking websites have you met in person?

All of them\Most of them\About half of them\A few of them\None of them

7. How often do you change your profile picture on social networking websites?

Extremely often\Very often\Moderately often\Slightly often\Not at all often

8. How easy do you think it is to modify your settings on your social networking websites?

Extremely easy\Very easy\Moderately easy\Slightly easy\Not at all easy

9. If you could use only one of the following social networking services, which would you use?

Facebook\Google+\MySpace\Viber\Twitter\Whats App

10. When you're on social networking websites, about how much of your time do you spend looking at what other people have posted?

All of it\Most of it\About half of it\Some of it\None of it

11. When you're on social networking websites, about how much of your time do you spend posting things about yourself?

All of it\Most of it\About half of it\Some of it\None of it

B. What about Viber (Awareness)

1. Had you read the Privacy Policy Before you installed Viber?

Yes\No\Maybe/I can't remember/I don't want to answer

2. If you read the Privacy Policy did you understand it?

Probably No\Yes\No/I'm not sure/I don't want to answer

3. Do you know that by installing viber your viber data are now considered as public data?

Yes\No/I don't know/I don't want to answer

4. Do you know that according to Viber's Privacy Policy Viber can share your data with third parties e.g. social networks like Facebook and Twitter?

Yes\No/I don't know/I don't want to answer

5. Do you know that Viber can collect data due to the agreement with other social networks like Facebook and Twitter?

Yes\No/I don't know/I don't want to answer

6. Do you know that someone could find your profile picture and other personal data like your full name or/and your profession/occupation?

Yes\No/I don't know/I don't want to answer

7. Do you know that strangers, employers or friends can follow your habits through Viber e.g. what time you switched on your mobile device or check your connection status?

Yes\No/I don't know/I don't want to answer

8. Do you know that through Viber you can be a target of spam messages?

Yes\No/I don't know/I don't want to answer

9. Do you know that through Viber you can be a target of electronic phishing?

Yes\No/I don't know/I don't want to answer

10. Do you know that by using linked data from multiple social networks such as Viber, Twitter, Facebook you may become electronic and physical monitoring target?

Yes\No/I don't know/I don't want to answer

11. After the above will you recommend Viber to a friend?

Yes\No/I don't know/I don't want to answer

12. Will you continue using Viber?

Yes\No/I don't know/I don't want to answer

References

- Almuhimedi H, Schaub F, Sadeh N, Adjerid I, Acquisti A, Gluck J, et al. (2014). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 787–796.
- Appelman M, Bosma J, Veerman G, (2011). Viber Communication Security. Unscramble the scrambled. System and network of engineering, University of Amsterdam. [online]. Available at: https://www.academia.edu/5717224/Viber_Communication_Security_unscramble_the_scrambled_Contents. [Accessed 25 Jul. 2017].
- Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, 313-324.
- Benenson Z, Reinfelder L. (2013). Should the users be informed? On differences in risk perception between Android and iPhone users. In Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK.
- Boksasp, Trond, and Eivind Utne (2012). "Android apps and permissions: Security and privacy risks."
- Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M. and Kargl, F. (2014). Privacy implications of presence sharing in mobile messaging applications. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia - MUM '14.
- Capistrano PE, Chena VJ (2015). Information privacy policies: The effects of policy characteristics and online experience. *Comp Standards Interfaces* 2015;42:24–31.
- Fletcher, K. (2003). Consumer Power and Privacy: The Changing Nature of CRM. *International Journal of Advertising*, 22, 249-272.
- Caruso, D. (1998). The Law and the Internet Beware. *Columbia Journalism Review*, 37 (1), 57-61.
- Gillmor, D. (1998). Violating Privacy is Bad Business. *Computerworld*, 32 (12), 38-39.
- Global Internet User Survey (2012), Internet Society <http://www.internetsociety.org/survey>
- GreekPhone. Lexicon Software GreekPhones. [online]. Available at: <http://www.11888.gr>. [Accessed 25 Jun. 2017].
- Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model. *Behavior and Information Technology*, 23 (6), 413-422.
- Google (2011). Google Image Search API (Deprecated). [online]. Available at: <https://developers.google.com/image-search/v1/jsondevguide>. [Accessed 25 Jun. 2017].

- Google (2016). What is Google Custom Search. [online]. Available at: <https://developers.google.com/custom-search/json-api/v1/overview>. [Accessed 25 Jun. 2017].
- Govani T., Pashley H. (2007). Student Awareness of the Privacy Implications while Using Facebook. Unpublished manuscript, 2007. [online] Available at :<http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf> . [Accessed 25 Jun. 2017].
- Gross, R., Acquisti, A. and Heinz, H. (2005). Information revelation and privacy in online social networks. Proceedings of the 2005 ACM workshop on Privacy in the electronic society - WPES '05, [online] pp.71-80. Available at: <https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf> [Accessed 25 Jun. 2017].
- Heather Clancy (2013). Yearning for a unified contact list? Sync.Me wants your number. [online]. Available at: <http://www.zdnet.com/article/yearning-for-a-unified-contact-list-sync-me-wants-your-number>. [Accessed 25 Jun. 2017].
- Loie Favre (2014). HOW TO SYNC CONTACT PHOTOS FROM FACEBOOK. [online]. Available at: <https://www.androidpit.com/how-to-sync-contact-photos-from-facebook>. [Accessed 25 Jun. 2017].
- McDonald A., Cranor L.F., (2008). The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008. Privacy Year in Review issue. [online] Available at: <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>. [Accessed 25 Jun 2017].
- Olmstead K. and Atkinson, M. (2015). Apps permissions in the google play. [online] Pew Research Center. Available at: <http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/> [Accessed 25 Jun. 2017].
- Pew Research Center (2015). Google Play Store Apps Permissions. [online] Available at: <http://www.pewinternet.org/interactives/apps-permissions>. [Accessed 25 Jun. 2017].
- Pitkänen, O. and Tuunainen, V. (2012). Disclosing Personal Data Socially — An Empirical Study on Facebook Users' Privacy Awareness. Journal of Information Privacy and Security, 8(1), pp.3-29.
- Rakib A, Ho S. (2011). Privacy concerns of users for location-based mobile personalization, In Proceedings of the International Conference on Information Resources Management;2011.
- Rust, R.T., Kannan, P.K., & Peng, N. (2002). The Customer Economics of Internet Privacy. Journal of the Academy of Marketing Science, 30, 455-464.
- Statista (2017a). Number of monthly active Facebook Messenger users from April 2014 to April 2017. Available at <https://www.statista.com/statistics/417295/facebook-messenger-monthly-active-users> . [Accessed 25 Jun 2017].
- Statista (2017b). Number of monthly active WhatsApp users worldwide from April 2013 to January 2017. Available at

- <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users> . [Accessed 25 Jun 2017].
- Statista (2017c). Number of unique Viber user IDs from June 2011 to March 2017. Available at <https://www.statista.com/statistics/316414/viber-messenger-registered-users> . [Accessed 25 Jun 2017].
- Sync.me. Caller ID and Phone Number Search. [Online]. Available at: <https://sync.me>. [Accessed 25 Jun. 2017].
- Tow W, Dell P, Venable J. (2008). Understanding information disclosure behaviour in Australian Facebook users. *J Inform Technol* 2008;25(2):126–36. [Online] Available at: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1004&context=acis2008> [Accessed 25 Jun. 2017].
- Truecaller: Caller ID & Dialer. [online] Available at: <https://play.google.com/store/apps/details?id=com.truecaller>. [Accessed 25 Jun. 2017].
- TRUSTe (2014), TRUSTe 2014 US Consumer Confidence Privacy Report, Consumer Opinion and Business Impact, Available at: <http://download.truste.com/dload.php/?f=4HKV87KT-447> . [Accessed 25 Jun. 2017].

Paper – V

AppAware: A Model for Privacy Policy Visualization for Mobile Applications

Research full-length paper

Track No 12- General Track

Paspatis, Ioannis, Ionian University, Corfu, GR, ipaspatis@ionio.gr

Tsohou, Aggeliki, Ionian University, Corfu, GR, atsohou@ionio.gr

Kokolakis, Spyros, University of Aegean, Samos, GR, sak@aegean.gr

Abstract

Privacy policies emerge as the main mechanism to inform users on the way their information is managed by online service providers, and still remain the dominant approach for this purpose. Literature notes that users find difficulties in understanding privacy policies because they are usually written in technical or legal language even, although most users are unfamiliar with them. These difficulties have led most users to skip reading privacy policies and blindly accept them. In an effort to address this challenge this paper presents AppWare, a multiplatform tool that intends to improve the visualization of privacy policies for mobile applications. AppWare formulates a visualized report with the permission set of an application, which is easily understandable by a common user. AppWare aims to bridge the difficulty to read privacy policies and android's obscure permission set with a new privacy policy visualization model. To validate AppAware we conducted a survey through questionnaire aiming to evaluate AppAware in terms of installability, usability, and viability-purpose. The results demonstrate that AppAware is assessed above average by the users in all categories.

Keywords: Awareness, Privacy policies, Mobile application permissions, Android.

1.Introduction

The great increase of smartphone users' in just 10 years from 85.000 users in 2010 to 2.5 billion in 2017 (Statista, 2017a) has led many computer program developers to turn to mobile application (apps) developers. In March 2017, Google Play Android Store had available for downloading nearly 3 billion mobile applications (apps) (Statista, 2017b) and the Apple store had more than 2.2 billion (Statista, 2017c) while just a decade ago these two webstores had almost 65.000 apps in total (Statista, 2018). A user who wants to install an app from the application store markets needs to read and accept its relevant privacy policy, commonly presented in a textual form. Cranor et al. (2008) concluded that it is unrealistic to believe that users would ever be capable to read every single privacy policy because of the length of such documents, the time that a user needs to spend and the legal language these policies are written in.

Our research objective is to demonstrate an alternate approach to represent a privacy policy, compared to the traditional textual approach. We introduce AppAware, a new visualization model for representing privacy policies for mobile apps. We show that AppAware can create a representative visualized privacy policy for a mobile app which is easy to read for the common user, enhances their privacy awareness and informs them for the threats they may encounter.

Many researchers have suggested alternate models of privacy policies representation by transforming them to more readable policies such as PPVM (Albalawi and Ghazinour, 2009) and RSLingo4Privacy (Da Silva et al., 2016). The main disadvantage of these models is that they transform a given policy, making it simpler and easier to understand, but they do not make more understandable the privacy threats deriving from a particular mobile application. Another disadvantage is that the above models didn't present any automation in transforming the privacy policies but it was necessary a human interaction for the transformation to get complete and validated. Contrary to the above models our approach does not focus on transforming a given privacy policy, but instead on creating a visualized privacy-threatening report regarding the specific permission set of a given mobile app. Our approach has many advantages over the traditional privacy policies and the existing privacy models, such as PPVM, in terms of efficiency and privacy accuracy. Moreover, the application of AppAware does not require any additional actions from mobile app developers. To the best of our knowledge, this is the first paper to propose a privacy threat visualization report deriving from the permission set of given mobile app. AppAware works both proactively and reactively by helping mobile app users to understand the threats they may encounter by accepting the terms and conditions of a given mobile app.

The paper is structured as follows. In section two we present the related work. Section three presents the methodology we followed and the preparation we made in order to develop AppAware. In section four, we demonstrate the steps we followed to evaluate AppAware through survey and we present our empirical questionnaire results (see Appendix). Finally, in section five presents the contribution of the paper and future work.

2. Privacy risks, awareness and policy visualization

In order to examine scholar disquisition associated to our research objective, we reviewed the literature on privacy policies as well as the available literature and resources on mobile apps' features and vulnerabilities. Our literature review analysis consists of three parts: potential risks/threats that mobile app users encounter, user privacy awareness, privacy policies' reading cost, and new visualization approaches. We narrow our efforts on Androids OS's and exclude IOS from our research because only Android's security and privacy settings can be changed by the user without any special expertise (Benenson & Reinfelder, 2013). In IOS users have limited capabilities of changing the security and privacy settings of an app. Apple (the Company providing IOS) claims that any app that is available through the official App store is reviewed by Apple's review process system for security and privacy issues. This feature does not allow users to change apps' settings.

2.1 Users' privacy concerns

Bandyopadhyay (2009) investigated the antecedents and consequences of consumer's online privacy concerns. He identified the main factors that influence consumers' privacy concerns such as vulnerability to information misuse, perceived ability to control the disclosure and use of private information, and characteristics of the consumer's cultural background. He also found that consumer's privacy concerns lead to limited willingness to disclose personal data online, to abandonment of e-commerce services or even to the total unwillingness to use the internet. Several studies had come to the same conclusions, that privacy concerns are determined by factors as awareness of information collection, perceived vulnerability to information misuse, experience with Internet use and cultural background of consumers (Sheehan and Hoy, 2000; Dinev and Hart, 2004; Bellman et al., 2004).

Buchenscheit et al. (2014) investigated if the use of the WhatsApp app could reveal users' behavior patterns and activities. Through an experiment they collected information on intended and actual behaviors (e.g., typical activities, typical sleeping hours), which they correlated with automatically obtained information from the usage of WhatsApp app. The participants, who didn't have significant privacy concerns for using the app, were surprised by the results highlighting that users do not fully realize the privacy implications of their online behaviors. Paspatis et al. (2017) used a pseudorandom dataset of 2000 telephone numbers and try to de-anonymize Viber users'. They found 682 users who had Viber installed and de-anonymized the 75% of them, revealing their full name, address and in about half of the cases their profile picture and occupation. After the de-anonymization process, authors conducted an empirical questionnaire and habits monitoring with 20 participants of the de-anonymization set. Most participants didn't have significant privacy concerns as they did not know that their data can be exposed and considered as public data or that someone can monitor their habits.

2.2 Users' privacy awareness and the cost of reading privacy policies

McDonald and Cranor (2008) tried to calculate the time and cost of users reading the privacy policies of each online service they visit. Through their empirical study they found out that every website user visit at least 1354 unique websites and that the average cost for the time they spend is 4.48 dollars per hour (if a Privacy Policy is read at home) or 35.86 dollars per hour (if the Privacy Policy should be read in office). They calculated that every website user would need 40 minutes per day for reading Privacy Policies when the average time of web surfing is 72 minutes per day. The total financial cost for all website users would be almost 781 billion dollars per year.

Kritzing and von Solms (2010) state that the most important factor for home users being vulnerable to security threats is their lack of awareness about risks of using the Internet. Karavaras et al. (2016) conducted an empirical survey with 190 participants to explore Facebook users' awareness regarding malicious link threats, revealing that their low awareness can make them vulnerable to such attacks. Church and Oliveira (2013) researched what users are concerned at most when they are using mobile apps such as WhatsApp. They found that most users were more concerned about the "last seen feature" wherewith someone can see at what exact time a user was read a message. Using this feature a user is capable to understand someone's habits such sleep routine. Almuhimedi et al. (2014) demonstrated that users low awareness regarding location data -among others by mobile apps and suggest a permission manager to protect their privacy. Graeef and Harmon (2002) found that privacy concerns vary by age, income and gender. In addition, they saw that younger users are more aware of their information leak while older users are concerned more about their financial privacy. To raise web users' awareness, Malandrino et al. (2013) produces NoTrace, a mozilla firefox add-on that monitor users' browsing activity and inform them what personal and sensitive information they leak towards third-party such as advertising companies. NoTrace is also capable to block or or alter the browser fingerprint information. Hazari and Brown (2013) conducted a questionnaire-based survey with 157 business students enrolling regarding privacy behavior, trust policies and technology and correlate their results with others researchers' previous studies. His results showed that individuals are concerned about their privacy and would like to control their digital reputation as it can directly impact their business relationships and/or employment prospects. He also suggested the importance of awareness training providing by institutions to make students aware of privacy issues.

2.3 Privacy policy visualization approaches

Barker et al. (2009) described purpose, visibility, granularity, retention and constraints as the key elements that form a privacy policy and categorized their research around a conceptual framework for data privacy. Ghazinour et al. (2009) presented a framework for visualizing privacy policies called Privacy Policy Visualization Model (PPVM). They suggested a graphical tool that combines Entity Relationship Modeling, Entity Relationship diagramming and the elements described by Barker et al. (2009) to show the association between the data provider, the collector and the data they collected. Albalawi and Ghazinour (2009) have evaluated PPVM using Jensen's (2014) Structured Analysis of Privacy (STARP) heuristics evaluation framework to inspect privacy usability and vulnerabilities and suggested solutions to improve usability issues encountered during evaluation. Domiongo-Ferrer (2009) suggested a three-dimensional conceptual framework for privacy policies. His proposal identifies privacy issues in a privacy policy that

relate to the data provider, house and third-parties with every issue is grouped to one these categories. Anwar et al (2009) described an access control model of assessing privacy policies through visualization. Da Silva et al (2016) suggested a multi-language framework tool based on Lingo programming language called RSLingo4Privacy which intends to improve the specification and analysis of a privacy policy. Their tool automatically classifies extracted text statements and text snippets from a policy into five classes: Collection -which data are collected; Disclosure -which data is disclosed and to whom; Retention -how long data will be available; Usage -why are they collecting users' data; and Informative -which is a general purposes class and after the conversion provides an improved version of the policy in a natural language. Kelley et al (2009) conducted a survey testing the readability, accuracy and comprehension of five different format privacy policies: full text policy in natural language, standardized table format, short standardized table, short natural language and layered notices. They concluded that the best results in all categories were provided by the two table-type policies. Micallef et al. (2017) conducted an empirical study to investigate users' preferences on multiple types of privacy policies such as combinations of visual nudges, vibration, audio and speech on mobile apps. They revealed that users are annoyed when low priority notification nudges use audio or speech to alert them and developers should prefer non – salient privacy nudges to inform them. Keith et al (2018) examined an approach to improve privacy policies through the design and usage of mediated content, such as video instead of textual privacy policies. They aimed to explore if design factors such as gender, animation style, music tone or color scheme affect users' perceived risk, perceived benefits and disclosure decisions. Their results indicate that the most effective video privacy policies are those that use female narrators with vibrant color palettes and light musical tones.

Research shows that users have low privacy awareness and privacy concerns which are raised when understanding the actual privacy threats. Studies also show that users facedifficulties on reading privacy policies, such as the difficult legal language they are written in. All the above, do not create the appropriate conditions for conscious consent for the disclosure of personal information. Additionally, the users are confronted with a fragmented approach, since they need to read and understand the different privacy policies of the million mobile apps that are available. Therefore, there is a challenge on creating a single approach that can assist users and resolve the problem of the million privacy policies the users need to read. AppAware target to address this issue by using as a foundation for user awareness the permission set of the mobile apps (which is what they do and not what they state they do) and not the privacy policy. This gives the opportunity to automatically transform a privacy policy to a visualized privacy report, with representative pictures and easy to read for the common user.

3. Methodology

In this section, we analyze our methodology for developing AppAware and for validating its effect on users' privacy awareness.

3.1 Technical Methodology

We developed AppAware with Java JDK. We chose to use java instead of other programming languages because of its compatibility with different operating systems such as Windows, Linux, IOS and because it

is easily modified to be used for android mobile devices (Android OS and its applications are written in a version of Java). To store our data, AppAware's global database is based on MySQL while there is a standalone version of AppAware that is using SQLite DB. We chose MySQL because its freeware, supports more than 10 million records per table while it supports and performs fast enough with many users simultaneously. The local version of AppAware is using SQLite db to store data. We chose SQLite to release users of the requirement of a local database installation such as MySQL or SQL Server. AppAware is following a different approach than the new models we referred in the related work section. Instead of trying to transform a given mobile app privacy policy into more comprehensive forms, AppAware creates a visualized report with images and privacy descriptions in natural language of the permissions that are obtained from an App during installation or use. In particular, we have matched every permission from the Android's permission set with a representative image, a permission description and a possible threat. We obtained permissions' descriptions from Pew Research (Olmstead and Atkinson, 2015) and we chose the associated images and possible threats based on google's image matching. We believe that the descriptive images of the visualized report will catch the eye of users and increase their privacy awareness. In this way, users may read the description of the permission they are giving access as well as the possible threat(s) they may encounter. Our module is consisted of four java classes: a) Dataset, b) AppData, c) AppHandling and d) AppPerms which cooperate as follows:

Dataset Class. This class includes all Android's Permissions. It is consisted of 3 fields: android's permission name, permission privacy description and potential threat. As we mentioned before permission privacy descriptions obtained from Pew Research (Olmstead and Atkinson, 2015) previous work. We chose these descriptions because of the natural language they used which is easy understandable for the common user.

AppData. This is AppAware's main class. From this class users can see which android applications are stored in the database as well as which permissions can be obtained during installation. Also, they can export the visualized report (figure 2, 3). For the purposes of our experiment we include to AppAware the twenty most famous applications for the 2017 (Hartmans, 2017).

AppHandling. From this class a user can add a new app that does not included to AppAware's database and send it for evaluation and permission matching. In order to add a new app, user must update AppAware's database to it latest version. Thus, users can also see stored apps with minimum details. After the app's evaluation and permission matching, AppAware's user is ready to create the new visualized report.

Figure 1 below shows AppAware's Schema:

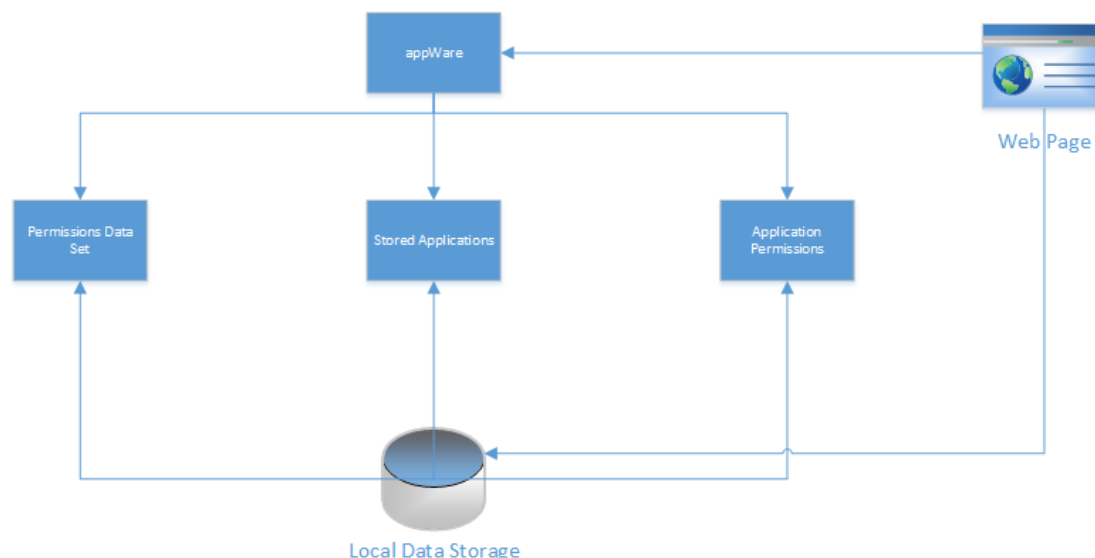


Figure 25. AppAware Schema

AppPerms. This is the class where more advanced users and administration team can match a new application with the permissions it gains upon install/use. After the matching, app's permissions are uploading to AppAware's web database in order to update AppAware's users. To avoid spam or false permissions matching, AppAware's Server will wait for a non-specified number of users to send permissions matching for the same app. After this step server will correlate the results and if there is a specific number of permissions matching will send an updated data set to AppAware's clients.

Permission : Precise location GPS and network_based
Threat : Location



Description : Allows the app to get your precise location using the Global Positioning System GPS or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use thi

Figure 26. Representative picture and description and threat from the visualized report

Permission : Directly call phone numbers
Threat : Overcharge



Description : Allows the app to call any phone number including emergency numbers without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services

Figure 27. Representative picture and description and threat from the visualized report

All AppAware classes are been showed to the Figures 4, 5, 6, 7 below.

id	application	description	id	permission	description	Allows access to	Threat
0	null	null	2	Full network acc...	Allows the app t...	Hardware	none
1	Facebook	facebook desc	3	View network co...	Allows the app t...	Hardware	Location
3	Linkedin	Linkedin data	4	Test access to p...	Allows the app t...	Hardware	none
5	Instagram	Instagram App	5	Modify or delete t...	Allows the app t...	User Info	Data Loss
6	Adobe Reader	Adobe Reader	6	Read phone stat...	Allows the app t...	User Info	Location
7	Amazon Kindle	Amazon Kindle	7	Prevent device fr...	Allows the app t...	Hardware	Power Abuse
8	Dropbox		8	Precise location ...	Allows the app t...	User Info	Location
9	ebay		9	View Wi-Fi conn...	Allows the app t...	User Info	Triangulation
10	Evernote		10	Control vibration	Allows the app t...	Hardware	None
11	WatchESPN		11	Approximate loc...	Allows the app t...	User Info	Location
12	Gmail		12	Receive data fro...	Allows apps to a...	Hardware	Overcharge
13	Chrome		13	Find accounts o...	Allows the app t...	User Info	Link Data
14	Google Maps		14	Take pictures an...	Allows the app t...	User Info	Privacy
15	Pandora		15	Run at startup	Allows the app t...	Hardware	Abuse
16	Shazam		16	Directly call phon...	Allows the app t...	User Info	Overcharge
17	Skype		17	Read your conta...	Allows the app t...	User Info	Privacy
18	Spotify		18	Record audio	Allows the app t...	User Info	Privacy
19	Twitter		19	Retrieve running ...	Allows the app t...	User Info	Link Data
20	WhatsApp		20	Read Google se...	Allows this app t...	Hardware	Statistics
21	YouTube		21	Read call log	Allows the app t...	User Info	Privacy
22	Viber		22	Google Play lice...	Can check if you ...	Hardware	None
23	Hotmail	Hotmail Client	23	Send SMS mess...	Allows the app t...	User Info	Overcharge
			24	Access extra loc...	Allows the app t...	User Info	Location
			25	Set wallpaper	Allows the app t...	Hardware	None
			26	Modify your conta...	Allows the app t...	User Info	Corrupt File Syst...

Figure 28. Class AppPerms

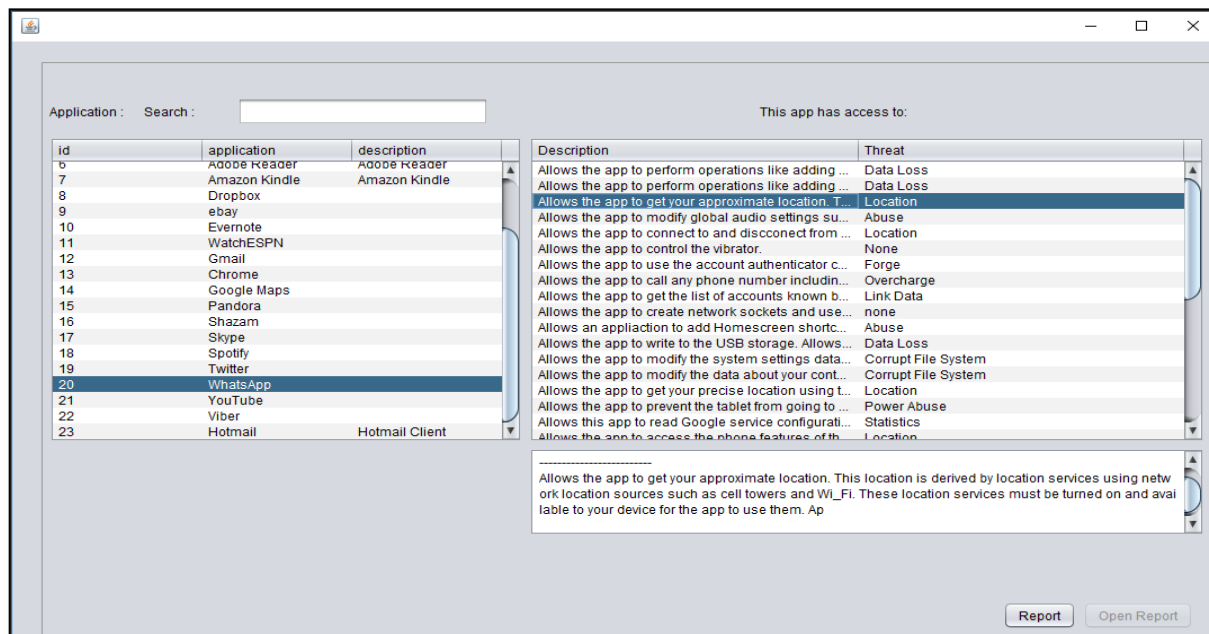


Figure 29. Class AppData

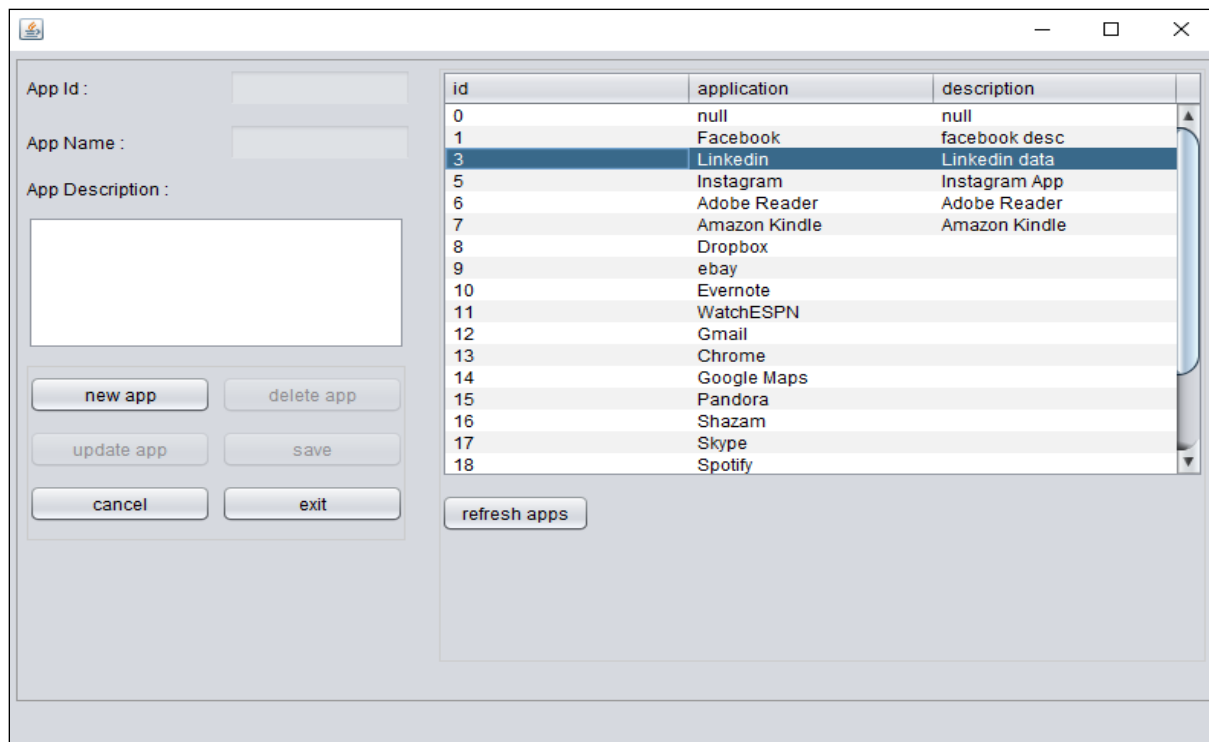
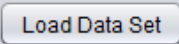


Figure 30. Class AppHandling



id	permission	description	Allows access to	Threat
2	Full network access	Allows the app to cr...	Hardware	none
3	View network conne...	Allows the app to vi...	Hardware	Location
4	Test access to prote...	Allows the app to te...	Hardware	none
5	Modify or delete the ...	Allows the app to wr...	User Info	Data Loss
6	Read phone status ...	Allows the app to ac...	User Info	Location
7	Prevent device from ...	Allows the app to pr...	Hardware	Power Abuse
8	Precise location GP...	Allows the app to ge...	User Info	Location
9	View Wi-Fi connecti...	Allows the app to vi...	User Info	Triangulation
10	Control vibration	Allows the app to co...	Hardware	None
11	Approximate locatio...	Allows the app to ge...	User Info	Location
12	Receive data from i...	Allows apps to acce...	Hardware	Overcharge
13	Find accounts on th...	Allows the app to ge...	User Info	Link Data
14	Take pictures and vi...	Allows the app to ta...	User Info	Privacy
15	Run at startup	Allows the app to ha...	Hardware	Abuse
16	Directly call phone n...	Allows the app to ca...	User Info	Overcharge
17	Read your contacts	Allows the app to re...	User Info	Privacy
18	Record audio	Allows the app to re...	User Info	Privacy
19	Retrieve running ap...	Allows the app to ret...	User Info	Link Data
20	Read Google servic...	Allows this app to re...	Hardware	Statistics
21	Read call log	Allows the app to re...	User Info	Privacy
22	Google Play license...	Can check if you ha...	Hardware	None
23	Send SMS messages	Allows the app to se...	User Info	Overcharge

Allows the app to view information about Wi-Fi networking such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.

icon :

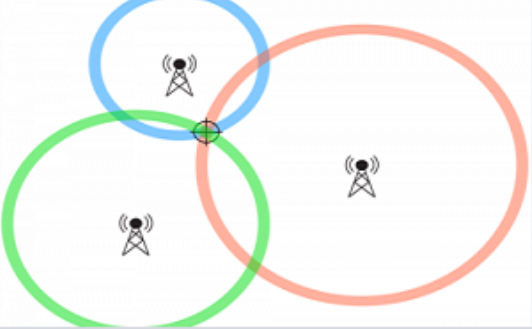


Figure 31. Class Dataset

AppAware is support database update function for future implementation. In case of a ready Apps-permission dataset be available in public, it will be capable to support as many apps there are in the dataset. Thus, AppAware users can create and export their dataset that created with AppData class and send it to AppAware’s team for evaluation and import to the web database. Until now, Playstore does not giving public and massive access to their apps database and their permission set. In case of Playstore give in public an app-permission set in public, AppAware will automatically update its global database.

3.2 Evaluation methodology

In order to evaluate AppAware, we conducted a survey using a questionnaire. The purpose of the survey was to investigate how mobile app users evaluate AppAware’s Visualized Report in terms of installability, usability, and viability-purpose compared to the traditional privacy policy of WhatsApp. The criteria and questions -except demographics- derived from ISO/IEC 9126-1 Software engineering — Product quality. All questions were Likert type and mandatory. To design and distribute the questionnaire (Appendix) we used Google Forms due to its popularity and characteristics, such as provision of real-time statistical results, the security and anonymity protection that it offers.

A requirement for participation to our survey was to install AppAware and use it for a trial period before answering the questionnaire. For this purpose, we did not target the general population, but instead we distributed the designed questionnaire to colleagues and undergraduate students of various disciplines. In order to test the effect of computer science knowledge on the AppAware evaluation we included a question about the profession or studies of the participants to maintain control over this characteristic of the sample. To complete the questionnaire, participants should first read WhatsApp’s privacy policy and then install AppAware and export the WhatsApp’s Visualized Report using it. The survey was running for 40 consecutive days and we received 73 answers. We consider that this number of responses is sufficient, especially given the obstacles caused by the requirement to install an unknown application or the refusal to participate because of installation problems. The 73 participants were equally distributed in terms of gender (36 Males, 35 Females, 2 unknown), were mainly aged between 18 – 34 years and most of them had at least bachelor degree. The demographics of the questionnaire are analyzed in detail in Table 1.

<i>Demographics (n=73)</i>		
Gender	Male	36 (49.3%)
	Female	35 (47.9)
	Other/Unknown	2 (2.7%)
Age	18-	1 (1.4%)
	18-34	54 (74%)
	35-44	10 (13.7%)
	44+	8 (11%)

Level of education	High School	4 (5.5%)
	Associate Degree	4 (5.5%)
	Bachelor Degree	32 (43.8%)
	Master's Degree	28 (38.4%)
	PhD Graduate Degree	5 (6.8%)
Profession	Economics	14 (19.2%)
	Political Science	7 (9.6%)
	Social Science	9 (12.4%)
	Computer Science	31 (42.5%)
	Educational Science	4 (5.5%)
	Other	8 (11%)

Table 22: Sample Demographics

4. AppAware users' evaluation

The questionnaire intended to collect users' opinion regarding aspects of AppAware installability, usability, and viability/purpose.

AppAware scored in all categories above average with mean values varying from 3.07 to 4.01 (scale 1 – 5). Our results in the category Viability and Purpose reveal that participants would prefer to use AppAware's Visualized Report than read the traditional privacy policy. In terms of installability, participants didn't confront any difficulties to install or understand how to use AppAware since the mean values in this aspect range from 3.48 to 4.04. Regarding usability and purpose, AppAware scored lower mean values ranging from 3.07 to 3.75.

The results are analyzed in Table 2, that includes three columns with column one demonstrating total mean values with all professions calculated, in column 2 we exclude participants with computer related degree and finally in column three we demonstrate the mean values only of participants with computer related degree.

Question	Total mean values	Mean values of participants
I believe It was easy to install AppAware to my system	3,81	4,02
I believe that I understand what the software does and its purpose	4,01	4,29
I believe that It was easy to learn how to use AppAware's basic functions	3,93	4,21
I believe that It was easy to learn how to use AppAware's advanced characteristics/functions/features	3,48	3,69
I believe that AppAware's Visualized report helped me to understand better the WhatsApp's privacy policy.	3,64	4,05
I believe AppAware's Visualized Report helped me to find the potential threats I may be confronted with using WhatsApp	3,68	4,05
I believe AppAware's Visualized Report was easy to read	3,47	3,83
I believe that AppAware's Visualized Report was easy to understand	3,38	3,74
I believe that the descriptions of AppAware's permission set are accurate.	3,75	4,10
I believe that the actual threat of AppAware's permission set is accurate.	3,74	4,10
I believe that AppAware is a stable Application	3,64	4,10
I believe that AppAware is a useful Application	3,53	3,88

I believe that AppAware is appropriate for its purpose	3,63	4,00
It was faster to read AppAware's Visualized Report than WhatsApp's privacy policy.	3,71	4,07
I prefer to use AppAware than to read the privacy policy of an App.	3,53	3,81
I believe that AppAware is a unique software tool	3,30	3,48
I believe that AppAware will be helpful to me	3,07	3,19

Table 2. Questionnaire results

5. Conclusions and future work

In this paper, we suggested a visualized model for representing privacy policies for mobile apps and the permissions they obtain upon installation. We processed android's permission set and we matched all permissions with a potential threat and a representative picture. We included in AppAware the 20 most popular applications for 2017 and then we evaluated AppAware using a survey with 73 participants. We focused our evaluation on installability, usability, and viability/purpose of AppAware. AppAware was evaluated above average in all categories especially in the usability category.

To the best of our knowledge, there is no other approach like AppAware. There are several approaches to visualize the text of a privacy policy, but there is no approach that enhances user understanding by creating a permission visualization model. The advantage of our approach is that a user does not need necessary to read all privacy policies of all mobile apps to visualize them but only to import the mobile apps and their permission set to AppAware's database. At the time of this paper we have included the 20 most popular mobile apps for the 2017. Unfortunately, we can't automatically import all available applications because Google Play store does not allow the use of crawlers or parsers.

AppAware provides significant implications for mobile app developers as well as marketplaces. Our findings show that app users would prefer to use a visualized report instead of the privacy policy of an app. App developers could provide the permission dataset they use in their apps. Researchers could use instantly and with ease their dataset to update public databases such as AppAware's. In this way, applications that target to mitigate users' privacy concerns and raise users' awareness could be up to date and help users to understand privacy threats and protect their data equally. For the same reason, we recommend app marketplaces to provide publicly the permission dataset for the apps they are hosting to assist transparency and give control to the users over their data. At the moment, AppAware is only a

client-server application created in java due to its multiplatform capabilities. In the future, we envision to develop AppAware into a web-accessible database as well as a web browser add-on.

Appendix

A. Demographics

1. What is your gender?

Male\Female

2. What is your age?

18-\18-34\35-44\30-39\40-49\50-59\60+

3. What is the highest level of school you have completed or the highest degree you have received?

Less than high school degree\High school degree or equivalent (e.g., GED) \Some college but no degree\Associate degree\Bachelor degree\Master's degree\P.H.D. Graduate degree

4. What is your profession?

Economics/Political Science/Social Science/Computer Science/Educational Science/Other

B. AppAware Evaluation (Likert Scale 1-5)

Installability

1. I believe It was easy to install AppAware to my system

Learnability

1. I believe that I understand what the software does and its purpose

2. I believe that it was easy to learn how to use AppAware's basic functions

3. I believe that it was easy to learn how to use AppAware's advanced characteristics/functions/features

4. I believe that AppAware's Visualized report helped me to understand better the WhatsApp's privacy policy.

Usability

1. I believe AppAware's Visualized Report helped me to find the potential threats I may be confronted with using WhatsApp.
2. I believe AppAware's Visualized Report was easy to read.
3. I believe that AppAware's Visualized Report was easy to understand.
4. I believe that the descriptions of AppAware's permission set are accurate.
5. I believe that the actual threat of AppAware's permission set is accurate.

Viability-Purpose

1. I believe that AppAware is a stable Application.
2. I believe that AppAware is a useful Application.
3. I believe that AppAware is appropriate for its purpose.
4. It was faster to read AppAware's Visualized Report than WhatsApp's privacy policy.
5. I prefer to use AppAware than to read the privacy policy of an App.
6. I believe that AppAware is a unique software tool.
7. I believe that AppAware will be helpful to me.

References

- Amran, A., Zaaba, Z., Singh, M. and Marashdih, A. (2017). Usable Security: Revealing End-Users Comprehensions on Security Warnings. *Procedia Computer Science*, 124, pp.624-631.
- Anwar, M., Fong, P., Yang, X. and Hamilton, H. (2010). Visualizing Privacy Implications of Access Control Policies in Social Network Systems. *Data Privacy Management and Autonomous Spontaneous Security*, pp.106-120.
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 706-714.
- Bandyopadhyay, S. (2011). Antecedents and Consequences of Consumers Online Privacy Concerns. *Journal of Business & Economics Research (JBER)*
- Barker K, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams. "A data privacy taxonomy." (in press) *BNCOD '09: The 26th British National Conference on Databases*. 12 pages, Birmingham, UK, 2009.
- Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, 313-324

Benenson Z, Reinfelder L. (2013). Should the users be informed? On differences in risk perception between Android and iPhone users. In Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK.

Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M. and Kargl, F. (2014). Privacy implications of presence sharing in mobile messaging applications. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia - MUM '14.

Budnitz, M. (1998). Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate. South Carolina Law Review, 49 (1), 847-886.

Church, K., & de Oliveira, R. (2013) What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS. 15th international conference on Human-computer interaction with mobile devices and services, Munich, August 30th, 2013, (pp. 352-361). ACM, Munich.

Da Silva, A., Caramujo, J., Monfared, S., Calado, P. and Breaux, T. (2016). Improving the Specification and Analysis of Privacy Policies - The RSLingo4Privacy Approach. Proceedings of the 18th International Conference on Enterprise Information Systems.

Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model. Behavior and Information Technology, 23 (6), 413-422.

Domiongo-Ferrer (2009). “A three-dimensional conceptual framework for database privacy”. In Secure Data Management 2007, volume 4721/2007, pages 193–202, Vienna, Austria, 2007.

Ghazinour, K. and Albalawi, T. (2016). A Usability Study on the Privacy Policy Visualization Model. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).

Graeff, T. and Harmon, S. (2002). Collecting and using personal data: consumers’ awareness and concerns. Journal of Consumer Marketing, 19(4), pp.302-318.

Hartmans A. (2017). The 20 most popular iPhone apps of 2017. Business Insider. Available at: <http://www.businessinsider.com/top-apple-iphone-apps-2017-12>

Hazari, S. and Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. Journal of Information Privacy and Security, 9(4), pp.31-51.

Jensen, C. (2004), “Toward a method for privacy vulnerability Analysis”, CHI 2004, extended abstracts on Human factors in computing systems, Publisher: ACM

Kambiz Ghazinour, Maryam Majedi, Ken Barker, A Model for Privacy Policy Visualization in 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2009.

Karavaras E, Magkos E, Tsohou A (2016) Low User Awareness Against social malware: An Empirical Study and Design of a Security Awareness Application.

Kelley, P., Cesca, L., Bresee, J. and Cranor, L. (2010). Standardizing privacy notices. Proceedings of the 28th international conference on Human factors in computing systems - CHI '10.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 840-847.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R. and Krishnamurthy, B. (2013). Privacy awareness about information leakage. *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society - WPES '13*.

McDonald A., Cranor L.F., (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* 2008. Privacy Year in Review issue. [online] Available at: <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>. [Accessed 25 Jun 2017].

Micallef, N., Just, M., Baillie, L. and Alharby, M. (2017). Stop annoying me! *Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17*.

Olmstead, K. and Atkinson, M. (2015). APPS PERMISSIONS IN THE GOOGLE PLAY. [online] Pew Research Center. Available at: <http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/> [Accessed 20 Jan. 2017].

Paspatis Ioannis, Tsohou Aggeliki and Kokolakis Spyros, "Mobile Application Privacy Risks : Viber Users' De-Anonymization Using Public Data" (2017). *MCIS 2017 Proceedings*. 32. Available at : <http://aisel.aisnet.org/mcis2017/32>

Raab, C.D. & Bennet, C.J. (1998). The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, 14 (4), 253-262.

Rindfleish, T.C. (1997). Privacy, Information Technology, and Healthcare. *Communications of the ACM*, 40, 92-100.

Saunders, K. & Zucker, B. (1999). Contracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers, and Technology*, 13 (2), 183-192.

Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy and Marketing*, 19 (1), 62-73.

Statista (2017a). Global cumulative shipments of smartphones using the Android operating system from 2007 to 2016. <https://www.statista.com/statistics/241943/forecast-of-global-cumulative-shipments-of-smartphones-using-android-os/>

Statista (2017b). Number of apps available in leading app stores as of March 2017. <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

Statista_(2017c). Number of available apps in the Apple App Store from July 2008 to January 2017. <https://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>

Statista (2018). Number of available applications in the Google Play Store from December 2009 to December 2017. <https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>

Tsohou, Aggeliki & Kosta, Eleni. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. *Computer Law & Security Review*. 10.1016/j.clsr.2017.03.027.

Wilson, S., Schaub, F., Dara, A., Liu, F., Cherivirala, S., Giovanni Leon, P., Schaarup Andersen, M., Zimmeck, S., Sathyendra, K., Russell, N., B. Norton, T., Hovy, E., Reidenberg, J. and Sadeh, N. (2016). The Creation and Analysis of a Website Privacy Policy Corpus. *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*.

Paper – VI



Information & Computer Security
Vol. 28 No. 1, 2020
pp. 116-132
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-04-2019-0049

The current issue and full text archive of this journal is available on Emerald Insight at:
<https://www.emerald.com/insight/2056-4961.htm>

AppAware: a Policy Visualization model for Mobile Applications

Abstract

Purpose: Privacy policies emerge as the main mechanism to inform users on the way their information is managed by online service providers, and still remain the dominant approach for this purpose. Literature notes that users find difficulties in understanding privacy policies because they are usually written in technical or legal language even, although most users are unfamiliar with them. These difficulties have led most users to skip reading privacy policies and blindly accept them. In an effort to address this challenge this paper presents AppAware, a multiplatform tool that intends to improve the visualization of privacy policies for mobile applications. **Design:** AppAware formulates a visualized report with the permission set of an application, which is easily understandable by a common user. AppAware aims to bridge the difficulty to read privacy policies and android's obscure permission set with a new privacy policy visualization model. Thus, we propose AppAware Parser, a mobile add-on that acts complementary with AppAware and helps mobile devices users to monitor the applications they installed to their smart device. **Findings:** To validate AppAware we conducted a survey through questionnaire aiming to evaluate AppAware in terms of installability, usability, and viability-purpose. The results demonstrate that AppAware is assessed above average by the users in all categories. **Originality:** In the best of our knowledge, there is no such approach as AppAware as an application nor AppAware parser as add-on.

Keywords: Awareness, Privacy policies, Mobile application permissions, Android.

1. Introduction

The great increase of smartphone users' in just 10 years from 85.000 users in 2010 to 2.5 billion in 2017 (Statista, 2017a) has led many computer program developers to turn to mobile application (apps) developers. In March 2017, Google Play Android Store had available for downloading nearly 3 billion mobile applications (apps) (Statista, 2017b) and the Apple store had more than 2.2 billion (Statista, 2017c) while just a decade ago these two webstores had almost 65.000 apps in total (Statista, 2018). A user who wants to install an app from the application store markets needs to read and accept its relevant privacy policy, commonly presented in a textual form. Cranor et al. (2008) concluded that it is unrealistic to believe that users would ever be capable to read every single privacy policy because of the length of such documents, the time that a user needs to spend and the legal language these policies are written in.

Our research objective is to demonstrate an alternate approach to represent a privacy policy, compared to the traditional textual approach. We introduce AppAware, a new visualization model for representing privacy policies for mobile apps. We show that AppAware can create a representative visualized privacy policy for a mobile app which is easy to read for the common user, enhances their privacy awareness and informs them for the threats they may encounter.

Many researchers have suggested alternate models of privacy policies representation by transforming them to more readable policies such as PPVM (Albalawi and Ghazinour, 2009) and RSLingo4Privacy (Da Silva et al., 2016). The main disadvantage of these models is that they transform a given policy, making it simpler and easier to understand, but they do not make more understandable the privacy threats deriving from a particular mobile application. Another disadvantage is that the above models didn't present any automation in transforming the privacy policies but it was necessary a human interaction for the transformation to get complete and validated. Contrary to the above models our approach does not focus on transforming a given privacy policy, but instead on creating a visualized privacy-threatening report regarding the specific permission set of a given mobile app. Our approach has many advantages over the traditional privacy policies and the existing privacy models, such as PPVM, in terms of efficiency and privacy accuracy. Moreover, the application of AppAware does not require any

additional actions from mobile app developers. To the best of our knowledge, this is the first paper to propose a privacy threat visualization report deriving from the permission set of given mobile app. AppAware works both proactively and reactively by helping mobile app users to understand the threats they may encounter by accepting the terms and conditions of a given mobile app.

The paper is structured as follows. In section two we present the related work. Section three presents the methodology we followed and the preparation we made in order to develop AppAware. In section four, we demonstrate the steps we followed to evaluate AppAware through survey and we present our empirical questionnaire results (see Appendix). In section five we propose AppAware Parser, a mobile app in progress concept model which acts complementary with AppAware. Finally, in section six presents the contribution of the paper and future work.

2. Privacy risks, awareness and policy visualization

In order to examine scholar disquisition associated to our research objective, we reviewed the literature on privacy policies as well as the available literature and resources on mobile apps' features and vulnerabilities. Our literature review analysis consists of three parts: potential risks/threats that mobile app users encounter, user privacy awareness, privacy policies' reading cost, and new visualization approaches. We narrow our efforts on Androids OS's and exclude IOS from our research because only Android's security and privacy settings can be changed by the user without any special expertise (Benenson & Reinfelder, 2013). In IOS users have limited capabilities of changing the security and privacy settings of an app. Apple (the Company providing IOS) claims that any app that is available through the official App store is reviewed by Apple's review process system for security and privacy issues. This feature does not allow users to change apps' settings.

2.1 Users' privacy concerns

Bandyopadhyay (2009) investigated the antecedents and consequences of consumer's online privacy concerns. He identified the main factors that influence consumers' privacy concerns such as vulnerability to information

misuse, perceived ability to control the disclosure and use of private information, and characteristics of the consumer's cultural background. He also found that consumer's privacy concerns lead to limited willingness to disclose personal data online, to abandonment of e-commerce services or even to the total unwillingness to use the internet. Several studies had come to the same conclusions, that privacy concerns are determined by factors as awareness of information collection, perceived vulnerability to information misuse, experience with Internet use and cultural background of consumers (Sheehan and Hoy, 2000; Dinev and Hart, 2004; Bellman et al., 2004).

Buchenscheit et al. (2014) investigated if the use of the WhatsApp app could reveal users' behavior patterns and activities. Through an experiment they collected information on intended and actual behaviors (e.g., typical activities, typical sleeping hours), which they correlated with automatically obtained information from the usage of WhatsApp app. The participants, who didn't have significant privacy concerns for using the app, were surprised by the results highlighting that users do not fully realize the privacy implications of their online behaviors. Paspatis et al. (2017) used a pseudorandom dataset of 2000 telephone numbers and try to de-anonymize Viber users'. They found 682 users who had Viber installed and de-anonymized the 75% of them, revealing their full name, address and in about half of the cases their profile picture and occupation. After the de-anonymization process, authors conducted an empirical questionnaire and habits monitoring with 20 participants of the de-anonymization set. Most participants didn't have significant privacy concerns as they did not know that their data can be exposed and considered as public data or that someone can monitor their habits.

2.2 Users' privacy awareness and the cost of reading privacy policies

McDonald and Cranor (2008) tried to calculate the time and cost of users reading the privacy policies of each online service they visit. Through their empirical study they found out that every website user visit at least 1354 unique websites and that the average cost for the time they spend is 4.48 dollars per hour (if a Privacy Policy is read at home) or 35.86 dollars per hour (if the Privacy Policy should be read in office). They calculated that every website user would need 40 minutes per day for reading Privacy Policies when the average time of web surfing is 72 minutes per day. The total financial cost for all website users would be almost 781 billion dollars per year.

Kritzinger and von Solms (2010) state that the most important factor for home users being vulnerable to security threats is their lack of awareness about risks of using the Internet. Karavaras et al. (2016) conducted an empirical survey with 190 participants to explore Facebook users' awareness regarding malicious link threats, revealing that their low awareness can make them vulnerable to such attacks. Church and Oliveira (2013) researched what users are concerned at most when they are using mobile apps such as WhatsApp. They found that most users were more concerned about the "last seen feature" whereby someone can see at what exact time a user was read a message. Using this feature a user is capable to understand someone's habits such as sleep routine. Almuhimedi et al. (2014) demonstrated that users' low awareness regarding location data -among others by mobile apps and suggest a permission manager to protect their privacy. Graeef and Harmon (2002) found that privacy concerns vary by age, income and gender. In addition, they saw that younger users are more aware of their information leak while older users are concerned more about their financial privacy. To raise web users' awareness, Malandrino et al. (2013) produces NoTrace, a mozilla firefox add-on that monitor users' browsing activity and inform them what personal and sensitive information they leak towards third-party such as advertising companies. NoTrace is also capable to block or alter the browser fingerprint information. Hazari and Brown (2013) conducted a questionnaire-based survey with 157 business students enrolling regarding privacy behavior, trust policies and technology and correlate their results with others researchers' previous studies. His results showed that individuals are concerned about their privacy and would like to control their digital reputation as it can directly impact their business relationships and/or employment prospects. He also suggested the importance of awareness training providing by institutions to make students aware of privacy issues.

2.3 Privacy policy visualization approaches

Barker et al. (2009) described purpose, visibility, granularity, retention and constraints as the key elements that form a privacy policy and categorized their research around a conceptual framework for data privacy. Ghazinour et al. (2009) presented a framework for visualizing privacy policies called Privacy Policy Visualization Model (PPVM). They suggested a graphical tool that combines Entity Relationship Modeling, Entity Relationship diagramming and the elements described by Barker et al. (2009) to show the association between the data provider, the collector and the data they collected. Albalawi and Ghazinour (2009) have evaluated PPVM using Jensen's (2014) Structured Analysis of Privacy (STARP) heuristics evaluation framework to inspect privacy usability and vulnerabilities and suggested

solutions to improve usability issues encountered during evaluation. Domingo-Ferrer (2009) suggested a three-dimensional conceptual framework for privacy policies. His proposal identifies privacy issues in a privacy policy that relate to the data provider, house and third-parties with every issue is grouped to one these categories. Anwar et al (2009) described an access control model of assessing privacy policies through visualization. Da Silva et al (2016) suggested a multi-language framework tool based on Lingo programming language called RSLingo4Privacy which intends to improve the specification and analysis of a privacy policy. Their tool automatically classifies extracted text statements and text snippets from a policy into five classes: Collection -which data are collected; Disclosure - which data is disclosed and to whom; Retention -how long data will be available; Usage -why are they collecting users' data; and Informative -which is a general purposes class and after the conversion provides an improved version of the policy in a natural language. Kelley et al (2009) conducted a survey testing the readability, accuracy and comprehension of five different format privacy policies: full text policy in natural language, standardized table format, short standardized table, short natural language and layered notices. They concluded that the best results in all categories were provided by the two table-type policies. Micallef et al. (2017) conducted an empirical study to investigate users' preferences on multiple types of privacy policies such as combinations of visual nudges, vibration, audio and speech on mobile apps. They revealed that users are annoyed when low priority notification nudges use audio or speech to alert them and developers should prefer non – salient privacy nudges to inform them. Keith et al (2018) examined an approach to improve privacy policies through the design and usage of mediated content, such as video instead of textual privacy policies. They aimed to explore if design factors such as gender, animation style, music tone or color scheme affect users' perceived risk, perceived benefits and disclosure decisions. Their results indicate that the most effective video privacy policies are those that use female narrators with vibrant color palettes and light musical tones.

Research shows that users have low privacy awareness and privacy concerns which are raised when understanding the actual privacy threats. Studies also show that users facedifficulties on reading privacy policies, such as the difficult legal language they are written in. All the above, do not create the appropriate conditions for conscious consent for the disclosure of personal information. Additionally, the users are confronted with a fragmented approach, since they need to read and understand the different privacy policies of the million mobile apps that are available. Therefore, there is a challenge on creating a single approach that can assist users and resolve the problem of the million privacy policies the users need to read. AppAware target to address this issue by using as a foundation for user awareness the

permission set of the mobile apps (which is what they do and not what they state they do) and not the privacy policy. This gives the opportunity to automatically transform a privacy policy to a visualized privacy report, with representative pictures and easy to read for the common user.

3. Web browser add-ons privacy approaches

Due to the evolution of the internet, privacy experts and researchers proposed web browsers add-ons tools to enhance users' privacy and awareness. Bruckner and Voss (2005) proposed MozPETS – a Privacy enhanced web browser add-on for Mozilla Firefox. MozPETS inspects the content of a website to find potential threats to the user's privacy and displays an emoticon next to the URL address bar. If users click on the emoticon then MozPETS displays the results of the test in detail. Li et al. (2009) proposed SpyShield – an add on to preserve users' personal data stealing from malicious add-ons. Akiyama et al. (2013) proposed the solution of using web browser add-ons for authentication and authorization purposes. They concluded that using browser add-ons for single sign on, users can mitigate the dangers in terms of identity and password stealing or phishing even if they have limited knowledge of privacy, security and awareness. Heidrerich et al. (2009) proposed a Document Object Model (DOM) sanitizer called DOMPurify as a web browser filtering client. The objective of DOMPurify was to prevent cross side scripting attacks.

On the other hand, researchers are questioning the use of browser extensions (Tsalis et al. 2015). Due to extensions mechanism, developers can create malicious browser add-ons and instead of privacy protection, lead to privacy incidents such as personal data stealing, data trafficking or even webpage data manipulation. Carlini et al. (2012) performed a security review of 100 Google Chrome's extensions and located 70 vulnerabilities in 40 of them while Barth et. Al. (2017) in their research, analyzed the 25 most downloaded extensions for Firefox and found that the 88% are trying to gain more permissions than necessary.

4. Methodology

In this section, we analyze our methodology for developing AppAware and for validating its effect on users' privacy awareness.

4.1 Technical Methodology

We developed AppAware with Java JDK. We chose to use java instead of other programming languages because of its compatibility with different operating systems such as Windows, Linux, IOS and because it is easily modified to be used for android mobile devices (Android OS and its applications are written in a version of Java). To store our data, AppAware's global database is based on MySQL while there is a standalone version of AppAware that is using SQLite DB. We chose MySQL because its freeware, supports more than 10 million records per table while it supports and performs fast enough with many users simultaneously. The local version of AppAware is using SQLite db to store data. We chose SQLite to release users of the requirement of a local database installation such as MySQL or SQL Server. AppAware is following a different approach than the new models we referred in the related work section. Instead of trying to transform a given mobile app privacy policy into more comprehensive forms, AppAware creates a visualized report with images and privacy descriptions in natural language of the permissions that are obtained from an App during installation or use. In particular, we have matched every permission from the Android's permission set with a representative image, a permission description and a possible threat. We obtained permissions' descriptions from Pew Research (Olmstead and Atkinson, 2015) and we chose the associated images and possible threats based on google's image matching. We believe that the descriptive images of the visualized report will catch the eye of users and increase their privacy awareness. In this way, users may read the description of the permission they are giving access as well as the possible threat(s) they may encounter. Our module is consisted of four java classes: a) Dataset, b) AppData, c) AppHandling and d) AppPerms which cooperate as follows:

Dataset Class. This class includes all Android's Permissions. It is consisted of 3 fields: android's permission name, permission privacy description and potential threat. As we mentioned before permission privacy descriptions obtained from Pew Research (Olmstead and Atkinson, 2015) previous work. We chose these descriptions because of the natural language they used which is easy understandable for the common user.

AppData. This is AppAware's main class. From this class users can see which android applications are stored in the database as well as which permissions can be obtained during installation. Also, they can export the visualized report (figure 2, 3). For the purposes of our experiment

we include to AppAware the twenty most famous applications for the 2017 (Hartmans, 2017).

AppHandling. From this class a user can add a new app that does not included to AppAware's database and send it for evaluation and permission matching. In order to add a new app, user must update AppAware's database to it latest version. Thus, users can also see stored apps with minimum details. After the app's evaluation and permission matching, AppAware's user is ready to create the new visualized report.

Figure 1 below shows AppAware's Schema:

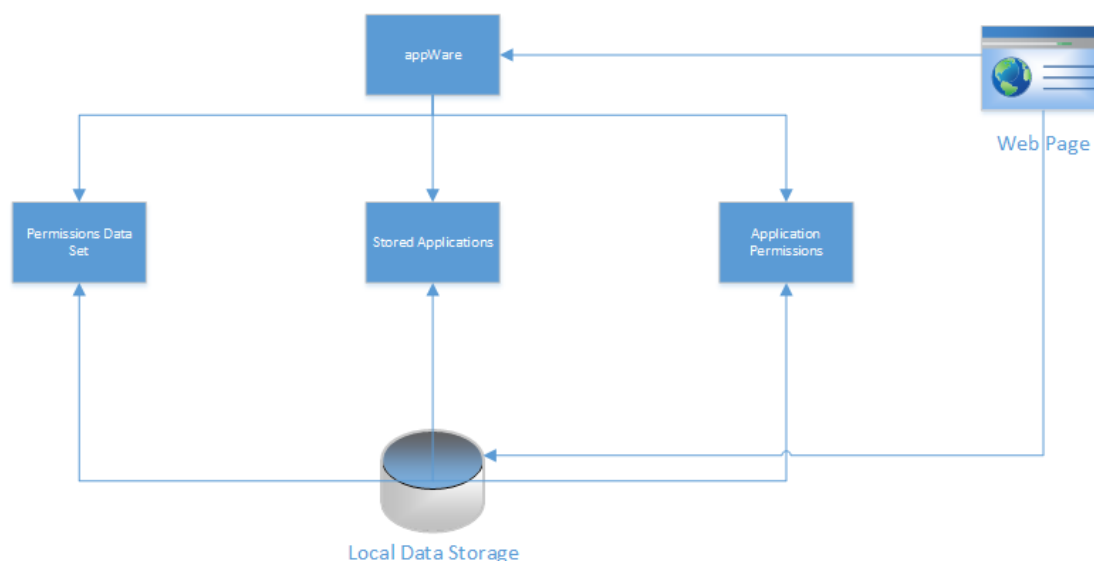


Figure 32. AppAware Schema

AppPerms. This is the class where more advanced users and administration team can match a new application with the permissions it gains upon install/use. After the matching, app's permissions are uploading to AppAware's web database in order to update AppAware's users. To avoid spam or false permissions matching, AppAware's Server will wait for a non-specified number of users to send permissions matching for the same app. After this step server will correlate the results and if there is a specific number of permissions matching will send an updated data set to AppAware's clients.

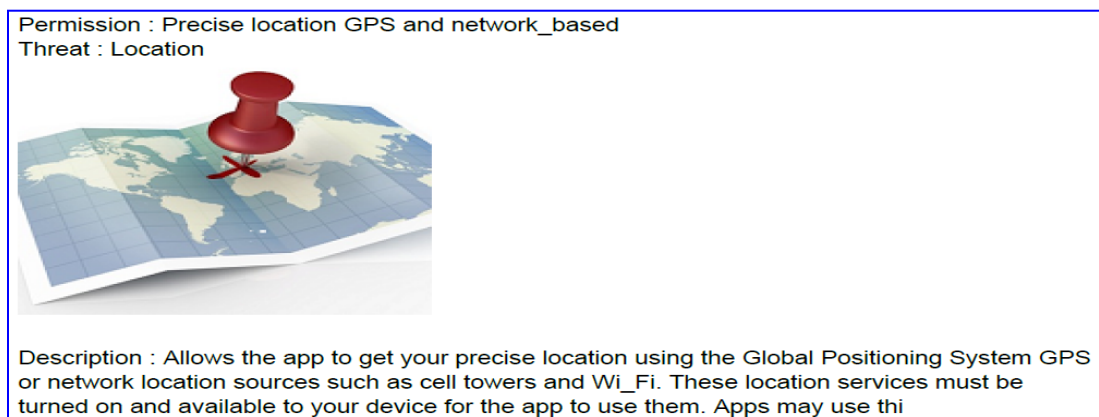


Figure 33. Representative picture and description and threat from the visualized report

Permission : Directly call phone numbers
Threat : Overcharge



Description : Allows the app to call any phone number including emergency numbers without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services

Figure 34. Representative picture and description and threat from the visualized report

All AppAware classes are been showed to the Figures 4, 5, 6, 7 below.

id	application	description	id	permission	description	Allows access to	Threat
0	null	null	2	Full network acc...	Allows the app t...	Hardware	none
1	Facebook	facebook desc	3	View network co...	Allows the app t...	Hardware	Location
3	Linkedin	Linkedin data	4	Test access to p...	Allows the app t...	Hardware	none
5	Instagram	Instagram App	5	Modify or delete t...	Allows the app t...	User Info	Data Loss
6	Adobe Reader	Adobe Reader	6	Read phone stat...	Allows the app t...	User Info	Location
7	Amazon Kindle	Amazon Kindle	7	Prevent device fr...	Allows the app t...	Hardware	Power Abuse
8	Dropbox		8	Precise location ...	Allows the app t...	User Info	Location
9	ebay		9	View Wi-Fi conn...	Allows the app t...	User Info	Triangulation
10	Evernote		10	Control vibration	Allows the app t...	Hardware	None
11	WatchESPN		11	Approximate loc...	Allows the app t...	User Info	Location
12	Gmail		12	Receive data fro...	Allows apps to a...	Hardware	Overcharge
13	Chrome		13	Find accounts o...	Allows the app t...	User Info	Link Data
14	Google Maps		14	Take pictures an...	Allows the app t...	User Info	Privacy
15	Pandora		15	Run at startup	Allows the app t...	Hardware	Abuse
16	Shazam		16	Directly call phon...	Allows the app t...	User Info	Overcharge
17	Skype		17	Read your conta...	Allows the app t...	User Info	Privacy
18	Spotify		18	Record audio	Allows the app t...	User Info	Privacy
19	Twitter		19	Retrieve running ...	Allows the app t...	User Info	Link Data
20	WhatsApp		20	Read Google se...	Allows this app t...	Hardware	Statistics
21	YouTube		21	Read call log	Allows the app t...	User Info	Privacy
22	Viber		22	Google Play lice...	Can check if you ...	Hardware	None
23	Hotmail	Hotmail Client	23	Send SMS mess...	Allows the app t...	User Info	Overcharge
24			24	Access extra loc...	Allows the app t...	User Info	Location
25			25	Set wallpaper	Allows the app t...	Hardware	None
26			26	Modify your conta...	Allows the app t...	User Info	Corrupt File Syst...

Figure 35. Class AppPerms

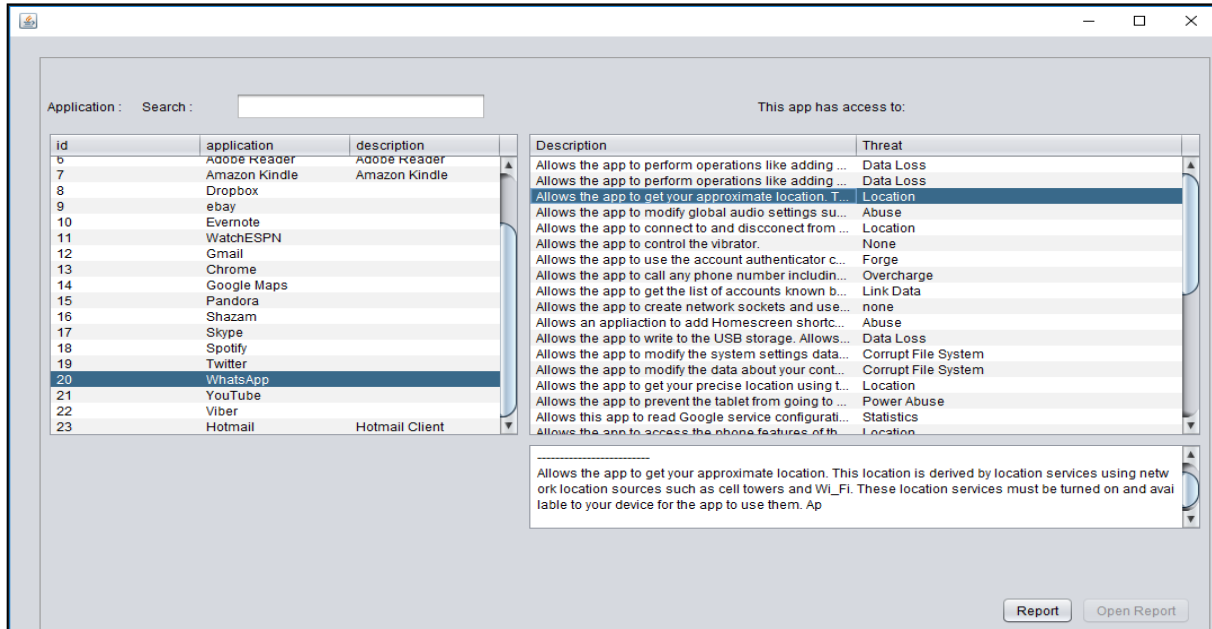


Figure 36. Class AppData

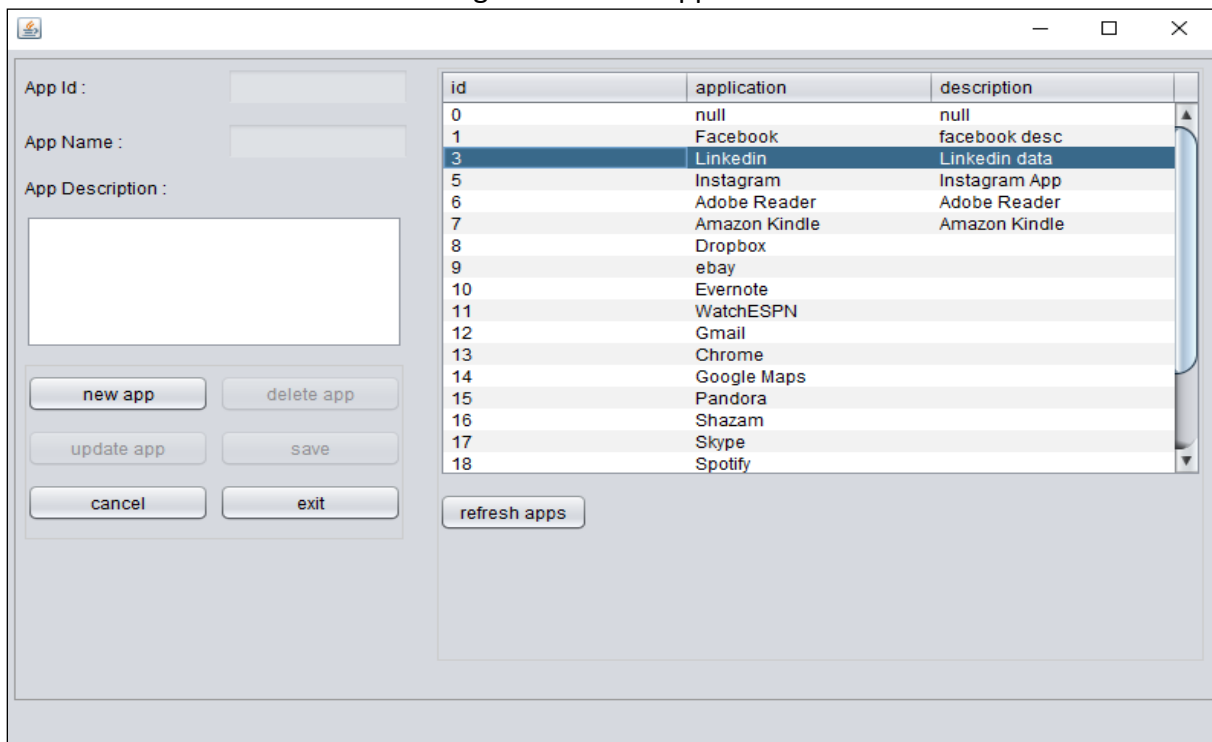


Figure 37. Class AppHandling

Load Data Set

id	permission	description	Allows access to	Threat
2	Full network access	Allows the app to cr...	Hardware	none
3	View network conne...	Allows the app to vi...	Hardware	Location
4	Test access to prote...	Allows the app to te...	Hardware	none
5	Modify or delete the ...	Allows the app to wr...	User Info	Data Loss
6	Read phone status ...	Allows the app to ac...	User Info	Location
7	Prevent device from ...	Allows the app to pr...	Hardware	Power Abuse
8	Precise location GP...	Allows the app to ge...	User Info	Location
9	View Wi-Fi connecti...	Allows the app to vi...	User Info	Triangulation
10	Control vibration	Allows the app to co...	Hardware	None
11	Approximate locatio...	Allows the app to ge...	User Info	Location
12	Receive data from i...	Allows apps to acce...	Hardware	Overcharge
13	Find accounts on th...	Allows the app to ge...	User Info	Link Data
14	Take pictures and vi...	Allows the app to ta...	User Info	Privacy
15	Run at startup	Allows the app to ha...	Hardware	Abuse
16	Directly call phone n...	Allows the app to ca...	User Info	Overcharge
17	Read your contacts	Allows the app to re...	User Info	Privacy
18	Record audio	Allows the app to re...	User Info	Privacy
19	Retrieve running ap...	Allows the app to ret...	User Info	Link Data
20	Read Google servic...	Allows this app to re...	Hardware	Statistics
21	Read call log	Allows the app to re...	User Info	Privacy
22	Google Play license...	Can check if you ha...	Hardware	None
23	Send SMS messages	Allows the app to se...	User Info	Overcharge

Allows the app to view information about Wi-Fi networking such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.

icon :

Figure 38. Class Dataset

AppAware is support database update function for future implementation. In case of a ready Apps-permission dataset be

available in public, it will be capable to support as many apps there are in the dataset. Thus, AppAware users can create and export their dataset that created with AppData class and send it to AppAware's team for evaluation and import to the web database. Until now, Playstore does not giving public and massive access to their apps database and their permission set. In case of Playstore give in public an app-permission set in public, AppAware will automatically update its global database.

Evaluation methodology

In order to evaluate AppAware, we conducted a survey using a questionnaire. The purpose of the survey was to investigate how mobile app users evaluate AppAware's Visualized Report in terms of installability, usability, and viability-purpose compared to the traditional privacy policy of WhatsApp. The criteria and questions - except demographics- derived from ISO/IEC 9126-1 Software engineering — Product quality. All questions were Likert type and mandatory. To design and distribute the questionnaire (Appendix) we used Google Forms due to its popularity and characteristics, such as provision of real-time statistical results, the security and anonymity protection that it offers.

A requirement for participation to our survey was to install AppAware and use it for a trial period before answering the questionnaire. For this purpose, we did not target the general population, but instead we distributed the designed questionnaire to colleagues and undergraduate students of various disciplines. In order to test the effect of computer science knowledge on the AppAware evaluation we included a question about the profession or studies of the participants to maintain control over this characteristic of the sample. To complete the questionnaire, participants should first read WhatsApp's privacy policy and then install AppAware and export the WhatsApp's Visualized Report using it. The survey was running for 40 consecutive days and we received 73 answers. We consider that this number of responses is sufficient, especially given the obstacles caused by the requirement to install an unknown application or the refusal to participate because of installation problems. The 73 participants were equally distributed in terms of gender (36 Males, 35 Females, 2 unknown), were mainly aged between 18 – 34 years and most of them had at least bachelor degree. The demographics of the questionnaire are analyzed in detail in Table 1.

<i>Demographics (n=73)</i>		
Gender	Male	36 (49.3%)
	Female	35 (47.9)

Age	Other/Unknown	2 (2.7%)
	18-	1 (1.4%)
	18-34	54 (74%)
	35-44	10 (13.7%)
	44+	8 (11%)
Level of education	High School	4 (5.5%)
	Associate Degree	4 (5.5%)
	Bachelor Degree	32 (43.8%)
	Master's Degree	28 (38.4%)
	PhD Graduate Degree	5 (6.8%)
Profession	Economics	14 (19.2%)
	Political Science	7 (9.6%)
	Social Science	9 (12.4%)
	Computer Science	31 (42.5%)
	Educational Science	4 (5.5%)
	Other	8 (11%)

Table 23: Sample Demographics

4.2 AppAware users' evaluation

The questionnaire intended to collect users' opinion regarding aspects of AppAware installability, usability, and viability/purpose. AppAware scored in all categories above average with mean values varying from 3.07 to 4.01 (scale 1 – 5). Our results in the category Viability and Purpose reveal that participants would prefer to use AppAware's Visualized Report than read the traditional privacy policy. In terms of installability, participants didn't confront any difficulties to install or understand how to use AppAware since the mean values in this aspect range from 3.48 to 4.04. Regarding usability and purpose, AppAware scored lower mean values ranging from 3.07 to 3.75.

The results are analyzed in Table 2, that includes three columns with column one demonstrating total mean values with all professions calculated, in column 2 we exclude participants with computer related degree and finally in column three we demonstrate the mean values only of participants with computer related degree.

Question	Total mean values	Mean values of participants

I believe It was easy to install AppAware to my system	3,81	4,02
I believe that I understand what the software does and its purpose	4,01	4,29
I believe that It was easy to learn how to use AppAware's basic functions	3,93	4,21
I believe that It was easy to learn how to use AppAware's advanced characteristics/functions/features	3,48	3,69
I believe that AppAware's Visualized report helped me to understand better the WhatsApp's privacy policy.	3,64	4,05
I believe AppAware's Visualized Report helped me to find the potential threats I may be confronted with using WhatsApp	3,68	4,05
I believe AppAware's Visualized Report was easy to read	3,47	3,83
I believe that AppAware's Visualized Report was easy to understand	3,38	3,74
I believe that the descriptions of AppAware's permission set are accurate.	3,75	4,10
I believe that the actual threat of AppAware's permission set is accurate.	3,74	4,10
I believe that AppAware is a stable Application	3,64	4,10
I believe that AppAware is a useful Application	3,53	3,88
I believe that AppAware is appropriate for its purpose	3,63	4,00
It was faster to read AppAware's Visualized Report than WhatsApp's privacy policy.	3,71	4,07
I prefer to use AppAware than to read the privacy policy of an App.	3,53	3,81
I believe that AppAware is a unique software tool	3,30	3,48
I believe that AppAware will be helpful to me	3,07	3,19

Table 2. Questionnaire results

5. AppAware Parser Concept model

To further enhance AppAware's capabilities we propose a complementary application called AppAware Parser. The philosophy behind AppAware Parser can be imprinted in four points:

AppAware Parser checks which applications of the given mobile device are installed and creates a report that enlists those applications. With the mobile device user's approval the list can be uploaded to AppAware's global database.

For every application that there is a record in AppAware's database, AppAware Parser creates a mobile friendly visualized privacy report and informs the mobile device user for every installed application what permissions this application gains and the potential dangers that the user can be confronted with; and

Informs the mobile device user about the applications that there is no information about in the AppAware's global database.

Figure 8 below shows AppAware Parser's Schema:

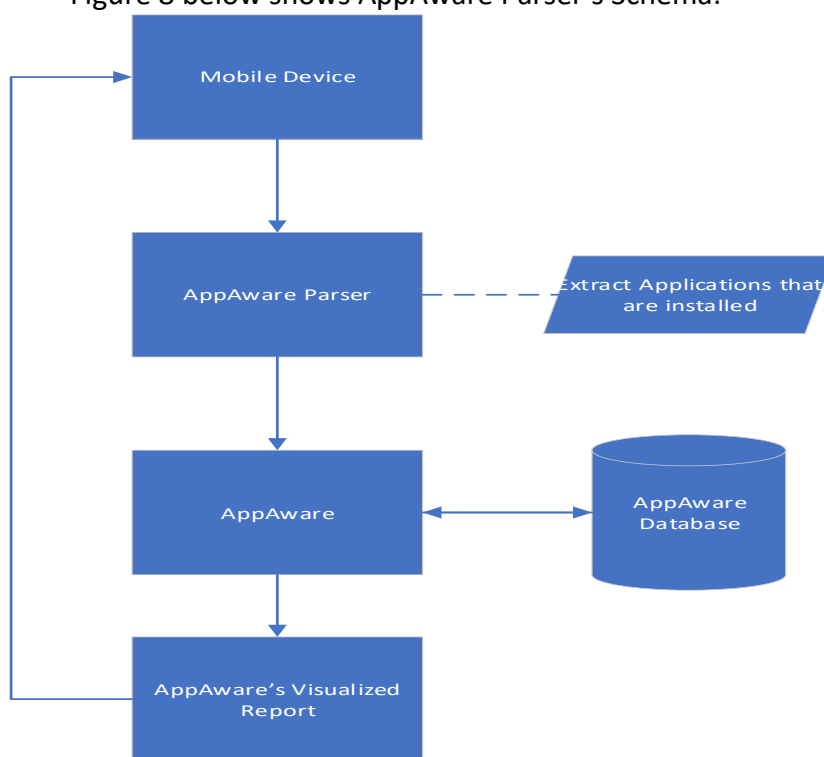


Figure 39. AppAware Parser Schema

After the first check of the installed applications in a given mobile device, AppAware Parser will continue to run in the background to monitor the manifest.xml of each application. In case of any changes, the AppAware Parser will inform the user and will propose to create a

new visualized privacy report. Also, in case of any new installation of an application AppAware parser will propose to create the visualized privacy report for that application. Currently, AppAware Parser is only a concept in progress model and we plan to implement in the future and evaluate its effectiveness in user privacy awareness.

Conclusions and future work

In this paper, we suggested a visualized model for representing privacy policies for mobile apps and the permissions they obtain upon installation. We processed android's permission set and we matched all permissions with a potential threat and a representative picture. We included in AppAware the 20 most popular applications for 2017 and then we evaluated AppAware using a survey with 73 participants. We focused our evaluation on installability, usability, and viability/purpose of AppAware. AppAware was evaluated above average in all categories especially in the usability category. Thus, we presented AppAware Parser, a browser add-on as a concept model. AppAware Parser is complementary application to AppAware and acts mostly pro-actively, trying to enhance users' awareness.

To the best of our knowledge, there is no other approach like AppAware. There are several approaches to visualize the text of a privacy policy, but there is no approach that enhances user understanding by creating a permission visualization model. The advantage of our approach is that a user does not need necessary to read all privacy policies of all mobile apps to visualize them but only to import the mobile apps and their permission set to AppAware's database. At the time of this paper we have included the 20 most popular mobile apps for the 2017. Unfortunately, we can't automatically import all available applications because Google Play store does not allow the use of crawlers or parsers.

AppAware provides significant implications for mobile app developers as well as marketplaces. Our findings show that app users would prefer to use a visualized report instead of the privacy policy of an app. App developers could provide the permission dataset they use in their apps. Researchers could use instantly and with ease their dataset to update public databases such as AppAware's. In this way, applications that target to mitigate users' privacy concerns and raise users' awareness could be up to date and help users to understand privacy threats and protect their data equally. For the same reason, we recommend app marketplaces to provide publicly the permission dataset for the apps they are hosting to assist transparency and give control to the users over their data. At the moment, AppAware is only a client-server application created in java due to its multiplatform capabilities. In the future, we envision to develop AppAware into a

web-accessible database. Also, we focus to present AppAware Parser as a full working model.

Appendix

A. Demographics

1. What is your gender?

Male\Female

2. What is your age?

18-\18-34\35-44\30-39\40-49\50-59\60+

3. What is the highest level of school you have completed or the highest degree you have received?

Less than high school degree\High school degree or equivalent (e.g., GED)
\Some college but no degree\Associate degree\Bachelor degree\Master's degree\P.H.D. Graduate degree

4. What is your profession?

Economics/Political Science/Social Science/Computer Science/Educational Science/Other

B. AppAware Evaluation (Likert Scale 1-5)

Installability

1. I believe It was easy to install AppAware to my system

Learnability

1. I believe that I understand what the software does and its purpose

2. I believe that it was easy to learn how to use AppAware's basic functions

3. I believe that it was easy to learn how to use AppAware's advanced characteristics/functions/features

4. I believe that AppAware's Visualized report helped me to understand better the WhatsApp's privacy policy.

Usability

1. I believe AppAware's Visualized Report helped me to find the potential threats I may be confronted with using WhatsApp.
2. I believe AppAware's Visualized Report was easy to read.
3. I believe that AppAware's Visualized Report was easy to understand.
4. I believe that the descriptions of AppAware's permission set are accurate.
5. I believe that the actual threat of AppAware's permission set is accurate.

Viability-Purpose

1. I believe that AppAware is a stable Application.
2. I believe that AppAware is a useful Application.
3. I believe that AppAware is appropriate for its purpose.
4. It was faster to read AppAware's Visualized Report than WhatsApp's privacy policy.
5. I prefer to use AppAware than to read the privacy policy of an App.
6. I believe that AppAware is a unique software tool.
7. I believe that AppAware will be helpful to me.

References

- Amran, A., Zaaba, Z., Singh, M. and Marashdih, A. (2017). Usable Security: Revealing End-Users Comprehensions on Security Warnings. *Procedia Computer Science*, 124, pp.624-631.
- Anwar, M., Fong, P., Yang, X. and Hamilton, H. (2010). Visualizing Privacy Implications of Access Control Policies in Social Network Systems. *Data Privacy Management and Autonomous Spontaneous Security*, pp.106-120.
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 706-714.
- Bandyopadhyay, S. (2011). Antecedents and Consequences of Consumers Online Privacy Concerns. *Journal of Business & Economics Research (JBBER)*.

Barth A., Felt A. P., Saxena P., Boodman A. (2009) Protecting browsers from extension vulnerabilities. In: 17th Network and Distributed System Security Symposium (NDSS '10), USA

Barker K, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams. "A data privacy taxonomy." (in press) BNCOD '09: The 26th British National Conference on Databases. 12 pages, Birmingham, UK, 2009.

Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, 313-324

Benenson Z, Reinfelder L. (2013). Should the users be informed? On differences in risk perception between Android and iPhone users. In Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK.

Bruckner Lars & Voss Marco (2005). MozPETs - A Privacy enhanced Web Browser. Darmstadt University of Technology. Security and Privacy Assurance in Advancing Technologies: New Developments Available at : <http://mozpets.sourceforge.net/>

Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M. and Kargl, F. (2014). Privacy implications of presence sharing in mobile messaging applications. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia - MUM '14.

Budnitz, M. (1998). Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate. *South Carolina Law Review*, 49 (1), 847-886.

Carlini N., Felt A., Wagner D. (2012) An evaluation of the google chrome extension security architecture. In: 21st USENIX Conference on Security, USA

Church, K., & de Oliveira, R. (2013) What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS. 15th international conference on Human-computer interaction with mobile devices and services, Munich, August 30th, 2013, (pp. 352-361). ACM, Munich.

Da Silva, A., Caramujo, J., Monfared, S., Calado, P. and Breaux, T. (2016). Improving the Specification and Analysis of Privacy Policies - The RSLingo4Privacy Approach. Proceedings of the 18th International Conference on Enterprise Information Systems.

Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model. *Behavior and Information Technology*, 23 (6), 413-422.

Domiongo-Ferrer (2009). “A three-dimensional conceptual framework for database privacy”. In *Secure Data Management 2007*, volume 4721/2007, pages 193–202, Vienna, Austria, 2007.

Ghazinour, K. and Albalawi, T. (2016). A Usability Study on the Privacy Policy Visualization Model. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).

Graeff, T. and Harmon, S. (2002). Collecting and using personal data: consumers’ awareness and concerns. *Journal of Consumer Marketing*, 19(4), pp.302-318.

Hartmans A. (2017). The 20 most popular iPhone apps of 2017. *Business Insider*. Available at: <http://www.businessinsider.com/top-apple-iphone-apps-2017-12>

Hazari, S. and Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, 9(4), pp.31-51.

Heiderich, M., Späth, C., & Schwenk, J. (2017). DOMPurify: Client-Side Protection Against XSS and Markup Injection. *ESORICS*.

Jensen, C. (2004), “Toward a method for privacy vulnerability Analysis”, CHI 2004, extended abstracts on Human factors in computing systems, Publisher: ACM

Kambiz Ghazinour, Maryam Majedi, Ken Barker, A Model for Privacy Policy Visualization in 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2009.

Karavaras E, Magkos E, Tsohou A (2016) Low User Awareness Against social malware: An Empirical Study and Design of a Security Awareness Application.

Kelley, P., Cesca, L., Bresee, J. and Cranor, L. (2010). Standardizing privacy notices. *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*.

- Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 840-847.
- Li L., Wang X., Choi J. (2007) SpyShield: Preserving privacy from spy add-ons. In Conference on Recent Advances in Intrusion Detection.
- Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R. and Krishnamurthy, B. (2013). Privacy awareness about information leakage. Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society - WPES '13.
- McDonald A., Cranor L.F., (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* 2008. Privacy Year in Review issue. [online] Available at: <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>. [Accessed 25 Jun 2017].
- Micallef, N., Just, M., Baillie, L. and Alharby, M. (2017). Stop annoying me! Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17.
- Olmstead, K. and Atkinson, M. (2015). APPS PERMISSIONS IN THE GOOGLE PLAY. [online] Pew Research Center. Available at: <http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/> [Accessed 20 Jan. 2017].
- Paspatis Ioannis, Tsohou Aggeliki and Kokolakis Spyros, "Mobile Application Privacy Risks : Viber Users' De-Anonymization Using Public Data" (2017). MCIS 2017 Proceedings. 32. Available at : <http://aisel.aisnet.org/mcis2017/32>
- Raab, C.D. & Bennet, C.J. (1998). The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, 14 (4), 253-262.
- Rindfleish, T.C. (1997). Privacy, Information Technology, and Healthcare. *Communications of the ACM*, 40, 92-100.
- Saunders, K. & Zucker, B. (1999). Contracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers, and Technology*, 13 (2), 183-192.
- Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy and Marketing*, 19 (1), 62-73.
- Statista (2017a). Global cumulative shipments of smartphones using the Android operating system from 2007 to 2016.

<https://www.statista.com/statistics/241943/forecast-of-global-cumulative-shipments-of-smartphones-using-android-os/>

Statista (2017b). Number of apps available in leading app stores as of March 2017. <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

Statista_ (2017c). Number of available apps in the Apple App Store from July 2008 to January 2017.
<https://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>

Statista (2018). Number of available applications in the Google Play Store from December 2009 to December 2017.
<https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>

Toyokazu A, Takeshi N, Kazutsuna Y, Motori N, Yasuo O. Design and Implementation of a Functional Extension Framework for Authn & Authz Federation Infrastructure using Web Browser Add-on. 2013 IEEE 27th International Conference on Advanced Information Networking and Applications.

Tsalis, N., Mylonas, A. and Gritzalis, D. (2016). An Intensive Analysis of Security and Privacy Browser Add-Ons. Lecture Notes in Computer Science, pp.258-273.

Tsohou, Aggeliki & Kosta, Eleni. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. Computer Law & Security Review. 10.1016/j.clsr.2017.03.027.

Wilson, S., Schaub, F., Dara, A., Liu, F., Cherivirala, S., Giovanni Leon, P., Schaarup Andersen, M., Zimmeck, S., Sathyendra, K., Russell, N., B. Norton, T., Hovy, E., Reidenberg, J. and Sadeh, N. (2016). The Creation and Analysis of a Website Privacy Policy Corpus. Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers).