

國立清華大學  
National Tsing Hua University

**隱私控制的雙重性質：**

文獻綜述、概念框架、和兩項實證研究

**The Dual Nature of Privacy Control:**

A Review, Framework, and Two Empirical Studies

科技管理學院

服務科學所 博士學位論文

College of Technology Management

Institute of Service Science Doctoral Dissertation

學號：105078891

姓名：張諾海 (Arturo Heyner Cano Bejar)

指導教授：雷松亞 博士 (Dr. Soumya Ray)

中華民國 111 年 05 月 18 日

## 摘要

一些研究表示，那些對個人資訊進行加強控制的人不太關心他們的隱私，而其他研究也發現，加強隱私控制只會加劇人們的隱私問題。因此，本論文主要關注兩個問題：對隱私控制不同看法的本質及其解釋，以及隱私控制在多大程度上能減輕人們的擔憂並影響其意圖與行為。進一步針對核心問題做進一步的探討，即對控制這件事，在心理層面人們對控制的表現，並通過研究它是如何演變進而影響其他方面。於此，我們認為存在著兩種不同且平行的隱私控制，主要的和次要的，它們辨識及解釋，人們接受和適應隱私問題是另一種健康的反應，能為自己提供了另一種自我控制感。我們在社交網絡平台的背景下使用結構方程(研究1-橫斷面研究)，和邏輯回歸在行動設備版本的 Facebook 中(研究2-准實驗)來深入理這兩種不同且平行的隱私控制。

在這兩項研究中，結果都表明，兩種類型的隱私控制分別對應於增加和減少的信息隱私問題並且它們來自文化所衍生出的個人價值觀。此外，二級隱私控制策略似乎是當前隱私控制概念化的主要部分。

**關鍵詞:** 二級隱私控制，信息隱私問題，一級隱私控制，准實驗，保護行為

## Abstract

While some research show that those experiencing enhanced control over their personal information are less concerned about their privacy, other studies are discovering contexts in which enhanced privacy control only worsens people's privacy concern. Thus, this dissertation focuses on two major issues: The nature and antecedent explanations for varying perceptions of privacy control, and the degree in which privacy control goes beyond mitigating concern and affects intentions and behaviors. We specifically argue for the existence of two distinct and parallel types of privacy control—primary and secondary—that recognize the fertile assertion that accepting and adjusting to privacy issues is another healthy response that provides oneself with a feel for control. We use structural equation modelling in the context of social networking platforms (Study 1 – a cross-sectional study) and logistic regression in the context of Facebook in mobile devices to deeply understand privacy control.

In both studies, the results show that the two types of privacy control correspond separately to increased and decreased information privacy concern and that they arise from culturally derived personal values. Moreover, secondary privacy control strategies seem to be a dominant portion of the current conceptualization of privacy control.

**Keywords:** Secondary privacy control, information privacy concern, primary privacy control, quasi-experiment, protective behaviors.

## Acknowledgements

I have begun writing this doctoral thesis without realizing that it would embody the unabated effort of 6 years of my life, the relentless guidance of my advisor, Dr. Soumya Ray, and the thoughtful advice of my doctoral committee.

First and foremost, I would like to express my deepest gratitude to my thesis advisor who out of his passion for research has had wisely used his patience and courage to deal with the challenges I posed to him during this complicated but rewarding enterprise.

I should also like to extend my grateful thanks to my committee members; Prof. Jennifer Claggett from Wake Forest University, Prof. Tien Wang from National Cheng Kung University, Prof. Pei-Yu Pai from National Cheng Chi University, and Prof. Shih-Chieh Hsu from National Sun Yat-Sen University, for their involvement and enormous help to increase the quality of this doctoral thesis.

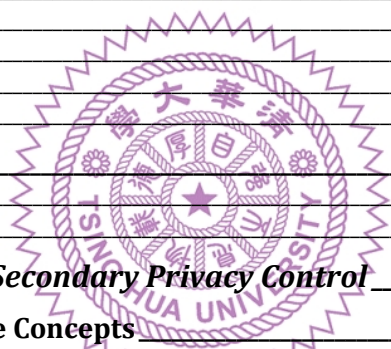
I could not have made it without the support of my Taiwanese family who gave me a home in Taiwan and so facilitated the accomplishment of my graduation as a doctor. Naturally, I will never be grateful enough to my Peruvian family for providing me the emotional sustain I many times needed.

Finally, I would also like to thank the critical comments of the DIGIT, MISQ, and WITS information systems communities because this manuscript also grew on their advice.

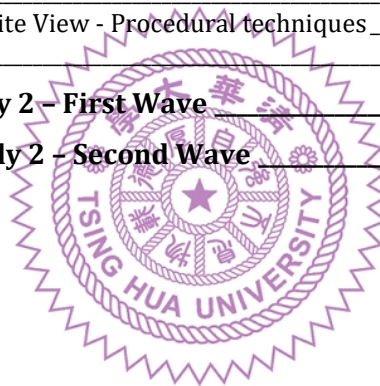
## Table of Contents

|   |             |
|---|-------------|
| <i>摘要</i>   | <i>i</i>    |
| <b>Abstract</b>   | <b>i</b>    |
| <b>Acknowledgements</b>   | <b>iii</b>  |
| <b>Table of Contents</b>  | <b>iv</b>   |
| <b>List of Tables</b>   | <b>vii</b>  |
| <b>List of Figures</b>  | <b>viii</b> |
| <b>Chapter 1: Introduction</b>                                  | <b>1</b>    |
| <b>Chapter 2: A Dual Perspective of Privacy Control</b>         | <b>6</b>    |
| <b>An Overview of Information Privacy Control</b>               | <b>6</b>    |
| Information Privacy   | 6           |
| General Privacy Control   | 7           |
| A Dual Perspective of Control                                   | 9           |
| Origins of Control  | 10          |
| Distinguishing Between Primary and Secondary Control            | 10          |
| A Dual Perspective  | 10          |
| Operationalizing Secondary Control                              | 13          |
| The Interrelation Between Secondary Control and Primary Control | 14          |
| Adopting a Dual Perspective of Privacy Control                  | 15          |
| The Interrelation Between Secondary and Primary Privacy Control | 17          |
| Cultural Factors and the Dual Privacy Controls                  | 18          |
| Collectivism  | 20          |
| Uncertainty Avoidance   | 21          |
| National Culture or Culturally-informed Personal Values         | 22          |
| <b>Chapter 3: Study 1</b>                                       | <b>24</b>   |
| <b>Social Networking Services and Protective Intentions</b>     | <b>24</b>   |
| <b>Secondary and Primary Privacy-Control Framework</b>          | <b>25</b>   |
| Privacy Control   | 27          |
| Agency and Control  | 27          |
| Culturally-Informed Personal Values and Control                 | 29          |
| Information Privacy Concern                                     | 33          |
| Privacy Control and Privacy Concern                             | 34          |
| General Privacy Risk Awareness and Privacy Concern              | 37          |
| Privacy Protective Intentions                                   | 37          |
| Important Correlates or Control Constructs and Variables        | 40          |
| <b>Empirical Validation of Study 1</b>                          | <b>41</b>   |
| Context: The Facebook SNS                                       | 41          |
| Survey Design and Deployment                                    | 42          |
| Measurement Items   | 42          |
| Data Collection   | 46          |
| Covariance Based Structural Equation Modeling (CB-SEM)          | 48          |
| Measurement Model   | 49          |
| Internal Consistency and Construct Validity                     | 50          |
| Structural Results  | 51          |
| Suppression Effect  | 54          |

|  |           |
|--|-----------|
| Cross Associations and Overriding Associations _____                       | 55        |
| Common-Factor vs. Composite Perspectives _____                             | 56        |
| <b>Discussion _____</b>  | <b>58</b> |
| Theoretical Contributions _____  | 59        |
| Managerial Contributions _____   | 61        |
| <b>Chapter 4: Study 2 _____</b>  | <b>63</b> |
| <b>Context: Smartphone Social Networking Services Apps _____</b>           | <b>63</b> |
| The App Tracking Transparency Feature - ATT _____                          | 64        |
| Exogenous Variation from a Privacy-Related Event _____                     | 66        |
| <b>Theory Development _____</b>  | <b>67</b> |
| Theoretical Framework _____  | 67        |
| Dual Privacy Controls and Upgrading Behavior _____                         | 68        |
| <b>Empirical Validation of Study 2 _____</b>                               | <b>69</b> |
| Study Design and Deployment _____  | 69        |
| Data Collection _____  | 70        |
| Definition of Variables _____  | 71        |
| Criterion and Auto-Regressor _____   | 71        |
| Predictors _____   | 72        |
| Correlates _____   | 73        |
| Data Analysis _____  | 73        |
| Logistic Regression Model _____  | 74        |
| Results _____  | 74        |
| <b>Discussion _____</b>  | <b>76</b> |
| Theoretical Contribution _____   | 76        |
| Managerial Contribution _____  | 77        |
| <b>Chapter 5: Alternative Views of Secondary Privacy Control _____</b>     | <b>78</b> |
| <b>Literature Review of Alternative Concepts _____</b>                     | <b>78</b> |
| Secondary Privacy Control and Privacy Escape-Avoidance Coping _____        | 78        |
| Secondary Privacy Control and Privacy Accommodation _____                  | 81        |
| Secondary Privacy Control and Privacy Primary Appraisal _____              | 82        |
| <b>Post Hoc Empirical Comparisons with Secondary Privacy Control _____</b> | <b>83</b> |
| Secondary Privacy Control vs. General Privacy Control _____                | 84        |
| Secondary Privacy Control vs. Privacy Wishful Thinking _____               | 85        |
| Secondary Privacy Control vs. Primary Privacy Control _____                | 85        |
| Cross-Lagged Panel Model Analysis _____                                    | 85        |
| Long-Term Nature of Secondary and Primary Privacy Controls _____           | 86        |
| Secondary Privacy Control as a Form of Privacy Concern _____               | 88        |
| <b>Discussion _____</b>  | <b>89</b> |
| Theoretical Contributions _____  | 90        |
| Managerial Contributions _____   | 91        |
| <b>Chapter 6: Repositioning Privacy Control _____</b>                      | <b>92</b> |
| <b>Overall Contributions _____</b>   | <b>92</b> |
| Overall Theoretical Contributions _____                                    | 92        |
| Overall Managerial Contributions _____                                     | 94        |
| <b>Limitations and Future Directions _____</b>                             | <b>96</b> |
| <b>Conclusions _____</b>   | <b>97</b> |



|  |            |
|--|------------|
| <b>References</b>  | <b>99</b>  |
| <b>Appendices</b>  | <b>122</b> |
| <b>Appendix A: Survey Items – Study 1</b>  | <b>122</b> |
| <b>Appendix B: Exploratory Factor Analysis of Dual Privacy Control</b>                       | <b>124</b> |
| <b>Appendix C: Non-Response Bias</b>   | <b>127</b> |
| <b>Appendix D: Sample vs. Population Demographics Compared</b>                               | <b>128</b> |
| <b>Appendix E: Confirmatory Factor Analysis – CFA and Principal Component Analysis – PCA</b> | <b>129</b> |
| <b>Appendix F: Common Method Variance</b>  | <b>131</b> |
| Marker Variable Technique  | 131        |
| Common Method Factor Technique   | 133        |
| <b>Appendix G: Variance Inflation Factor Values</b>  | <b>136</b> |
| <b>Appendix H: Suppression Effects</b>   | <b>137</b> |
| <b>Appendix I: Composite Model Analysis</b>  | <b>139</b> |
| Assessing the Measurement Model  | 139        |
| Measurement Quality  | 139        |
| Common Method Bias in a Composite View - Procedural techniques                               | 143        |
| Structural Results   | 144        |
| <b>Appendix J: Survey Items – Study 2 – First Wave</b>                                       | <b>146</b> |
| <b>Appendix K: Survey Items – Study 2 – Second Wave</b>                                      | <b>147</b> |



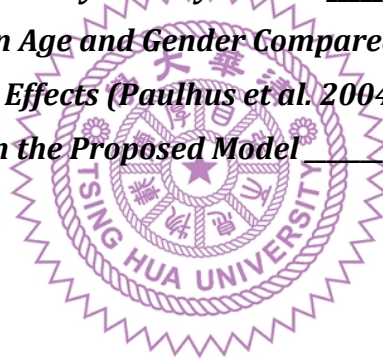
## List of Tables

|  |     |
|--|-----|
| <i>Table 1: Secondary Control in the Fields of Psychology, Health, and Education</i>           | 12  |
| <i>Table 2: Studies on Culture and Secondary Control</i>                                       | 19  |
| <i>Table 3: Conceptualization of Constructs in the Proposed Model</i>                          | 26  |
| <i>Table 4: Demographic Information of Respondents</i>   | 47  |
| <i>Table 5: Sample of Qualitative Responses of Privacy Strategies on Facebook</i>              | 47  |
| <i>Table 6: Measurement Quality and Correlations</i>   | 51  |
| <i>Table 7: Proposed, Saturated, and General Privacy Control Structural Models</i>             | 53  |
| <i>Table 8: Structural Results of the Composite Proposed Model</i>                             | 57  |
| <i>Table 9: Data Descriptives</i>  | 74  |
| <i>Table 10: Logistic Regression Dual Privacy Controls and General Privacy Control Models</i>  | 75  |
| <i>Table 11: Secondary Privacy Control vs. Privacy Escape-Avoidance Models</i>                 | 81  |
| <i>Table 12: Secondary Control as a Form of Concern</i>  | 89  |
| <i>Table A1: Survey Items</i>  | 122 |
| <i>Table A1: Survey Items (Continuation)</i>   | 123 |
| <i>Table B1: Exploratory Factor Analysis of Secondary Privacy Control</i>                      | 124 |
| <i>Table B2: Exploratory Factor Analysis of Primary Privacy Control</i>                        | 125 |
| <i>Table C1: First 50 and Last 50 Response Comparison</i>                                      | 127 |
| <i>Table E1: Confirmatory Factor Analysis</i>  | 129 |
| <i>Table E2: Principal Component Analysis of Distancing and Exiting Intentions</i>             | 130 |
| <i>Table F1: Original Correlation Table</i>  | 132 |
| <i>Table F2: CMV-Adjusted Correlation Table</i>  | 132 |
| <i>Table F3: Original and CMV-Adjusted Proposed Models</i>                                     | 133 |
| <i>Table F4: Common Method Factor Technique</i>  | 134 |
| <i>Table F4: Common Method Factor Technique (Continuation)</i>                                 | 135 |
| <i>Table G1: Variance Inflation Factors</i>  | 136 |
| <i>Table I2: Item Variance Inflation Factor Results</i>  | 142 |
| <i>Table I3: Composites Variance Inflation Factor Results</i>                                  | 144 |
| <i>Table I4: Structural Results of Proposed and Alternative Models – Composite Perspective</i> | 145 |



## List of Figures

|   |     |
|---|-----|
| <i>Figure 1: Conceptualization of Proposed Model</i>                                  | 26  |
| <i>Figure 2: Software Update Message on iPhone</i>                                    | 67  |
| <i>Figure 3: Conceptual Framework</i>   | 68  |
| <i>Figure 4: Lagged Quasi-Natural Experimental Design</i>                             | 71  |
| <i>Figure 5: Secondary Privacy Control vs. Privacy Escape-Avoidance Coping</i>        | 79  |
| <i>Figure 6: Secondary Privacy Control vs. Privacy Accommodation</i>                  | 82  |
| <i>Figure 7: Correlation of Privacy Control Constructs</i>                            | 84  |
| <i>Figure 8: Correlation of Dual Privacy Controls and Privacy Wishful Thinking</i>    | 85  |
| <i>Figure 9: Distribution of Respondents Based on their Dual Control Orientations</i> | 87  |
| <i>Figure 10: CLPM Analysis of Secondary and Primary Privacy Controls</i>             | 87  |
| <i>Figure B1: Parallel Analysis of Secondary Privacy Control</i>                      | 124 |
| <i>Figure B2: Parallel Analysis of Primary Privacy Control</i>                        | 126 |
| <i>Figure D1: Sample vs. Population Age and Gender Compared</i>                       | 128 |
| <i>Figure H1: Types of Suppression Effects (Paulhus et al. 2004)</i>                  | 137 |
| <i>Figure H2: Suppression Effects in the Proposed Model</i>                           | 138 |



## Chapter 1: Introduction

Being in touch with others is one of the most desirable and enjoyable activities for people (Harter and Arora 2008). Not surprisingly, we spend progressively more time of every day in our favorite social networking platform, with an average of two and a half hours in 2022 (Statista 2022a). Naturally, managers provide more and better functionality that facilitate the various activities people engage in when socializing. Furthermore, with the inclusion of mobile app services, social media has an enormous capacity for communication, computation, storage, and retrieval of information (Crossler and Bélanger 2019). These converging technologies have further amplified the way we share particulars with others to the extent that it is increasingly difficult for users to be entirely cognizant of what information they are sharing, who has access to it, and its ramifications. But as users of technology, we are increasingly aware that the more people who have access to these data, the wider the door opens to unethical purposes and unforeseeable outcomes (Leetaru 2018), creating unavoidable latent threats to our privacy (Mason 1986).

As the privacy climate in industry and society changes, the concept of privacy is becoming an inexorably urgent issue within the information systems academic community (Al-Natour et al. 2020, Bélanger and Crossler 2011, Bellman et al. 2004, Dinev et al. 2015, Gopal et al. 2018, Lowry et al. 2011, Malhotra et al. 2004, Osatuyi 2015, Pavlou 2011, Smith et al. 1996, Xu et al. 2012, Zhang et al. 2022). The privacy literature has grown in the number and scope of privacy-related constructs studied, but some part of it has converged on the important role of privacy control in mitigating privacy concern (Dinev and Hart 2004, Malhotra et al. 2004, Xu et al. 2012), suggesting that information privacy is a story of control and concern. Even in the early years of Internet use, researchers had already noted that over three-quarters of the public felt they had lost all control over how companies were using and sharing their personal information (Culnan 1993). But while researchers have long focused on the nature of privacy concern (Malhotra et al. 2004, Zhang et al. 2022), fewer studies were directed to learn about privacy

control. In this dissertation, I seek to strengthen our understanding of privacy control to provide a fuller picture of information privacy.

Privacy control captures what users think they can do and what they expect to happen about the erosion of their privacy. The major research stream finds that those who have control over their privacy can mitigate the risks of privacy loss and, in turn, their concern about privacy (Xu et al. 2012). However, some recent studies suggest that privacy control sometimes worsen one's perceptions of information privacy concern in some contexts (Miltgen and Peyrat-Guillard 2014, Wang et al. 2016). Additionally, while the information systems literature has considered agentic antecedents to privacy control (Xu et al. 2012), the psychology literature suggests that perceptions of control can also generally arise from one's cultural make-up. And while the information systems literature has largely examined the effect of privacy control on privacy concern, other disciplines have argued and found that general control directly affects intentions and behaviors (Weisz et al. 1984). Thus, this work takes on two major questions: *what is the nature and antecedent explanations for varying perceptions of privacy control, and to what degree does it go beyond mitigating concern and affect intentions and behaviors?*

Based on a comprehensive review of studies on perceived control from the literature of mental and physical health, education, and psychology, we propose that privacy control is not a single notion – it has a dual nature that we cannot neglect. While we primarily conceive of privacy control as users relying on themselves and taking action to change their privacy conditions, we find that users can also have a secondary method to enhance their feeling of privacy control by relying on the market or government to help them stay protected. Additionally, based on the influence of cultural values on control perceptions (Weisz et al. 1984), it is further proposed that personal cultural values affect the dual perceptions of privacy control. And most important, we will show that these two senses of privacy control have distinguishably different, and often unintuitive, outcomes that could stretch beyond simply mitigating concern.

The growing complexity of managing one's information in social networking platforms serves as an exemplary context in which to learn about the dual nature of privacy control, their agentic and cultural antecedents and the resulting self-protective intentions and behaviors of technology users. Social networking services are turning into a battleground in the fight to maintain privacy, with companies, governments, and ordinary users taking opposing sides. Some of the most dominant social-networking platforms, like Facebook, strongly encourage users to represent themselves using their authentic day-to-day identity (Newcomb 2018), and so sharing information has strong privacy implications as it can be directly linked to their off-line activities. Moreover, social-network users enjoy enormous flexibility for self-expression, from posting, mentioning and tagging others, checking-in at locations, streaming candid videos, and more. Such activities make social networking services more prone to privacy violations, and so the information privacy practices of social network services are increasingly questioned by citizens, consumers, business leaders, scholars, and government regulators (Hitlin et al. 2019). We are especially interested in the case of Facebook, where consumer behavior is being converted into a commercial asset (The Economist 2019) – a charge to which Facebook has responded in recent years by opening up many settings and features that purport to give users greater control over their privacy (Newcomb 2018).

This manuscript contains a specifically developed framework that puts in perspective the workings of secondary privacy control and primary privacy control in social networking platforms. Primary privacy control conceptually reflects the general view of privacy control in the information systems literature that individuals rely on themselves to carefully craft their online social connections and interactions and take advantage of privacy settings. For example, they might selectively choose friends to include in their network, untag themselves from sensitive photos, or change settings that limit who can see their profile. Secondary privacy control reflects how individuals rely on powerful others, such as government, market forces, or just plain good fortune, to stay protected from privacy issues. For example, they might choose to believe that a company cannot afford to harm them or that government

and market regulations will protect their privacy outcomes in the future. Using both mechanisms, technology users try to convince themselves that their privacy is assured. In our later post hoc analyses, we also compare these dual privacy controls against seemingly similar concepts in the coping and accommodation literatures.

We conducted two studies to understand the nature, antecedents, and outcomes of these dual privacy controls discussed above. In Study 1, we construct a model of the dual privacy controls that includes constructs of agency, personal cultural values and protective intentions. We fit this model against cross-sectional survey data of Facebook users. The proposed framework integrates personal and proxy agency from our prior understanding of privacy control into SNS self-efficacy and SNS regulations of the government and market. New to the study of privacy control in this framework are the cultural concepts of uncertainty avoidance and collectivism as differential antecedents of the dual privacy controls. Additionally, Study 1 includes exit and distancing intentions as distinctive outcomes of the dual privacy controls.

Our Study 2 is a complementary quasi-natural experiment that examines the actions of iPhone users who have Facebook. In particular, we seek to predict and understand their response to an actual external event: the offering by Apple of an operating system upgrade that enforces prohibition of data collection across apps in the App Store (and particularly targeted at the Facebook app). In this quasi-experiment, we will examine how secondary privacy control might have effects on actual user behavior – which in this case is timely updating of their operating system to take advantage of the new privacy-protection features of their device.

A convergent finding of both studies is that technology users gain a sense of control over their privacy using the two proposed modes of privacy control. We discover why some users are motivated to take steps to protect their privacy while others simply follow their own routines as if privacy issues were not of concern to them. More specifically, Study 1 shows that under a secondary privacy control

orientation, users focus on exploiting the benefits of social networking services and so choose to rely on powerful others for privacy protection, thereby reducing their information privacy concern. Additionally, this secondary privacy control orientation arises in those seeking support in regulations and from one's collectivistic value. Intriguingly, the general notion of privacy control is thought to be equivalent to what we call primary privacy control, but both studies show that it empirically correlates to secondary privacy control. Meanwhile, Study 2 shows that a sense of secondary privacy control significantly decreases the likelihood of users upgrading their mobile phone operating system, even when it contains important changes that protect their privacy. We also find that users with a primary privacy control orientation are more likely to upgrade their mobile phone operating system.

These results also provide fertile information for managers and practitioners alike who have to deal with privacy issues in their day-to-day business execution. While a secondary privacy control orientation could benefit social networking services as users prefer not to exit (Study 1), this orientation also deters efforts to shield users from privacy issues as individuals avoid organizational initiatives (Study 2). For example, these users prefer not to upgrade their iPhone system, containing technical embedded protection, even when doing so provides them with tangible control over their data sharing. Through the antecedents, managers are provided with actionable gripping points for enterprises to recognize users and so improve user-retention and the adoption of developments intended to protect their privacy. Moreover, this research opens the debate about whether current privacy control settings provided by enterprises work the way they were intended to. It is our belief that privacy related policies and practices must understand and respect the great dilemma that modern information services pose to users.

## Chapter 2: A Dual Perspective of Privacy Control

### An Overview of Information Privacy Control

#### Information Privacy

Even when managing our online reputation can sometimes feel out of our control (van de Hoven et al. 2019), people are concerned with providing the right impression to others, or at the very least an intact one (Leary and Kowalski 1990). With various digital technologies available, balancing what and how much information we display to construct ourselves online, against information we consider private, has never been more challenging. Any information technology that provides access to information in individuals' private sphere will necessarily have to contend with privacy issues (van den Hoven et al. 2019). An exemplar of this tension in controlling our privacy is with today's social networking services. Facebook, in particular, is the focus of concerns with recurrent information privacy breaches (Holmer 2021, The Economist 2019). Moreover, its ample technical support for previously unimagined forms of interaction overexposes private information which not only have personally harmful consequences (Orben and Dunbar 2017) but also makes people vulnerable to the manipulation of their opinion (Confessore 2018).

Academics have been studying privacy for over a hundred years and across different domains of the social sciences (Cavazza et al. 2015, Smith et al. 2011, Whitman 2004). While there exist various definitions of privacy (Solove 2008), researchers agree that they can be encompassed as a "*personal boundary regulation process*" (Zhang et al. 2022). Additionally, early work in information systems, sought to explain the roots of privacy concern, recognize that privacy fundamentally represented how well people feel they can "*control transactions*" between themselves and others to enhance autonomy and minimize vulnerabilities (Dinev and Hart 2004). Thus, this dissertation embraces a recent definition of privacy by van den Hoven et al. (2019) that not only captures its fundamental element, *control*, but that also corresponds to the technological circumstances in which it is studied: "*Informational privacy*

*in a normative sense refers typically to a non-absolute moral right of persons to have direct or indirect control over access to (1) information about oneself, (2) situations in which others could acquire information about oneself, and (3) technology that can be used to generate, process or disseminate information about oneself.”*

This definition also suggests that privacy control, being it over one’s image, reputation, or use of one’s data (Bélanger and Crossler 2011), is as much dependent on the self as it is on others who can affect privacy outcomes, such as relevant authorities that promote privacy control mechanisms. Privacy control is now understood to be vital for individuals, and people without it often restrain themselves from voicing opinions on particular topics (Whitley 2009). There is also a broader and extrinsic need for service providers to assure online users of privacy – people who fear loss of information privacy avert from engaging in information-based activities, including those that could be beneficial to themselves, to service providers, or to society (De Hert 2008).

### **General Privacy Control**

In the information systems literature, the story of privacy began with initial efforts to model and empirically validate information privacy constructs as a form of concern that captured various information privacy perceptions in organizational (Smith et al. 1996) and Internet settings (Malhotra et al. 2004). While the notion of privacy concern keeps evolving over time (Hong and Thong 2013, Zhang et al. 2022), researchers have parallelly articulated privacy as a group of distinct but related concepts such as privacy control, privacy risk, self-protective privacy behaviors, and more (Al-Natour et al. 2020, Dinev et al. 2013, Dinev et al. 2015, Dinev and Hart 2004, Dinev and Hart 2005, Dinev and Hart 2006, Hong et al. 2019, Pavlou 2011, Smith et al. 2011, Son and Kim 2008, Xu et al. 2011, Xu et al. 2012). Of these, the general sense of privacy control, *general privacy control* in this manuscript, has come to be an important mediating construct that captures various individual-level traits and, in turn, offers a cohesive explanation for privacy concern (Bélanger and Crossler 2011, Dinev and Hart 2004, Xu et al. 2012).



Moreover, having privacy control play a central role in models of information privacy marks the convergence between conceptualizations of privacy as a form of control in other fields mentioned earlier (Cavazza et al. 2015, van den Hoven et al. 2019, Whitman 2004) and information systems privacy models.

We learn from these information systems studies of privacy control that it generally comes about from both one's own sense of agency as well as from an understanding of the agentic role of outside forces such as regulations (Xu et al. 2012). Beyond its antecedents, the critically important outcome explained by this general privacy control construct is information privacy concern (Dinev and Hart 2004, Xu et al. 2012). We are largely told that those who feel control over their information should perceive less potential for risks and so have less reason to be concerned about their privacy (Dinev and Hart 2004, Xu et al. 2012). Privacy concern, in turn, is often credited for ultimately influencing self-protective behaviors (Bélanger and Crossler 2011, Miltgen and Peyrat-Guillard 2014, Son and Kim 2008).

However, there are significant challenges in our preliminary understanding of privacy control that precludes us from modeling privacy control in more practical ways. First, apart from internal and external agency, little is known about what other personal dispositions or influences shape our perceptions of privacy control. The literature points us in the direction that privacy control could be enhanced as people reduce uncertainty about what impression their information gives to others (Dinev and Hart 2004), but no theory has been proposed about what those factors could be, let alone, empirical studies have examined those unknown factors. As a result, it is not easy to be sure whether artifacts and policies independently alter perceived control, or if other spurious effects might be at play. Similarly, the research on the full range of outcomes of privacy control is scant. Although prior studies have made the case for its relationship with privacy concern, there is need for formal arguments for or against privacy control directly impacting users' responses to privacy threats.

Even the fundamental relationship between privacy control and privacy concern is not consistent. One stream of literature argues, and finds, that our sense of privacy control reduces our privacy concern

because gaining control allows us to directly mitigate risks (Dinev and Hart 2004, Xu et al. 2012). But alternative views posit that privacy control might have different consequences in some information systems contexts. For example, Wang et al. (2016) found privacy control to be positively related to perceptions of privacy risks and concerns in their smartphone context, and surmised that mobile users might be more aware of privacy risks as they gain control. Similarly, Miltgen and Peyrad-Guillard (2014) highlight that North European citizens, compared to those in the South, show important differences in their interpretation of privacy concern, and attribute this difference to a sense of responsibility and faith— notions that seem to imply attempts to gain control over one’s privacy. All these views are compelling and demonstrate the potentially multifaceted and powerful role of control perceptions. But to generalize our understanding of the relationship between the two concepts, we need a finer understanding of privacy control that can distinguish why and how it can relate to privacy concern in different ways.

It seems to be that the time is ripe for a deeper investigation into privacy control. The idea exposed in this manuscript is born from the recognition that the concept of information privacy control entered our field as an adaptation of the more general notion of human control in psychology (Dinev and Hart 2004). As a consequence, to conceptualize and operationalize privacy control in the most generalizable ways, we must dig deeper into the psychology and psychometry of control itself. We must first ask where our sense of control generally comes from and how it is best to measure it.

### **A Dual Perspective of Control**

This systematic revision of the literatures of psychology, healthcare, education and others will discover that some of the nuances of control that have worked their way into privacy control have roots and primacy in western notions of success and healthy behavior, whereas there can be other ways of managing uncertainty in this world. It will also uncover that people across cultures can shift fluidly between, and even simultaneously use, both modes of control to balance successful outcomes against psychological harm.

## Origins of Control

The origin of the word ‘control’ owes to the innovative use of dual scrolls by the English Exchequer in the 1200s to keep duplicate entry records. Its etymology is based on the Latin *contrarotulare* describing the opposing but synchronized rotating mechanics of two scrolls in practical use for comparing accounting information (Smart 1994). By creating a master roll against which to check an examined roll, the Exchequer could exert ‘control’ over records and thereby bring unprecedented accuracy, integrity, and nonrepudiation to record-keeping. That the notion of control is based on an early information technology of sorts, makes it all the more relevant in today’s Information Age.

The concept of control has since evolved in usage to become an expression of human ability to alter our external environment to achieve our goals. White’s seminal work on behavioral motivation (1959) systematically balances earlier views of humans as merely reacting to needs, by identifying a necessary inner motive in interactions: “*The living system expands, assimilates more of the environment, transforms its surroundings so as to bring them under greater control.*” Feeling in control is so deeply rooted in humans that we even intentionally create opportunities for more challenging interactions with the environment only to attempt to gain control over these new circumstances (White 1959). While a minimal degree of frustration and fear can also stimulate our need for control (White 1959), dealing with uncontrollable situations is physically and psychologically harmful to people (Abramson et al. 1978). Thus, humans seek, by all possible means, to gain control and are reluctant to lose it.

## Distinguishing Between Primary and Secondary Control

### A Dual Perspective

When people see no other way but to relinquish control, they have even lost faith (Frankl 1984). Faith is so indistinguishable from life that losing it means there is no reason to live within the realm of reality (Fromm 1968). Aware of these extreme consequences, Rothbaum et al. (1982) propose a reinterpretation of passive behaviors, often thought as displays of relinquished control. They postulate that, in parallel to

the most common interpretation of control, there exists a secondary form of control that arises when one believes one cannot change the outcome of an undesirable situation.

This *feel of control* reflects people's clutch at faith so that perceptions of inevitability translate into attempts to gain back *the feeling of being in control* (Rothbaum et al. 1982). The secondary route to control allows individuals to reconcile their natural desire for control with the frustration of encountering an immutable environment. Secondary control-oriented individuals suspend themselves in this feeling and so can still enjoy the subjective, and at times the objective, benefits of gained control through other powerful forces (Morling and Evered 2006). An expression of secondary control of health outcomes might be: "*It is a fact that I feel ill, but with a bit of luck everything will turn out right*" (Grootenhuis and Last 2001). Here, luck is reified as a powerful agent that one can depend on to change outcomes, which reinvigorates one's *sense of control* no matter how illusory it might seem. In contrast, primary control reflects our perception of the self as a most powerful agent and translates into persistent efforts to succeed by changing our environment in accordance to our values and desires. A contrasting expression of primary control in the context of health outcomes would be: "*When I feel sick, I like to know of its causes in order to prevent it from occurring again*" (Seginer et al. 1993). Here, effort to gain knowledge is expected to enable the subject to take actions to manage health-related outcomes.

As humans' need to change the environment is pervasive, we attempt to stretch our reach of control to as many relevant domains as possible. However, people often attempt to do so by saving effort and time (Bechwati and Xia, 2003). Given our concern with various aspects of existence (Kelly 1955), we compensate our lack of resources by keeping a *feel of control* in those aspects that, at the moment, escape our persistent investment of energy and time (Rothbaum et al. 1982). Secondary control is this *feeling of control* humans obtain from momentarily relying on powerful others as a way to avoid the frustrations of relinquishing control in those domains of concern. Moreover, secondary control is found to be essential not only in life threatening situations but also in more mundane situations such as gambling

and dealing with the stress of schooling (Ejova et al. 2010, Hall et al. 2006a, 2006b). Thus, secondary control is a way to cognitively extend control over aspects that cannot receive our immediate attention and so protects us against the tarnishing consequences of relinquishing control.

Since the inception of the distinction of secondary and primary control, researchers in fields such as psychology, education, and health have compared and contrasted how people use these two modes of control in dealing with stressful situations and subjective well-being (Table 1). These findings largely concur that secondary control helps people avoid the frustration of investing intensive effort and time to deal with stressful situations they believe they have low or no ability to change on their own. Remarkably, secondary control strategies let people regain a feel that they are in control. The specific strategies of secondary control are revealed in the operationalization of this concept across these studies.

**Table 1:** Secondary Control in the Fields of Psychology, Health, and Education

| Authors                              | Domain   | Type of Study                         | Measures of Secondary Control  | Outcomes of Control  |
|--------------------------------------|--|---------------------------------------|--|--|
| <i>Band and Weisz (1988)</i>         | Life situations: receiving a bad grade, getting an injection | Qualitative Interview                 | Social/spiritual support<br>Emotion-focused avoidance<br>Pure cognition  | Adaptation   |
| <i>Haynes et al. (2009)</i>          | Life situations: gardening, vacuuming                        | Qualitative interview                 | Positive reappraisal,<br>Optimistic social comparisons,<br>Downgrading task importance,<br>Downgrading expectations,<br>Reengagement with a new task | Perceived stress<br>Physical well-being<br>Psychological well-being                            |
| <i>Seginer et al. (1993)</i>         | Life situations: transition to modern life                   | Cross-sectional surveys (two studies) | Predictive, interpretive, vicarious, and illusory strategies   | Adaptation to modern life  |
| <i>Chipperfield and Perry (1999)</i> | Household chores   | Cross-sectional survey                | Lowering expectations<br>Accepting personal limitation   | Physical health<br>Perceived health  |
| <i>Grootenhius et al. (1996)</i>     | Parents of children with cancer                              | Cross-sectional, interview/survey     | Predictive, interpretive, vicarious, and illusory strategies   | Parental efforts to cope   |
| <i>Hall et al. (2006a)</i>           | Academics: course completion, course experience              | Longitudinal survey                   | Interpretive strategies  | Perceived stress<br>Physical health<br>Illness symptoms and behaviors                          |
| <i>Hall et al. (2006b)</i>           | Academics: transition to university, course experience       | Longitudinal survey                   | Predictive, interpretive, vicarious, and illusory strategies   | Motivation (course withdraw)<br>Emotion (anger, regret, happiness, pride)<br>Performance (GPA) |
| <i>Thompson et al. (1998)</i>        | Aging: physical appearance                                   | Cross-sectional survey                | Acceptance<br>Predictive, interpretive, vicarious, and illusory strategies   | Perceived depression<br>Perceived anxiety  |
| <i>Langer et al. (2005)</i>          | Health: unplanned, minor procedures                          | Cross-sectional interview             | Elicited from respondents  | Perceived distress<br>Attributions of blame  |
| <i>Wrosch et al. (2002)</i>          | Health: caregiving to elders                                 | Longitudinal interview/survey         | Positive reappraisal<br>Lowering aspirations   | Subjective well-being  |
| <i>Weisz et al. (1994)</i>           | Health: children with leukemia, hair loss                    | Cross-sectional survey                | Self-selected  | Adjustment and adaptation  |

## Operationalizing Secondary Control

People use secondary control, a type of control in its own right, “*when they adjust some aspect of the self and accept circumstances as they are*” (Morling and Evered 2006). These investigators reveal, in a review of the secondary control literature, that the capacity of individuals to both accept and adjust to new conditions is consistent with most studies discussing secondary control strategies. Moreover, they argue that this view more closely reflects the original conceptualization of secondary control. However, a look into other forms of operationalization might shed light into these reasons.

Rothbaum et al. (1982) expanded on the nature of secondary control by proposing four broad types of secondary-control strategies: interpretive, predictive, illusory, and vicarious. We can get a sense of these strategies by examining measurement items from a study that used these four strategies to understand students coping with poor school performance (Hall et al. 2006b). Under interpretive secondary control, people try to understand and derive meaning from a taxing situation: “*Regardless of what my grades are, I try to see and appreciate how my experience can make me a stronger person overall.*” Under predictive secondary control, people attempt to predict outcomes so as to avoid disappointment: “*I’m reluctant to commit to a program major or minor because I want to keep my options open for as long as I can.*” Under illusory secondary control, one associates with chance or luck to deny bad outcomes: “*I often feel that my academic performance and experience has been kind of a ‘blessing in disguise’.*” Under vicarious secondary control, people associate with powerful others that might offer resolution: “*Knowing that other students have the same grades as I do gives me a comforting feeling of having something in common with others.*”

These various strategic means have had uptake in many applied studies of secondary control, but many of these quantitative studies have not been able to reliably confirm that these broad strategies are discriminable factors (Seginer et al. 1993, Grootenhuis et al. 1996). Moreover, studies on secondary control do not uniformly use all four strategies (see Table 1). For instance, a secondary control is

interpreted as lowering expectations of being personally responsible for effecting change as a protective psychological mechanism against experiencing future personal failure (Wrosch et al. 2002). Instead, they turn to other explanations or forces to supply for their own limited agency. People who have lost faith in their own ability to affect outcomes might regain a sense of control by accepting, coping with, or accommodating to challenging situations. There is, however, a common denominator for these secondary control strategies: to silence the need to change one's current situation and, instead, justify an undesirable condition so as to reclaim peace-of-mind from *assuming that things are under control*.

Another stream of research has interpreted secondary control as serving and supporting the functions of primary control (e.g., Heckhausen and Schulz 1995) and so measures of secondary control only include the acceptance of new circumstances and avoid the strategies used by those individuals with this orientation (Morling and Evered 2006). One drawback of interpreting secondary control as acceptance is that there is considerable overlap with the notion of coping (Morling and Evered 2006) (a discussion of similar constructs of secondary control is in the section "similar constructs").

Overall, these two alternative forms of operationalizing secondary control have resulted in either low empirical support or reflect an insisting focus on the most common idea of control as changing the environment and not the self, that overlaps with the notion of coping. Thus, Rothbaum et al.'s original conceptualization of secondary control seems to be best suited by operationalizing it as both acceptance and adjustment (Morling and Evered 2006). Secondary control is in its own right a provocative and powerful new perspective on control, and so researchers have also been interested in its relation to primary control.

#### The Interrelation Between Secondary Control and Primary Control

It is largely agreed that individuals use secondary and primary control strategies, sometimes simultaneously, to deal with specific situations (Chipperfield et al. 1999, Gould 1999, Hall et al. 2006b,

Morling et al. 2000, Weisz et al. 1994). For instance, Chipperfield et al. (1999) found that when exposed to complex situations, such as dealing with too many house chores, adults are likely to rely on both types of controls. Similarly, Hall et al. (2006b) found that students often rely on primary and secondary control when attempting to achieve good academic performance. However, at least one study found that secondary control potentially serves to compensate for low primary control (Bailis et al. 2005).

Overall, it would seem that the use of primary or secondary control strategies is a matter of personal preference rather than a matter of complementarity or substitution. Interestingly, most studies looking at the interrelationship between primary and secondary control do so under the lens of cultural differences. An intriguing finding is that the interpretation of secondary control as relegated to only serve the goals of primary control cannot explain the control in Asian or other cultures (Gould 1999). In what follows, secondary control and primary control are discussed in the realm of privacy as secondary privacy control and primary privacy control, respectively.

Adopting a Dual Perspective of Privacy Control

Privacy in its more basic form of individual seclusion or small-group intimacy is sought by all in the animal kingdom (Westin 1967). As such, information privacy is a fundamental domain in the life of individuals and so in societies at large. We all are concerned about the impression we give to others (Origgi 2018), but we differ in the way we gain control over our privacy as suggested by the two-process model of human control (Rothbaum et al. 1982). In this manuscript, it is theorized that control over one's privacy exists in two general forms: secondary privacy control and primary privacy control.

The conceptualization of secondary privacy control in the context of social networking platforms is based on the most relevant characteristics of secondary control. *Secondary privacy control* represents attempts to gain a feeling of control over one's privacy by accepting and adjusting to undesirable privacy conditions. First, secondary control-oriented individuals seek to accept and adjust part of their self to



circumstances outside their ability to affect, while transferring all sense of duty to powerful others (Rothbaum et al. 1982). Likewise, it is expected that social-network users with a secondary privacy control orientation will avoid directly dealing with threats to their own privacy. Instead, such users might be inclined to defer their responsibility and protection to authorities who, at that time, have more power to enact privacy changes than themselves. Also, secondary control-oriented individuals enhance their *feeling of control* to protect their psychological being from the destructive consequences of the loss of control (Rothbaum et al. 1982). Analogously, a secondary privacy control orientation implies that these individuals can save the day from privacy threats as they believe they cannot, at that time, confront these issues and protect themselves in these digital environments. And so, users with a secondary privacy control orientation might likely have to reframe their complacency about privacy, both for themselves and those around them, as a form of good. Yet, having aligned themselves on the side of the inevitable, the great payoff for users with a secondary privacy control orientation is that it obviates any need for a personal stance or action that would hamper how they exploit the benefits of social-networking systems or other relevant domains in life.

The conceptualization of primary privacy control is also based on relevant aspects of primary control, which emerges in people who want to obtain better outcomes than they expect, and feel capable of enacting strategies to ensure these are realized (Rothbaum et al. 1982). Similarly, social networking users under primary privacy control might directly confront privacy issues because they feel they can make a difference in not only their own privacy, but perhaps even broadly for others. But primary control is not an easy path to take (Bandura 2001, Heckhausen and Schulz 1995). And so, users with a primary privacy control orientation will have to continuously invest time and effort into learning how their social network systems work, so as to utilize its features and develop behavioral strategies to make certain that their information disseminates appropriately. *Primary privacy control* are attempts to gain control over

one's privacy by personally changing undesirable privacy conditions. In view of today's fast changing information technologies, it will require constant vigilance against new developments and threats.

#### The Interrelation Between Secondary and Primary Privacy Control

Prior findings regarding the coexistence of secondary and primary control and the way developmental psychologists and biologists view healthy psychological and biological development as the maintenance of equilibrium or homeostasis (Piaget 1970, Cannon 1929) suggest that a healthy scenario is such where secondary privacy control and primary privacy control can simultaneously be used to maintain an equilibrium in their concern over privacy. Protecting one's privacy is no easy task, as evidenced by the increasing amount of privacy settings provided to users of social networking services (Facebook 2020a). To deal with this complexity, users might spend time and effort to configure basic privacy settings while simultaneously assuring themselves that the social-network platform should be taking privacy seriously enough that users do not need to understand or exercise every setting and option. Thus, social-network users might rely more on one at certain times but are free to avail both.

This reasoning is also aligned with the lead of Rothbaum et al. (1982) who state (p. 8): "*Neither process [primary and secondary control] is thought to exist in pure form, often both processes are intertwined, as when persons negotiate and compromise [...] the difference between primary and secondary control should be thought of as a difference in emphasis*" However, there seems to be a differential preference for the primacy of use of primary or secondary control strategies among cultures that emphasize action (Heckhausen and Schulz 1995) versus those that emphasize interdependence (Gould 1999). Thus, individuals valuing action might primarily rely on primary privacy control strategies while those who value relational norms might mainly rely on secondary privacy control strategies.

The information systems literature suggests that people's sense of privacy control increases as they reach certainty in how others could see them if their data were available to them (Dinev and Hart

2004). Even within smaller geographical regions such as Europe, people are concerned with the management of their privacy to the same degree as the difference in their sense of responsibility and faith— notions that are closely related to the dual privacy controls and the reduction of uncertainty (Miltgen and Peyrad-Guillard 2014).

### **Cultural Factors and the Dual Privacy Controls**

There exist cultural differences in people's perceptions and motivations. From an ontological perspective, people growing in the East part of the world, in contrast to those living in the West, consistently interpret the occurrences in the world from a more holistic perspective (Ji et al. 2000). Ethnotheories or the common understanding of psychological concepts such as human action (e.g., control) reflect the accumulated cultural knowledge transferred to the individual by means of cultural absorption (Oerter et al. 1996). This difference due to cultural values has deep implications in how individuals think about control and in the outcomes they seek. While reasoning from an object-focused angle considers the individual to be the main causal agent and personal outcomes the most relevant, a holistic-focused orientation implies reasoning in terms of interrelations of objects and so conforming to reality is the most relevant outcome (Ji et al. 2000, Markus and Kitayama 1991). Moreover, studies have also found that the saliency of secondary or primary control is related to the cultural background of individuals (Gould 1999, Morling and Evered 2006) which in many cases does not corresponds with the national culture (Morling 2000).

Given that one's conception of control is tightly bound to the values inculcated in one's upbringing and environment, people attempt to gain control in ways compatible with their lifestyles, cultural traditions and value orientations (Seginer et al. 1993). Moreover, empirical findings from the literature on dual controls shows that people's preference for a specific type of control, either primary or secondary, depend on the person's culturally informed preferences regarding collectivist action (Morling and Evered 2006, Oerter et al. 1996, Sasaki and Kim 2010, Weisz et al. 1994) and the management of

uncertainty (Zhou et al. 2012, Weisz et al. 1994). While these papers largely use Hofstede’s cultural dimension of collectivism to distinguish between control preference orientations (Table 2), Weisz et al. (1984), in a qualitative study, also highlight the importance of rules (e.g., uncertainty avoidance) and social roles (e.g., collectivism) in allowing such predictability of social situations.

**Table 2: Studies on Culture and Secondary Control**

| Authors                             | Domain  | Subjects                                    | Type of Study                        | Implications of Cultural Values  |
|-------------------------------------|---|---|--------------------------------------|--|
| <i>Boiger et al. (2008)</i>         | Studying abroad                               | Foreigners in Japan                         | Cross-sectional survey               | Cultural fit associated with less psychological adjustment; primary control was associated with better sociocultural adaptation.   |
| <i>Morling (2000)</i>               | Fitness: choosing classes, making mistakes    | US<br>Japan                                 | Exploratory                          | US nationals report choosing fitness classes based on convenience and class difficulty, suggesting primary control; Japanese nationals report choosing based on ability and attribute mistakes to their ability misfit with the exercise level, suggesting secondary control; people used secondary control regardless of primary control.                       |
| <i>Weisz et al. (1984)</i>          | Life situations: Child rearing, socialization | US<br>Japan                                 | Observational                        | There are disadvantages of a one-sided pursuit of either form of control; an important goal, both for individuals and for cultures, is an optimally adaptive blend of primary and secondary control.   |
| <i>Oerter et al. (1996)</i>         | Philosophy: conceptualization of human nature | US, Japan<br>Indonesia<br>Korea             | Observational interview              | Both types of control present across cultures: primary control dominates among US nationals, and secondary control dominates in Eastern, collectivist cultures. Subjects from different cultures conceptualize control at different levels of complexity.  |
| <i>Sasaki and Kim (2010)</i>        | Religion: religious habits                    | US<br>Korea                                 | Observational journaling             | Coping strategies vary between individualist and collectivist cultures; collectivist (vs. individualist) people prefer social coping strategies over religious coping.   |
| <i>Zhou et al. (2012)</i>           | Reasoning: cognitive styles                   | China<br>Western                            | Various Experiments<br>Survey        | Prolonged experiences of control deprivation had the opposite effect of causing Chinese participants to shift back toward a strongly holistic style of thinking, while analytic approaches (primary control) are favored by individuals across cultures; there are cultural differences in the cognitive aspects of people.                                      |
| <i>Essau and Trommsdorff (1996)</i> | Academic challenges                           | US<br>Malaysia<br>Germany                   | Cross-sectional interview/survey     | In comparison to US and German nationals, Malaysian students used significantly more emotion-focused strategies; most subjects used both problem-focused and emotion-focused strategies.   |
| <i>Trommsdorff (1994)</i>           | Future orientation                            | Germany                                     | Conceptual                           | To resolve uncertainty, people want to know what the future will be like and to possibly control the future.   |
| <i>Seginer et al. (1993)</i>        | Transition to modernity                       | US, Canada<br>Germany<br>Malaysia<br>Israel | Cross-sectional survey (two studies) | Malaysian students made more use of secondary control strategies than US and German students in dealing with the uncertainty of transitioning to modern life. In a second study, students applied both types of control strategies to deal with the loss of predictability and uncertainty that characterize a transition process.                               |
| <i>Morling and Evered (2006)</i>    | Various                                       | n/a   | Metareview                           | Secondary control attracted researchers’ attention because it counterintuitively frames “maladaptive” behavior, such as passivity, in positive ways; secondary control challenges traditionally Western messages about what healthy people do; secondary control emphasizes flexibility in a culture that often prioritizes certainty, decisiveness, and action. |

Coming from an anthropological and psychological perspectives of the challenges every society faces, Hofstede’s seminal proposition of cultural values conceives uncertainty avoidance, among the five cultural values proposed, as the closest to relate to predictability in social interactions. In contrast, he proposes power distance as concerned with power inequality, and masculinity with the emotional roles

of individuals. Long-term orientation, conceptually one's focus on the present or future, seems to be less clearly separated from the other cultural values as it seems to overlap with all of them. Interestingly, Hofstede also suggests that collectivism, a cultural value related to the way individuals integrate into societies, has important implications on one's motivations to predict situations from a group's identity perspective. Thus, guarding against unknowns or favoring one's values of relatedness reduce uncertainty in navigating social situations.

Information systems researchers have recognized that cultural values are important to understand information privacy concern (Bellman et al. 2004, Milberg et al. 1995). Interestingly, some studies show that from all the five cultural values considered by Hofstede (1980), collectivism and uncertainty avoidance help people navigate the online marketplace and deal with uncertainty in transacting with others (Lim et al. 2004). Some find safety in aligning themselves with more powerful groups and simply following prescribed roles (Stets and Burke 2000), whereas others reduce uncertainty through their own efforts and so heavily rely on rules and instructions to make informed decisions. This divergence mirrors, to some extent, our distinction of the dual privacy controls. In the context of social networking services, users constantly present aspects of themselves to others and so face continuous uncertainty about how these others see them (Origgi 2018). Thus, the culturally-informed personal values of collectivism and uncertainty reduction suggested from the control literature in other areas and the information systems literature might be a natural fit to the study of information privacy control.

### Collectivism

Across studies and fields, researchers agree that secondary control is beneficial for humans and practiced across countries, but that this approach is more often seen in cultures of the east (Morling and Evered 2006). As could be seen in Table 2, the psychology literature on secondary control finds that cultural differences, especially along the collectivism-individualism dimension, exist in preferred orientations

towards control. Moreover, the findings of these studies challenge the understanding of what healthy people do (Weisz et al. 1984). The distinction between secondary and primary control was fundamentally motivated by a reinterpretation of ‘maladaptive behaviors’ such as passivity and withdrawal that wrongly classified healthy people, especially in Asian cultures, as unhealthy (Rothbaum et al. 1982, Weisz et al. 1984). As such, the notion of secondary control seems to entail being flexible with one’s personal goals in favor of one’s in-group desire (Morling and Evered 2006).

Uncertainty reduction is a common theme to collectivism and control. Collectivism is a cultural characteristic of those who rely on the role others have in society to reduce uncertainty in their interactions and so is closely related to the conception of secondary control (Weisz et al. 1984). For example, when encountering taxing situations collectivistic individuals avoid assuming responsibility, accept their fate or pray for help (Essau and Trommsdorff 1996). Analogously, in the context of privacy, collectivists must guide their interaction based on their perceptions of roles in their social network and so adopt prescribed behaviors that eventually help them reduce uncertainty regarding privacy.

#### Uncertainty Avoidance

Although that reducing uncertainty is a human need has been widely accepted (Trommsdorff 1994), recent research shows that perceiving uncertainty in one’s environment ‘alerts’ one’s sense of control, which in turn explains the different reactions people have to uncertainty (Mittal and Griskevicius 2014). The information systems literature also recognizes that control merely reduces the uncertainty in the environment (Hwang et al. 2005). In particular, people’s culturally informed values alter how people conduct themselves in personal matters and when interacting with others (Weisz et al. 1984). More specifically, uncertainty avoidance, a cultural value from Hofstede’s seminal work on culture (Hofstede 1980), is regarded as an important component in the reduction of uncertainty (Shuper et al. 2004). Thus, whereas collectivism is seen as more related to accepting and adjusting to unchangeable circumstances

(Essau and Trommsdorff 1996), uncertainty avoidance is seen as a cultural preference for direct action to change a situation (Hwang et al. 2005).

Uncertainty avoidance is a cultural characteristic of those who rely on structures of information such as rules and instructions to personally deal with uncertainty in their interactions and so exert continuous efforts to primarily control the outcome of their decisions (Weisz et al. 1984). For example, individuals facing serious health conditions try to get as much information to foster a sense of control (Babrow and Kline 2000). Under privacy pressures, individuals with uncertainty avoidance values might search or even build their own structures of information to use them as ways to achieve the protection of their privacy.

National Culture or Culturally-informed Personal Values

It is important to note that conventional stereotypes of countries of the east as being collectivist and passive, versus countries of the west as being individualistic and action-oriented, might be too simplistic. In some studies, for example, Asian participants under prolonged deprivation of direct control adopt an action-oriented nature similar to people of individualist cultures (Zhou et al. 2012). Also, certain ethnicities within individualist countries can exhibit a more collectivist mindset than others (Oerter et al. 1996). Generally, differences of cultural values between individuals might outweigh differences between regions (Yoo et al. 2011). Moreover, while Hofstede's theory of a national culture has great application at the macro-level, it would be challenging to think that all Japanese are collectivistic to the same degree. In contrast, it seems to be more intuitive to imagine that people in the same nation are influenced to different degrees and by different cultures (e.g., national, organizational, ethnic, religious) (Hofstede 1980, Yoo et al. 2011).

Interestingly, research in the information systems field has also challenged the assumption that different cultural values can only be observed at a national level, as suggested by Hofstede (1980) (Srite

and Karahanna 2006, Straub et al. 2002). Based on the literature of cultural psychology and cultural traits measured by personality tests at the individual level of analysis and taking into consideration Hofstede's cultural aspects, Srite and Karahanna successfully test the influence of personal cultural values on constructs of the theory of acceptance with two studies with samples coming from a multicultural university in the USA. That is, the authors studied cultural values using two samples uniquely drawn from a country.

Armed with nearly four decades of thought, 45 work, and reflection in psychology, education, healthcare, and elsewhere on the differences between secondary and primary control, we can start exploring the proposed implications of reconstructing privacy control as secondary privacy control and primary privacy control. The first study, Study 1, provides a deeper appreciation of control to formulate and empirically test a framework of privacy control that incorporates the major advances in information privacy literature with the renewed conceptualization of control in other fields. More broadly, this balanced and theory-rich perspective of control have implications in new and emerging areas of information systems where human cognition must meet and accept and adjust to information technology stressors. The second study, Study 2, offers a different setting yet also related to social networking services that takes advantage of an external event which allows to capture their causal effect on behavioral outcomes. This quasi-natural experiment, offers relevant managerial insights by discovering that secondary privacy control can be of benefit for social network companies to retain users, but also warning them about the risk involved with these strategies in deterring users to accept organizational solutions to protect them. All-in-all, both studies provide support for the soundness of this new perspective of information privacy control.



## Chapter 3: Study 1

### Social Networking Services and Protective Intentions

Social network users, in contrast to members of other social media such as online communities, join social network platforms to gather with people they principally know from their face-to-face interactions and with whom they share strong interpersonal ties (Karahanna et al. 2018). Additionally, social network platforms are places where people look for entertainment and even hold records of their own lives and for their own use. Moreover, these platforms offer the functionality to establish job connections, expand businesses, or even for finding a job (Sreenivasan 2022). These digital interactions require users the representation of their real selves and so they must demonstrate their authentic values. Research on social network services have also emphasized these unique characteristics as the maintenance of one's identity (Boyd and Ellison 2008, Karahanna et al. 2018). As a consequence, users' personal information widely appears in these environments and so issues around their privacy have a great impact on them.

As platforms designed mainly to maintain social relationships, social network services offer great flexibility for self-representation (Boyd and Ellison 2008, Karahanna et al. 2018), from tools to craft one's personal profile to various features that enhance one's social interactions. Moreover, many functionalities enabled by social network services promote highly unstructured ways of expression. For example, users can sometimes generally describe their own biography. Alternatively, interaction features allow users to follow others or manage their list of friends to create complex graphs of interrelationships. Thus, managing the impression users give to others on these platforms is not simply limited to privacy settings, but open to the full agency of users as they use the various affordances of the platform. Moreover, users can calibrate their level of self-disclosure in various ways such as writing messages in ways that protect their privacy.

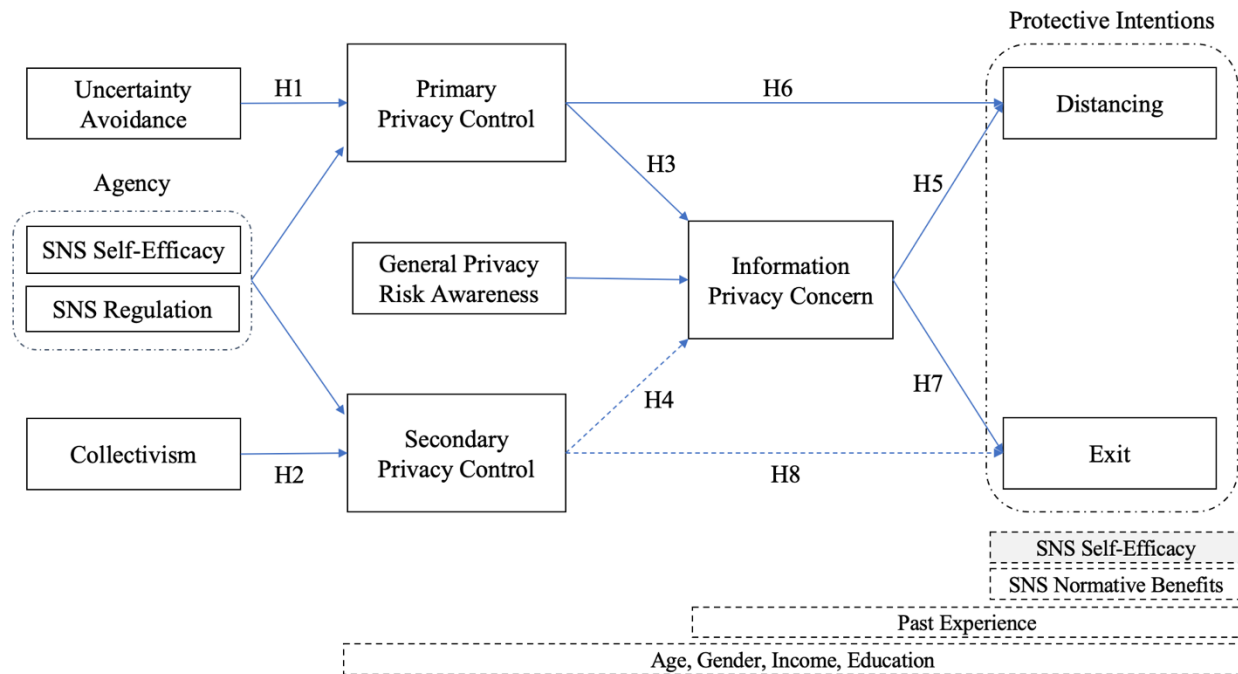
Furthermore, social networking users must continuously invest effort to balance their privacy protection with the creation and maintenance of their personal relations. As such, balancing the trade-off

between privacy and interpersonal relations is more salient in social networking platforms than in other social media where users can remain anonymous or pseudonymous. Thus, social networks form a context where primary privacy control strategies would be exercised to their greatest extent. At the same time, users of these platforms must inevitably follow the expectations of their most valued relations, be family, friends, one's broader community, or even colleagues. These obligations translate into constraints about the way in which interactions must be carried out, and so secondary privacy control will be very salient as one cannot always execute the privacy strategies, they personally desire.

Similarly, different groups of people, and so cultures, gather in social networking platforms for their interactions. The worldwide mixture of users is of the most favorable scenarios for researchers to observe the ample variability of people's concerns regarding privacy. Moreover, in interacting with members of their in-group, users naturally rely on their personal values and agentic orientations which contribute to their reactions to privacy threats. Importantly, an alarming increment of privacy breaches in social networking platforms is affecting their user-base. Overall, the mixture of cultural groups and privacy threats set favorable conditions to the expression of users' privacy concerns and privacy control strategies.

### **Secondary and Primary Privacy-Control Framework**

We build a conceptual framework particularly developed to complement our current understanding of information privacy control (Figure 1) alongside a conceptualization table (Table 3).



Notes: Negative associations use dashed lines; Correlates are in dashed boxes, and are positioned below the constructs they are associated with.

Figure 1: Conceptualization of Proposed Model

Table 3: Conceptualization of Constructs in the Proposed Model

| Construct                      | Definition   | Representative Item   |
|--------------------------------|--|---|
| SNS Self-Efficacy              | A sense of mastery over the full range of self-expression features available on social networking platforms.   | "I believe I can succeed at using most any feature on Facebook to which I set my mind."   |
| SNS Regulation                 | Confidence in the power of government regulation and industry self-regulation to safeguard privacy on social networking platforms.                                       | "I am confident that the government or market can be effective in enforcing mechanisms to protect user's privacy on platforms like Facebook." |
| Uncertainty Avoidance          | Degree to which an individual generally perceives rules, regulations, instructions and procedures to be important for their development in the face of risky situations. | "Rules/regulations are important to me."  |
| Collectivism                   | Degree to which an individual generally perceives a group to be a more powerful force than oneself in influencing decisions.   | "Group success is more important than individual success."  |
| Secondary Privacy Control      | Attempts to gain a feeling of control over one's privacy by accepting and adjusting to undesirable privacy conditions.   | "Whatever privacy issues there are on Facebook, things will work out for the best anyway."  |
| Primary Privacy Control        | Attempts to gain a control over one's privacy by personally changing undesirable privacy conditions.   | "No matter what Facebook does with my information, I like to take steps to keep my privacy safe."   |
| Information Privacy Concern    | A tendency to worry about information privacy.   | "I am concerned that Facebook may share my preferences and information with other parties without getting my authorization."                  |
| General Privacy Risk Awareness | Externally acquired information on common privacy vulnerabilities.   | "In general, it could be risky for people to put personal information on Facebook."   |
| Distancing Intention           | Intentions to distance oneself from the platform and its users.  | "In future, I plan to delete contents on my Facebook timeline to hide somethings from others."  |
| Exit Intention                 | Intentions to stop using the platform altogether.  | "In future, I plan to stop using my Facebook account at some point to maintain my privacy."   |

Using the two-process model of control theory (Rothbaum et al. 1982), this fairly complex framework describes a cohesive story of control and concern that can explain the surprising findings in the information systems literature (Miltgen and Peyrad-Guillard 2014, Wang et al. 2016). While the framework also includes our current understanding of agentic antecedents (Xu et al. 2012), attention is directed to the differential effects of the newly proposed personal cultural-value antecedents on secondary and primary privacy controls. Moreover, the model shows that privacy protective intentions are as much the product of privacy concern as of the two dissimilar privacy control orientations.

### **Privacy Control**

The research on information privacy control has asserted that a sense of agency is the key antecedent to IT users' perceptions of privacy control, and that this sense of agency can come from one's own inner confidence or from faith in outside regulations (Xu et al. 2012). But although agency lets people see that desired outcomes are achievable, people also need to be certain about how to go about achieving such outcomes (Lewis 1930, Pouget et al. 2016, Trommsdorff 1994). The culturally informed personal values identified in the literature of dual controls and in the information systems literature deal with the ways in which people manage major uncertainties in life such as how others see us.

### **Agency and Control**

Information systems researchers have argued that privacy control comes fundamentally from a sense of agency, be it a personal sense or one derived from associating with powerful others (Xu et al. 2012). Personal agency is most often represented as self-efficacy (Bandura 1982), an individual's perceived mastery towards one's environment (Bandura 2006). This well-understood representation of agency in information systems that continues to be seen as an important factor that impacts how we interact with information technology across almost every conceivable context (Crossler and Bélanger 2019, Kim et al. 2012, Marakas et al. 2007, Ray et al. 2014, Thatcher and Perrewé 2002, Venkatesh 2000).

Social networking services provide users with a platform on which they can exercise their social mastery, in terms of how they present and manage their image to others – for example, in their public profiles, their comments, and other activities on their timeline (Karahanna et al. 2018). Adjusting the numerous privacy settings is a starting point for users to manage their privacy (Crossler and Bélanger 2019), but users can use a fuller set of social and technological capabilities to manage their reputation. For example, users can be more careful in how they word their submitted content, or more strategic in selecting photos and events to share. Users can also choose to remove tags and mentions to alter their visibility or decide whether to check-in or not. Thus, it is not enough to examine self-efficacy from the narrow point-of-view of manipulating privacy settings. Instead, we conceive of a broader SNS self-efficacy, which relates to one’s sense of mastery over the full range of self-expression features available on social networking services.

Although self-efficacy is the most powerful expression of personal agency (Bandura 2006), privacy regulation is the hallmark of proxy agency in information privacy research (Xu et al. 2012). Such a proxy sense of agency is a cognitive tie that arises from associating with efficacious others (Rothbaum et al. 1982). However, the mere presence of regulatory authorities does not reassure users; reassurance requires they must also perceive regulatory entities to be efficacious in enforcing regulations (Pavlou and Gefen 2004). Thus, the construct of *SNS regulation* captures one’s confidence in the power of government regulation and industry self-regulation to safeguard privacy on social networking platforms.

This model recognizes that previously proposed agentic antecedents, represented by SNS self-efficacy and SNS regulation, will correspond to enhanced secondary and primary privacy control orientations in a social networking context. Both senses of agency should lead users to believe that their direct actions to exercise control over their privacy are likely to succeed and that the platforms cannot thwart their intentions. However, although social networking services take their own measures to safeguard users’ personal information, recent privacy breaches have raised the need for regulatory

agencies to take part in privacy protection matters in social networking services and beyond (The Economist 2019). Thus, a strong sense of agency is also beneficial to users who would rather accept and adjust to reduced privacy conditions because they can be optimistic about re-exerting control at a later point in time or they can simply rely on regulations to feel they are keeping privacy issues under control.

Importantly, SNS self-efficacy is also proposed to have effects beyond the dual privacy control mediators in the model. Generally, self-efficacy has demonstrated to be an omnipotent concept that has direct effects on behavior (Crossler and Bélanger 2019) even when mediators are proposed (Ray et al. 2014). Consequently, it is not possible to discard the influence of SNS self-efficacy on distancing and exit intentions. Nonetheless, it is expected that a user's sense of agency alone does not indicate which of the two dual privacy controls will be favored.

Culturally-Informed Personal Values and Control

Research in the information systems literature have suggested that a sense of privacy control increases with certainty about the direction of their reputations (i.e., Dinev and Hart 2004). The dual controls literature highlights that cultural values that emphasize the importance of social structures such as rules and social roles facilitate the predictability of social situations (Weisz et al. 1984). Moreover, the literature on cultural values also suggest that uncertainty avoidance and collectivism are the closest related to attaining predictability of social interactions (Hofstede 1984).

Societies that seem to better deal with threats to their progress by building their own rules or adopting a given structure of rules are said to value uncertainty avoidance (Hofstede 1980). Uncertainty avoidance is conceived as the degree to which an individual generally perceives rules, regulations, instructions and procedures to be important for one's development in the face of risky or new situations (Jung and Kellaris 2004, Yoo et al. 2011). Social network users who value uncertainty avoidance might rely on self-developed or existing rule-of-thumb responses that can protect their privacy. Such users

might consider the ramifications of posting sudden personal thoughts or candid photos, and habitually restrain themselves from doing so. They might also worry about how they will be perceived when they are tagged or mentioned on other people's postings, and might develop a personal policy of actively removing tags or mentions when they receive notifications of those. These users are essentially undertaking a primary control orientation by envisioning outcomes that might require them to take appropriate actions to reduce uncertainty and risk (Trommsdorff 1994, Zhou et al. 2012).

In addition to avoiding risky outcomes using response heuristics, uncertainty avoidance motivates people to gain a deeper understanding of their situation so as to be certain that their strategies will succeed and make outcomes predictable (Gefen and Straub 2004, Bordia et al. 2004). Similarly, these users might also be willing to gain a more deeply understanding of how their social networking platforms manage privacy so they can keep generating new privacy protective habits. Social networking users high on uncertainty avoidance are likely to take precautions that they have come to understand ought to generally protect their privacy under all circumstances, and not just in response to new developments. For example, they might consider searching online or asking their friends in order to understand how their privacy settings work and so be ready to limit who is able to find or view their profile. From their understanding of how profile information and postings are interpreted, they might also plan to omit certain information on their profile or might think of deleting their own previous postings to manage the overall impression of their timeline. These users are again taking a primary control orientation, by building their understanding of problems and circumstances to ensure successful outcomes (Rothbaum et al. 1982).

Overall, we expect social-networking users who value uncertainty avoidance to take a primary privacy-control approach, wherein they foresee risky outcomes and seek to understand successful strategies, so that they can employ privacy heuristics, adjust settings, and manage their presence on the platform. In contrast, we do not expect users low in uncertainty avoidance to adopt a primary privacy control orientation because they would not feel the need to personally seek ways to avoid risk and gain

deeper understanding. Such users would thus lack the necessary motivation to invest effort and time in finding, crafting or following privacy protective strategies.

*H1: Uncertainty avoidance will be positively associated with primary privacy control.*

Privacy appears to be a common issue across cultures, though different societies focus on different aspects of it (Whitman 2004) and so an alternative to investing personal efforts at uncertainty avoidance, or in addition to it, some people value reducing uncertainty about themselves and others by identifying with a powerful group and embracing their goals and purposes. This value, known as collectivism, is often considered to be a broad cultural-level trait (Hofstede 1980). But collectivism beliefs vary greatly between individuals of the same cultures, wherein it is the degree to which individuals generally perceive a group to be a more powerful force than themselves in influencing decisions (Yoo et al. 2011). Those who possess a collectivist trait tend to identify with the most relevant group to enhance their own effectiveness (Weisz et al. 1984). But this strategy requires submerging one's own sense of self at times, in favor of a sense of collective agency (Rothbaum et al. 1982, Zemba et al. 2006). Collectivism beliefs allow individuals to temporarily silence personal needs to enhance the value of following the group's goals and purposes (Hogg 2009). In reducing uncertainty around privacy, a collectivistic value is the natural counterpart to uncertainty avoidance because it allows users to follow heuristics and make future outcomes predictable, albeit without investing personal effort.

People who value collectivism seek a degree of certainty that their personal beliefs align with those of others, and so they align themselves with a desirable group that provides them a sense of identity and allows them to predict in-group undertakings (Hogg 2009). Similarly, social networking users who value collectivism conform with the norms and beliefs of their family, friends, and broader community, to gain a sense of identity and to feel safe in risky social interactions. Such users, for example, might consider revealing similar information their family, friends or community choose to disclose as a way of reciprocity to them. They might also plan to share personal information they expect their family, friends,



or community expect to know about them. More generally, these users might feel they can safely disclose information with the group because they assume these others act in prescribed ways. People who value a collectivistic trait adopt a secondary control orientation because by conforming with the group's demands they profit from predictable outcomes (Trommsdorff and Essau 1998, Weisz et al 1984).

Those who embrace collectivism define themselves and others as aspects of their group, which not only shields them from perceiving personal risks, but also allows them to blame others in case of group losses (Zemba et al. 2006). Similarly, social networking users who embrace collectivistic values can only perceive privacy threats to their group and so deliberately avoid considering threats to their own privacy, in addition to likely blame social networking services for privacy loss. Such selective attention might translate into seemingly 'doing nothing' to protect their personal privacy on these platforms. However, when finally feeling their personal privacy under imminent threat, they might decide to defer responsibility to chance, or blame external entities for not taking the necessary steps to protect them in privacy matters. These approaches correspond to secondary control strategies where people deliberately allow powerful forces to decide the appropriate ways to respond to social situations (Zhou et al. 2012).

Overall, social networking users with a collectivistic value more likely desire to fit in with their family, friends and community and so adopt secondary privacy control strategies. These strategies allow them not only to build harmonious and interdependent social relationships but also to find shelter in them in the face of privacy threats. Contrary, users with scarce collectivistic values are not expected to align with secondary privacy control strategies because these individuals might think of their goals and identity as separated from those of their group.

***H2: Collectivism will be positively associated with secondary privacy control.***

Rothbaum et al.'s (1982) theory on the dual nature of control has been recognized as adequate to study control among people varying in cultural values (Ji et al. 2000, Trommsdorff and Essau 1998, Weisz et al. 1984). Intentionally, the effect of uncertainty avoidance on secondary privacy control is not proposed

as it would be counterintuitive to imagine that the effort and time invested in creating and following ways to provide the desired impression of oneself to others might lead to acceptance and adjustment of privacy issues. Similarly, the effects of collectivism on primary privacy control are not proposed as those who see their privacy contingent to their in-group are unlikely to perceive personal threats to their privacy, let alone feel motivated to invest effort and time to protect it.

### **Information Privacy Concern**

Even early investigations into the disclosure of digital personal information foresaw imminent threats to privacy in the Information Age (Mason 1986). As expected, the continuous developments in information processing capabilities of public and private organizations facilitated unwitting storage, intentional misuse, unauthorized access, and loss of users' information (Buchanan et al. 2007). These increasing threats to privacy gave rise to counter-efforts in information systems research to understand the implications of personal information disclosure, with *privacy concern* becoming the seminal construct of interest in this direction (Smith et al. 1996). Privacy concern is defined as “*one's tendency to worry about information privacy*” (Malhotra et al. 2004). Privacy concern is important because it influences key outcomes such as disclosing information, resisting online transactions, spreading negative word-of-mouth, or even adopting new technologies (Culnan and Armstrong 1999, Son and Kim 2008). Researchers have since delved into information privacy concern in a wide range of information systems: general Internet use (Hong and Thong 2013), online commerce (Dinev and Hart 2006), synchronous communications (Jiang et al 2013), and location-based mobile services (Xu et al 2012). The information privacy concern construct has consequently grown into a large multi-dimensional concept in information systems research that came to encompass all of the factors regarding privacy perceptions (Malhotra et al. 2004, Smith et al. 1996). Recent studies have even included concerns about peers obstructing one's privacy protection into the conception of privacy concern (Zhang et al. 2022).

In studying why people disclose personal information, researchers have correlated information privacy concern with perceptions of fairness in the collection, manipulation, and use of personal identifiable information by service providers (Malhotra et al. 2004, Smith et al. 1996). The growing consensus is that users' sense of fairness is only met when a service grants them control over their submitted information (Hong and Thong 2013, Malhotra et al. 2004), making information privacy control a necessary condition to establish one's level of concern. Eventually, privacy control emerged in the literature as a construct in its own right, as a precursor to privacy concern (Dinev and Hart 2004, Wang et al. 2016, Xu et al. 2012).

#### Privacy Control and Privacy Concern

The conventional wisdom is that privacy control reduces one's privacy concern (Dinev and Hart 2004, Xu et al. 2012). Researchers attribute this ameliorating effect of privacy control to how it reduces users' risk perceptions of their own privacy vulnerability to opportunistic behavior of service providers (Culnan and Armstrong 1999). However, not all empirical studies of privacy control and privacy concern arrive at the same findings. Prior to the separation of the two constructs, a study that pitted privacy control as a dimension of a second-order privacy-concern construct found that privacy control perceptions were positively correlated to other aspects of privacy concern (Malhotra et al. 2004). We deduce from that finding that the more privacy control one has over one's information, the more concerned one is. An empirical study of information disclosure intentions of mobile app users found that, against theorized expectations, privacy control perceptions increased one's concern for privacy risks (Wang et al. 2016). Similarly, qualitative studies have also found that compared to inhabitants of the south, those from north Europe show important differences in their interpretation of privacy concern (Miltgen and Peyrad-Guillard 2014). More relevant to this discussion, these authors attribute the difference in privacy concern to differences in their sense of responsibility and faith: both notions closely linked privacy control.

The tension of both these streams of findings suggests that the relation between privacy control and privacy concern is complex. In the following lines it is argued that this complexity arises because of the dual nature of privacy control. Specifically, it is expected that social network users with a primary privacy control orientation might always be concerned about their privacy, even if they feel momentarily secure. Being present and aware of one's environment is a defining characteristic of the way in which people with a primary control orientation function effectively (Rothbaum et al. 1982). These users are determined to proactively lower uncertainty by understanding their risks of information disclosure, taking care of the way they use the various affordances of social networking platforms, and nurturing their confidence by learning to deal with similar situations and platforms in future opportunities. These users should be concerned about providing information to even seemingly benevolent service providers or they might express concern about new developments in the social networking platform that could affect their privacy in future. Consequently, they have the motivation and means to stay alert for new threats.

This postulation is in line with the study of information disclosure on mobile apps (Wang et al. 2016) which surmised that information systems users with a high sense of privacy control might simply be more aware of the risks entailed in online activities. Moreover, it is also in line with the study of interpretations of information privacy concern in different cultures (Miltgen and Peyrad-Guillard 2014), in which they attribute these differences to the concept of responsibility. The expectation that a determination to obtain results leads to enhanced awareness is more generally echoed in other areas of research. For example, research on entrepreneurship suggests that a natural desire to personally '*fulfil a vision*', which reflects primary control, keeps individuals in a state of high alertness rather than being lulled to inattentiveness (Yu 2001). In contrast, it is not expected that social network users with a low sense of primary privacy control to remain ever-vigilant to privacy risks, as they lack motivation to reduce personal uncertainty and lack the relevant agency needed to continuously and indefinitely counter such threats. In summary, this proposition goes against conventional wisdom and anticipates users who

are more strongly oriented towards primary privacy control to have increased levels of information privacy concern.

*H3: Primary privacy control will be positively associated with information privacy concern.*

Complementary, for some users, privacy control could reduce information privacy concern if they tap into feelings of secondary privacy control. The goal of the secondary control orientation is to achieve peace-of-mind when facing challenging situations that people cannot personally overcome (Morling and Evered 2006). It is expected that social networking users with a secondary privacy control orientation attempt to reduce uncertainty about how others see them by aligning themselves with their views and the way they perform in these sociotechnical environments. These users might also have faith in the efficacy of regulatory mechanisms to help them envision that everything will simply turn out fine under the trusted guidance of government and industry. Given their stronger collectivist leanings, these users might mainly consider whether privacy issues threaten their larger relevant in-group rather than themselves. This collectivist approach would allow them to largely dismiss the personal costs of privacy loss, and focus on the benefits of networking with friends, family, and community. A remarkable consequence of delegating responsibility and cost away from one's self, is that people under secondary control can even rationalize positive outcomes from negative circumstances (Hall et al. 2006b).

Thus, social networking users oriented towards secondary privacy control have a fairly positive outlook on their personal privacy while recognizing general risks for others on these platforms. In contrast, those not oriented towards secondary privacy control do not have faith in regulations or cannot overlook the personal costs of privacy loss, so they are quite likely to remain concerned about privacy. Overall, social networking users with a secondary privacy control orientation might be able to lower their information privacy concern.

*H4: Secondary privacy control will be negatively associated with information privacy concern.*

## General Privacy Risk Awareness and Privacy Concern

Beyond the personal orientation of privacy control, users are constantly informed of privacy related events on social network platforms via news media, online discussions, and other word-of-mouth (Malhotra et al. 2004). This external information about social networking privacy developments does not include one's specific privacy concern, but rather the awareness of the general privacy risk inherent to all users of the social networking platform. Users exposed to these media reports regarding privacy breaches must at least entertain the possibility of being affected by these issues themselves. Researchers have found that this externally acquired information on common privacy vulnerabilities generally frames users' degree of concern about their own privacy because they must decide whether these specific risks threaten them (Dinev and Hart 2006, Tyler and Cook 1984). For example, exposed users to media have an increased need to reclaim their data or data ownership expressed by their desire to download their profile, photos, and other content automatically, not to mention their enhanced desire to demand corrections of inaccurate or deceptive content (Shipman and Marshall 2020). In line with other studies, we accept that it is vitally important to distinguish between the effects of the dual privacy controls and the effect of broader risk assessments on one's specific privacy concern. Thus, we include general privacy risk awareness in our model as an important correlate of privacy concern.

### **Privacy Protective Intentions**

People strike a balance between misrepresenting themselves and managing relations with others (DePaulo et al. 1996, Jiang et al. 2013, Origgi 2018). Privacy related intentions such as disclosing personal information is unequivocally believed to be determined by one's information privacy concern (Hong and Thong 2013, Pavlou 2011). More broadly, users concerned with the privacy practices of service providers will strategize ways to protect themselves from potentially opportunistic behavior, and sometimes they will do so in ways that are unfavorable to the provider's business model (Baumer et al. 2013, Son and Kim 2008, Wisniewski et al. 2014). As this study emphasizes the individual control of

outcomes, we are most interested in private actions that aim to directly alter one's immediate privacy outlook, rather than public actions that mainly aim for abstract long-term societal impact (Son and Kim 2008). Consequently, only platform-specific actions that users can undertake such as distancing oneself from the platform and other users by reducing information provision, and exiting the platform altogether (Baumer et al. 2013, Wisniewski et al. 2014) are considered.

Internet users, out of concern for their privacy, can refuse to give personal information for services (Son and Kim 2008). Distancing from a social network goes beyond simply refusing to provide new information and includes even removing prior posts, photos, tags, and mentions of oneself by others. In the context of social networking, researchers have found many users intensively manage their interpersonal privacy boundaries by carefully handling their reputations in these ways (Wisniewski et al. 2014). However, users with low information privacy concern might not distance themselves from the service because doing so would only curtail their ability to enjoy the benefits of their network. But social network users with high information privacy concern should resort to distancing as a way of mitigating future concerns.

*H5: Information privacy concern will be positively associated with distancing intention.*

Proactively changing one's environment is a hallmark of primary control (Hall et al. 2006a). Thus, it is likely that social network users with a strong sense of primary privacy control proactively apply *a priori* strategies that allow them to stay a step ahead of potential privacy breaches, regardless of their current level of concern. For example, as part of their daily interactions, they may regularly ensure they do not appear in unintended posts, tags, or other materials. These users might also attempt to reduce their interactions in these platforms by limiting their time spent on social networking platforms. In contrast, because they are not motivated to independently pursue actions to alter privacy outcomes, it is not expected that users low in primary privacy control will distance themselves from the platform or their network. Nor that users with a secondary privacy control orientation correlate to distancing intentions

because they generally avoid taking strong but risky actions to avoid outcomes, preferring instead to accept and adjust themselves to the inevitable.

*H6: Primary privacy control will be positively associated with distancing intention.*

A more definitive way to lower one's specific privacy risks is to simply terminate relations with the social network platform. Exiting a service relationship is an extreme response by consumers to concerns about the deteriorating quality of a service (Hirschman 1970). Probably, users highly concerned about their privacy would be inclined toward erasing their digital presence by abandoning, deactivating or even deleting their accounts as a form of exit. These users might also ruminate ahead of time on important questions such as whether and how to inform their family, friends, or closer circle about their decision to leave the social networking service. The possible effect of privacy concern on exits has been raised in exploratory empirical research (Baumer et al. 2013, Son and Kim 2008) but has not been formally theorized or empirically confirmed. Users low in information privacy concern might not be motivated to exit their social networking platform. If they did, they would incur the costs of losing online access without any benefits from doing so.

*H7: Information privacy concern will be positively associated with exit intention.*

Secondary control generally lets individuals be selective in their focus of attention to avoid taking immediate responsibility (Zhou et al. 2012). Thus, it is not expected that users with a secondary privacy control orientation take the direct actions required to leave a platform. Moreover, social network users with a sense of secondary privacy control are likely to focus more on the personal benefits of using social network platforms than on the risks. In contrast, users with a more salient secondary privacy control orientation might not distance themselves from the service provider because these users are not motivated to independently pursue privacy outcomes.

*H8: Secondary privacy control will be negatively associated with exit intention.*



## **Important Correlates or Control Constructs and Variables**

The major constructs in our proposed model do not reflect the many positive motivations and benefits in users' privacy calculations (Dinev and Hart 2006). Social networks benefit users by allowing them to remotely and efficiently maintain in-group status with important social groups, regardless of their perceptions of control and concern. Such intangible social rewards motivate users to disclose private information to their social network because normative expectations such as reciprocity govern their interactions (Jiang et al. 2013). Thus, as an important correlate of distancing and exit intentions, *SNS normative* includes the perceptions of this range of benefits of using social network platforms in line with the expectations of others that is included in the proposed model as a correlate of the outcomes.

Based on prior empirical findings (Xu et al. 2012), past experience capturing negative experiences with privacy issues significantly impacted users' concerns and intentions to use location-based services. Evidence suggests that men and women might benefit differently from secondary versus primary control (Chipperfield and Perry 2006, Seginer et al. 1993). Similarly, studies on aging have posited that preferences for primary rather than secondary control strategies might be linked to differences in resource access (Chipperfield et al. 1999). And lastly, income is one major socioeconomic difference between cultural groups (Yoo et al. 2011). Consequently, single-item measures of gender, age, and income are included in the proposed model as correlates of the dual privacy controls, information privacy concern, and protective privacy intentions.

In addition to the correlates, potential unpredicted effects were tested in a full model that considers cross effects on our mediators and overriding effects of antecedents on outcomes. Moreover, a comparison of the effects of secondary privacy control and primary privacy control with general privacy control found in the literature (Xu et al. 2012) is proposed to account for potential differences or similarities in constructs.

## **Empirical Validation of Study 1**

A fundamental motivation of this study was to adapt the dual nature of control from the psychology literature to the privacy context to understand why some users of social networking services seemed to be less concerned about their privacy. In the paragraphs above, secondary privacy control and primary privacy control were proposed within their respective nomological network and accompanied by the corresponding expansion of hypotheses. It is time to seek validation for the proposed framework through a cross-sectional survey of Facebook users. The following paragraphs also describe how the needs to refine and provide behavior as outcomes guided efforts to design and validate the second study, Study 2.

### **Context: The Facebook SNS**

Social networking services are of special interest because they offer great flexibility in expression and reputation management. Facebook in particular, strongly encourages users to retain their day-to-day identity and roles to their family, peers, and broader community (Facebook 2020b). Facebook offers users more ways to build their reputation in front of others than other networking services such as Instagram or Pinterest (Karahanna et al. 2018): users can share their opinions, views, interests, personal information, or photos at various places on the platform and for as long as they want. Furthermore, when a user mentions a friend's username in a post, Facebook gives readers a hyperlink to immediately access their friends' profile. This extend of flexibility afforded through technological features enabled in their platform allow users to represent themselves as they want to be seen by others. So, the varied levels of self-disclosure that users can choose to exercise yields a high variation in levels of dual privacy controls and privacy concern perceptions among users.

Facebook is one of the most widely used social networking services (Edison Research 2019, 2022). Thus, people from different cultures and socioeconomic backgrounds gather in this platform to engage in various types of social interactions (Vasalou 2010). Moreover, the flexibility for self-expression and the varied backgrounds of users allow the company, and third-party observers, to collect

a rich amount of data about each user (Fowler 2022). Not surprisingly, Facebook is constantly the focus of public controversy regarding privacy (Heiligenstein 2022). As a response, Facebook has also introduced settings that allows users to set limits on how much of their information and posted content others can see (Facebook 2020a). The company has steadily broadened the set of measures that they assert give users more control in responding to privacy threats as evidenced by this excerpt: *“In January [of 2018], Facebook released a set of privacy principles explaining how users can take more control of their data.”* (Newcomb 2018). Thus, an increased variance in users’ assorted privacy related beliefs and awareness is expected, with some users taking these issues to heart while others dismissing the revelations. Additionally, given the number of users of this platform, the results of this study can be generalized to most social networking services.

## **Survey Design and Deployment**

### Measurement Items

The survey was developed based on the identification of validated scales for each of the constructs in the literatures of information systems, achievement motivation, organizational research, marketing, and clinical psychology (see Appendix A). Items from these scales were at times modifies to match the Facebook context, and at others, adapted without modifications.

The collection of items for SNS self-efficacy comprises four out of eight considered in the organizational literature (Chen et al. 2001). These items capture respondents’ confidence in successfully using a broad range of Facebook features, in contrast to those relate to exceptionally difficult tasks not easily present in users, and those related to personal goals that do not apply to the use of social networking services. Items for SNS regulation from Gefen and Pavlou (2006), adapted to the Facebook context, comprise those related to the degree to which individuals are confident of governments or market self-regulation actions to protect and resolve issues around privacy. Items for culturally-informed personal

values such as uncertainty avoidance and collectivism were borrowed from the marketing literature (Yoo et al. 2011) without adaptation, as they reflect personal traits and characteristics for any decision making. For uncertainty avoidance, only three items reflect the general importance of rules and regulations to the individual, thus, the other two items measuring organizational tasks that did not match this context were avoided. Similarly, only three items of collectivism capture the importance of group success as a value, while the other two items were related to sacrifice and loyalty that were too extraordinary for the context of using a web service.

Control implies using certain means to achieve important goals (Morling and Evered 2006), and as such, any type of control is a combination of a strategy and an expected result (Hall et al. 2006b). Thus, both secondary and primary control approaches integrate the expectation of a favorable result from a feasible personal strategy. But, where the two forms of control differ in the goal of their strategy-outcome combination: whereas secondary control entails to accept and adjust to challenging situations, primary control entails to solve or master trying situations (Rothbaum et al. 1982, Chipperfield and Perry 1999). The seminal conceptualization of a two-process model of control explains seeking control to either achieve or avoid particular results. Although some studies operationalized secondary and primary control as beliefs regarding desirable or undesirable results (Seginer et al. 1993), more recent research further added control strategies about how and in which direction efforts are invested. Combining control strategies and result beliefs is thought to reflect the “*personal use of control-enhancing techniques*” (Hall et al. 2006b) and more faithfully represent Rothbaum et al.’s (1982) original conceptualization (Morling and Evered 2006). Thus, secondary and primary privacy control were adapted from studies of dual controls in psychology (Grootenhuis et al. 1996, Hall et al. 2006b, Thompson et al. 1998) that more faithfully understand the concept of secondary privacy control (Rothbaum et al. 1982).

Secondary control is proposed to be a composite with four-dimension (Hall et al. 2006b) but most studies considering the four dimensions have mostly found that only one or two of them worked as

expected (see Operationalizing Secondary Control). Additionally, as a new construct to the information systems literature, the benefits and drawbacks of secondary privacy control might be better appreciated if a holistic notion is discussed only in contrast to primary privacy control, at least to sets solid grounds for further development. Nonetheless, an analysis of its composite nature is later in place. Eight items were adapted from the secondary control literature (Grootenhuis et al. 1996, Hall et al. 2006b, Thompson et al. 1998) and then examined in terms of their conceptual match, acceptance and adjustment to privacy challenges. They were also empirically analyzed to find the best match of common variance. Eventually, the best three items matching both criteria were selected to represent secondary privacy control (Appendix B). For example, those agreeing with “*Whatever privacy issues there are on Facebook, things will work out for the best anyway*” acknowledge that there are privacy issues on Facebook and then attempt to adjust to them by aligning themselves with luck, God, or any other powerful force. Likewise, primary privacy control is operationalized in four items capturing personal efforts to obtain desired privacy outcomes. “*No matter what Facebook does with my information, I like to take steps to keep my privacy safe*” represents a reliance on personal strategies that will result in protecting their privacy.

Information privacy concern captures context-specific characteristics given their advantage over general privacy concern measures (Malhotra et al. 2004). Items are adapted from three of Smith et al.’s (1996) dimensions of privacy concern: data collection, improper access, and unauthorized secondary use of data. However, the protection against errors dimension is excluded as it involves “*concerns that protections against deliberate and accidental errors in personal data are inadequate*” (Smith et al. 1996). Service-related error concerns seem to be more salient in research contexts such as location-based services where data is collected automatically by the provider without direct user input. However, error concern might be less relevant in the Facebook context where users primarily enter their own data, and so deliberate or accidental errors relate to user actions rather than the service. Compared to information privacy concerns, general privacy risk awareness is meant to capture the effects of exposure to privacy

news and opinions over the media. Four items for this concept are adapted from Malhotra et al.'s (2004) risk belief construct, with the omission of reversed items to avoid survey misresponse (Swain et al. 2008).

Distancing and exit intentions were created based directly on definitions from prior empirical research (Baumer et al. 2013, Wisniewski et al 2014). Analogous to Wisniewski et al.'s (2014) voice-related outcomes, three items were created for distancing – a recovery mechanism that allows social networking users to remain functional but less accessible on Facebook. Distancing intentions relate to the management of privacy, for instance, requesting friends to remove mentions of one's username, asking friends to delete content, and deleting one's own content. Baumer et al.'s (2013) conceptualization of an extreme privacy recovery response – exit-related outcome. Three items capture exit intentions focused on the different ways in which one can terminate usage: voluntary stopping, deactivation, and deletion of one's account.

Included in this framework, there are measures of covariates meant for statistical control. SNS normative benefits has three items adapted from Venkatesh et al. (2003) proposed to affect intentions. As they are subjective norms around technology use, they assess to what degree one's social-network use is valued by salient others (Jiang et al. 2013). Specifically, one item relating to 'actual help' that we do not expect to find in our online context was avoided. Personal experience with privacy issues used three items borrowed from Xu et al. (2012) who found them exacerbating information privacy concern. These items also consider the direct experience one gets from knowing others facing privacy issues. Single-item demographic measures of gender and age, and socioeconomic characteristics of income and education were all included in the framework to affect mediators and outcomes. Specifically, age was aggregated into age ranges as reported in consumer studies of Facebook (Hoadley et al. 2010). Moreover, age seems to be an important factor in the saliency of secondary and primary control (Chipperfield and Perry 1999). A set of qualitative information corresponding to respondents' perceptions of privacy on Facebook and their strategies to protect themselves was collected. We hoped that giving respondents

these qualitative opportunities would foster their deeper reflection and give us another perspective on privacy control.

#### Data Collection

Facebook is a rich context for privacy research at this moment, and a particular domain in which to examine the dual nature of privacy control. In ensuring that respondents are fully aware of the latest features and practices of Facebook, this study only includes respondents with a profile on the Facebook platform. An invitation reached 6,500 panelists in North America through an online marketing company. Out of 364 respondents, we identified 305 qualified respondents who were Facebook users with an active profile; this yielded an acceptable response rate of 5.6% comparable to other studies of information systems found in meta-analyses of response rates (Sivo et al. 2006, Pinsonneault and Kraemer 1993). The differences from the comparison between the first and the last 50 respondents in terms of demographics and means of estimated construct scores (Miller and Smith 1983, Sivo et al. 2006) is not significant (Appendix C). Additionally, the demographics and socioeconomic characteristics of this sample were similar to those of the population of Facebook users (Armstrong and Overton 1977, Miller and Smith 1983) (Appendix D). For example, the chi-squared parameter for the age distribution ( $\chi^2=42.01$ ,  $df=5$ ,  $p\text{-value}=0.999$ ), and for the gender distribution ( $\chi^2=0.02$ ,  $df=1$ ,  $p\text{-value}=0.345$ ) are both insignificant. Overall, the possibility that this sample contains variance attributed to non-response is low. On average, 48.2% of respondents were male and 51.8% female and the largest age bracket was from 35 to 44 years old (Table 4).

**Table 4: Demographic Information of Respondents**

| Gender     |             | Income*               |            | Education*              |            | Ethnicity |             |
|------------|-------------|-----------------------|------------|-------------------------|------------|-----------|-------------|
| Male       | 147 (48.2%) | less than \$30 000    | 27 (8.85%) | High school or less     | 2 (0.7%)   | Caucasian | 200 (65.6%) |
| Female     | 158 (51.8%) | \$30 000 - \$44 999   | 42 (13.8%) | High school graduated   | 26 (8.5%)  | Others    | 95 (31.1%)  |
|            |             | \$45 000 - \$59 999   | 48 (15.7%) | Some college            | 74 (24.3%) | NA        | 10 (3.3%)   |
|            |             | \$60 000 - \$79 999   | 53 (17.4%) | Vo-tech graduated       | 8 (2.6%)   |           |             |
| <b>Age</b> |             | \$80 000 - \$99 999   | 41 (13.4%) | College graduated       | 97 (31.8%) |           |             |
| Under 18   | 0 (0.0%)    | \$100 000 - \$124 999 | 30 (9.8%)  | Some post graduate work | 16 (5.2%)  |           |             |
| 18 - 24    | 7 (2.3%)    | \$125 or more         | 44 (14.4%) | Post graduate degree    | 71 (23.3%) |           |             |
| 25 - 34    | 64 (21.0%)  | Refused               | 9 (3.0%)   | Refuse to answer        | 0 (0.0%)   |           |             |
| 35 - 44    | 110 (36.1%) |                       |            |                         |            |           |             |
| 45 - 54    | 70 (23%)    |                       |            |                         |            |           |             |
| 55 - 64    | 7 (2.3%)    |                       |            |                         |            |           |             |
| 65 or      | 47 (15.4%)  |                       |            |                         |            |           |             |

Sample size (305); \* The sum does not equal 305 due to missing values.

Moreover, Table 5 shows nine sampled qualitative responses from male (45.5%) and female (55.5%) respondents between the 35-65 years old. They are separated into four combinations of the dual privacy controls, from high to low for each sense of control. The responses often indicate the users' combinations of strategies. Overall, control and concern are pervasive characteristics.

**Table 5: Sample of Qualitative Responses of Privacy Strategies on Facebook**

|                         |      | Secondary Privacy Control  |  |
|-------------------------|------|--|--|
|                         |      | Low  | High   |
| Primary Privacy Control | High | <p>"Limit information-sharing settings. If Facebook shares in defiance of this setting, they are liable. Limit what I say about myself (personal info) to Facebook, including [date-of-birth]. Maintain control over who can see &amp; respond to posts: I have a strict policy on who I "friend," as it has to be someone I know reasonably well. I use it as a friends &amp; family account only, so not open to everyone to reply/post on."</p> | <p>"I am concerned about the privacy issues with Facebook, but I realize that if I use Facebook that I will [not] be able to totally control the privacy issues, so I just try to be careful when i am on Facebook."</p> <p>"I feel exposed I do not have all the control of my information."</p>  |
|                         | Low  | <p>"My first suggestion would be reading up on the history of Facebook business practices that regard user privacy. Again, so much can be taken from so little and it is critical that someone that is 'new' to Facebook should be aware of the risks (despite the measures that have been taken since the huge privacy breach)."</p>  | <p>"It is a concern to me but mostly on the end of Facebook itself on how they take our personal information and distribute it. What we post and share is really under our control of whom we allow to see it and who we have on our friends lists. Bottom line: if I don't want someone to know something about me, I won't tell them. Period."</p> |
|                         | Low  | <p>"Not to have a Facebook account"</p> <p>"Never been a huge problem for me"</p>  | <p>"Be prepared to share your life when you log on to Facebook."</p> <p>"I stay off it and try not to worry about it when using it."</p>   |

**NOTES:** Nine sample responses to qualitative questions posed to respondents regarding strategies they use to protect their privacy on Facebook, and what advice they had for new users; Responses are the original text provided by respondents and have not been modified or corrected. Cases were categorized from averaged items of their primary and secondary privacy control responses.



## **Covariance Based Structural Equation Modeling (CB-SEM)**

In psychology, the empirical literature on secondary vs primary control has espoused a composite approach to modeling constructs (Hall et al. 2006b; Seginer et al. 1993) because the strategies for secondary control, in particular, are seen as heterogeneous and not always in concordance. Similarly, operationalizations of general privacy control in information systems (e.g., Dinev and Hart 2004, Xu et. al 2012) have also favored a composite modeling approach wherein their major constructs are viewed as weighted sums of their measurement items. Studies taking the composite modeling approach have used techniques such as exploratory factor analysis with regression, or the Partial Least Squares Path Modeling (PLS-PM) approach that is often seen as more suitable to exploring theory where concepts and measurements are not yet well defined (Hair et al. 2019).

However, most of our constructs have been tested and validated in prior empirical research and our hypothesized relationships argue for established principles of secondary versus primary control in the context of information privacy. And we have specifically argued that secondary privacy control should be seen as a convergent concept that captures how technology users sacrifice their expectations to match the inevitable loss of privacy which assures them psychological control when caring for every single aspect of their lives turns overwhelming. Moreover, a composite operationalization of secondary control has often obtained significant effects from one or at most two dimensions (Grootenhuis et al. 1996, Seginer et al. 1993) suggesting further need to understand their operationalization and even conceptual making. Interestingly, when proposing the four dimensions, Rothbaum et al. (1982) also warns about the conceptual overlap between dimensions. Consequently, before we understand the details of the components of secondary privacy control, it would seem wise to provide a global view of its origin and impact.

Thus, the constructs on the proposed framework (see Figure 1) are modelled as common factors or latent variables whose nature reflects upon the shared variance of their measured items. Following

current practice in research using covariance methods (Burns et al. 2019, Califf et al. 2020, Kuem et al. 2019, Trieu et al. 2022), a confirmatory factor analysis (CFA) of their measurement items was necessary. This analysis tells whether the variance shared between items and construct is sufficient to consider them reliable measures of that construct and so represents an assessment of the viability of the measurement model. The structural model viability assessment requires a path estimation through Covariance-Based Structural Equation Modeling (CB-SEM) where the constructs undergo a test to know if they represent what they are supposed to be measuring, and to ensure that no two-constructs are similarly explained by the items originally designed to measure one of them. Convergent and discriminant validity, respectively, enables the proper estimation of the relationships of a model. The principle of unidimensionality assures that each measured item reflects at most one single underlying construct (Hair et al. 1998). As the CB-SEM results of this study are not directly comparable to the composite model estimates from prior research, an examination of the proposed model using a composite perspective appears later.

### **Measurement Model**

In the R statistical platform (R Core Team 2017), the SEMinR (Ray et al. 2020) and the LAVAAN (Rosseel 2012) packages were used for model parameter specifications and estimation, respectively. CB-SEM uses the maximum likelihood approach to provide estimates of model parameters describing the state of the model. These estimates include item reliability, internal consistency, and convergent and discriminant validity. After running a CFA, items are expected to have a minimum standardized loading of 0.70 to indicate that at least half of the variance of the latent variable is explained by that specific item (Bagozzi and Yi 1988, Zhang et al. 2022).

Generally, items not reaching 0.70 were removed. As newly introduced notions to the information system literature, the secondary privacy control measurements alongside the primary privacy control measures were first analyzed using exploratory factor analysis (EFA) to see if any of the dimensions proposed by Rothbaum et al. (1982) were empirically salient in this study. In addition, this analysis was

accompanied by a conceptual validation. From both perspectives, empirical and theoretical, three items out of eight were chosen for secondary privacy control ( $\lambda_{SPC2}=0.748$ ,  $\lambda_{SPC4}=0.779$ ,  $\lambda_{SPC5}=0.912$ ) and four items out of five for primary privacy control ( $\lambda_{PPC1}=0.776$ ,  $\lambda_{PPC2}=0.811$ ,  $\lambda_{PPC4}=0.763$ ,  $\lambda_{PPC5}=0.797$ ). Additionally, the confirmatory factor analysis detected four items in three different constructs with low loadings (Appendix E). They were removed from the analysis. Two items related to the ‘collection’ dimension of the information privacy concern construct showed low loadings ( $\lambda_{CLL1}=0.632$  and  $\lambda_{CLL2}=0.648$ ). Removing these items did not represent a conceptual loss given that a third item (CLL3) had loaded sufficiently well ( $\lambda_{CLL3}=0.789$ ) to capture this dimension and maintain the original intent of information privacy concern. Similarly, we removed one item with from the collectivism construct (COL1;  $\lambda_{COL1}=0.443$ ) as it seems that and one item from past experience (PEXP3;  $\lambda_{PEXP3}=0.515$ ) as they loaded poorly on their respective constructs.

#### Internal Consistency and Construct Validity

Overall, the model fit parameters showed good fit (Gefen et al. 2011, Hooper et al. 2008, Zhang et al. 2022). Fit metrics included  $\chi^2=1566.608$ ,  $df=873$ ,  $p\text{-value}<0.001$ ,  $\chi^2/df=1.794$ ,  $RMSEA=0.051$ ,  $SRMR=0.040$ ,  $CFI=0.934$ ,  $NNFI=0.922$ , and  $TLI=0.922$ . Moreover, all values were within recommended ranges for studies in the category of sample sizes greater than 250 and with more than 30 measured variables (Hair et al. 2014). Table 6 shows the latent variables correlations alongside the measurement quality including parameters for internal consistency, and convergent and discriminant validity. The internal consistency estimation for each factor surpasses the 0.70 threshold (Bagozzi and Yi 1988), suggesting that the underlying measured variables represent a single common explanation for each factor. The average variance extracted, which is the average variance of a factor that is explained by its items, also surpasses 0.50 (Bagozzi and Yi 1988). Finally, discriminant validity, which we measured as the degree to which items reflecting a factor share more variance with that factor than with

other factors in the model, was assessed successfully by ensuring that the square root of AVE is higher than the construct correlations with other constructs (Fornell and Larcker 1981).

**Table 6:** Measurement Quality and Correlations

|      | Mean | SD   | CR ( $\rho$ C) | AVE  | $\sqrt{AVE}$ | SEFF         | REG          | COL          | UNA          | SPC          | PPC          | RISK         | PCON        | DIST         | EXIT         | NORM        | PEXP        | AGE          | GEN         | INC  | EDU  |  |
|------|------|------|----------------|------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|-------------|--------------|--------------|-------------|-------------|--------------|-------------|------|------|--|
| SEFF | 5.12 | 1.68 | 0.91           | 0.71 | 0.84         | 1.00         |              |              |              |              |              |              |             |              |              |             |             |              |             |      |      |  |
| REG  | 3.42 | 1.77 | 0.94           | 0.80 | 0.89         | 0.16         | 1.00         |              |              |              |              |              |             |              |              |             |             |              |             |      |      |  |
| COL  | 4.16 | 1.57 | 0.77           | 0.62 | 0.79         | <b>0.01</b>  | 0.38         | 1.00         |              |              |              |              |             |              |              |             |             |              |             |      |      |  |
| UNA  | 5.71 | 1.25 | 0.84           | 0.64 | 0.80         | 0.13         | <b>0.09</b>  | 0.16         | 1.00         |              |              |              |             |              |              |             |             |              |             |      |      |  |
| SPC  | 3.69 | 1.64 | 0.86           | 0.66 | 0.82         | 0.21         | 0.61         | 0.47         | 0.12         | 1.00         |              |              |             |              |              |             |             |              |             |      |      |  |
| PPC  | 5.77 | 1.34 | 0.87           | 0.62 | 0.79         | 0.27         | -0.12        | <b>-0.02</b> | 0.51         | <b>-0.01</b> | 1.00         |              |             |              |              |             |             |              |             |      |      |  |
| RISK | 6.00 | 1.19 | 0.92           | 0.75 | 0.86         | 0.15         | -0.21        | -0.16        | 0.41         | -0.14        | 0.29         | 1.00         |             |              |              |             |             |              |             |      |      |  |
| PCON | 5.49 | 1.53 | 0.94           | 0.70 | 0.83         | 0.13         | -0.19        | <b>-0.06</b> | 0.30         | -0.22        | 0.46         | 0.45         | 1.00        |              |              |             |             |              |             |      |      |  |
| DIST | 4.22 | 1.88 | 0.89           | 0.74 | 0.86         | -0.12        | <b>-0.09</b> | <b>0.03</b>  | <b>0.08</b>  | <b>-0.11</b> | <b>0.10</b>  | 0.16         | 0.49        | 1.00         |              |             |             |              |             |      |      |  |
| EXIT | 3.69 | 1.98 | 0.97           | 0.92 | 0.96         | -0.23        | <b>-0.10</b> | <b>0.03</b>  | <b>0.05</b>  | -0.17        | <b>0.05</b>  | 0.13         | 0.39        | 0.78         | 1.00         |             |             |              |             |      |      |  |
| NORM | 4.70 | 1.75 | 0.90           | 0.74 | 0.86         | 0.26         | 0.18         | 0.22         | 0.16         | 0.20         | <b>0.09</b>  | 0.13         | <b>0.09</b> | <b>-0.04</b> | <b>-0.03</b> | 1.00        |             |              |             |      |      |  |
| PEXP | 3.27 | 1.71 | 0.89           | 0.79 | 0.89         | <b>0.08</b>  | 0.18         | 0.25         | <b>0.08</b>  | 0.17         | <b>-0.01</b> | 0.14         | 0.31        | 0.37         | 0.36         | 0.14        | 1.00        |              |             |      |      |  |
| AGE  | 4.48 | 1.34 | .              | .    | .            | -0.25        | <b>-0.05</b> | -0.12        | 0.13         | <b>-0.07</b> | 0.13         | 0.14         | <b>0.00</b> | <b>-0.10</b> | <b>-0.05</b> | -0.13       | -0.25       | 1.00         |             |      |      |  |
| GEN  | 0.48 | 0.50 | .              | .    | .            | <b>-0.04</b> | <b>0.05</b>  | 0.17         | <b>-0.01</b> | <b>-0.07</b> | <b>-0.05</b> | <b>0.04</b>  | <b>0.09</b> | 0.17         | 0.20         | <b>0.02</b> | <b>0.05</b> | <b>0.02</b>  | 1.00        |      |      |  |
| INC  | 3.27 | 1.71 | .              | .    | .            | <b>0.04</b>  | <b>-0.05</b> | <b>0.01</b>  | <b>0.01</b>  | <b>0.06</b>  | <b>0.04</b>  | <b>-0.08</b> | <b>0.08</b> | 0.21         | <b>0.09</b>  | 0.17        | <b>0.03</b> | <b>-0.03</b> | <b>0.09</b> | 1.00 |      |  |
| EDU  | 4.72 | 1.67 | .              | .    | .            | <b>-0.04</b> | <b>-0.07</b> | <b>0.08</b>  | <b>-0.01</b> | <b>0.04</b>  | <b>-0.04</b> | <b>0.04</b>  | <b>0.09</b> | 0.15         | <b>0.09</b>  | 0.19        | <b>0.09</b> | -0.15        | <b>0.09</b> | 0.33 | 1.00 |  |

NOTES: Mean: construct mean; SD: construct standard deviation; CR ( $\rho$ C): composite reliability; AVE: average variance extracted; SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy threats; AGE: age; GEN: gender; INC: income; EDU: education. Correlations in **bold** are insignificant at  $p < 0.05$

## Structural Results

Before examining the structural results, the possibility of common method variance (CMV) was examined with an analysis employing two techniques. Cross-sectional studies measure all constructs using a single measurement method at a single time. As such, the use of a single method to collect data accounts for some, or even considerable variance in the observed variables and consequently in the estimation of the parameters of interest (Burton-Jones 2009). Two different methods, a marker variable technique and a common method factor (CMF) technique, were used to assess the influence of common method bias (Appendix F).

First, the marker variable technique (Lindell and Whitney 2001, Malhotra et al. 2006), and second the more rigorous common method factor approach (Podsakoff et al. 2003). Using the first method, the

path estimates significance increased for some relationships after accounting for CMV (second-smallest correlation,  $r=0.01$ ). However, except for a change from non-significance to significance occurred in a major hypothesized relation, that between secondary privacy control and distancing intentions ( $\beta=-0.08$ ,  $p\text{-value}=0.059$  to  $\beta=-0.08$ ,  $p\text{-value}=0.023$ ). Interestingly, the path estimates and the variance explained showed no variation in valence or size. In relation to the common method factor approach, a common method factor that reflects upon all the items in the model, including control variables, was included in the estimation algorithm. To control for common method variance without making the model unidentified, it was necessary to constrain this new construct's covariance with each and all other constructs to zero. The average sum of squared item loadings explained 59% of item variance. The measurement error accounted for 24%, and common method variance explained 17% which is similar or even lower than in comparable studies (e.g., Ma and Agarwal 2007, Ray et al. 2014). Overall, both methods show that the influence of common method variance in the proposed model is acceptable.

The structural relations in the proposed model were first assessed to test the hypotheses (Table 7). Another model including general privacy control instead of dual privacy controls helps understand the nature of prior conceptualizations within the nomology of the dual controls. Additionally, the saturated model considers the cross-effects from antecedents to mediators and from mediators to outcomes, and the overriding-effects from the agentic and cultural antecedents to outcomes. Allowing for such associations can challenge the proposed hypotheses and so provide direction in the quest to understand the real nature of privacy control.

**Table 7:** Proposed, Saturated, and General Privacy Control Structural Models

|      | Proposed Model |          |           |          |          | General Privacy Control Model |                |           |          | Saturated Model |           |                |          |          |          |          |           |
|------|----------------|----------|-----------|----------|----------|-------------------------------|----------------|-----------|----------|-----------------|-----------|----------------|----------|----------|----------|----------|-----------|
|      | R <sup>2</sup> | PPC      | SPC       | PCON     | DIST     | EXIT                          | R <sup>2</sup> | GPC       | PCON     | DIST            | EXIT      | R <sup>2</sup> | PPC      | SPC      | PCON     | DIST     | EXIT      |
| SEFF | 0.27 ***       | 0.13 *   |           |          | -0.19 ** | -0.28 ***                     | 0.18 **        |           |          | -0.22 ***       | -0.30 *** | 0.26 ***       | 0.16 **  | -0.06    |          | -0.16 ** | -0.24 *** |
| REG  | -0.22 **       | 0.49 *** |           |          |          |                               | 0.56 ***       |           |          |                 |           | -0.15 *        | 0.48 *** | -0.09    | 0.05     | 0.08     |           |
| UNA  | 0.47 ***       |          |           |          |          |                               | -0.09          |           |          |                 |           | 0.50 ***       | -0.16 ** | 0.10     | 0.07     | -0.04    |           |
| COL  |                | 0.31 *** |           |          |          |                               | 0.16 *         |           |          |                 |           | -0.11          | 0.36 *** | 0.01     | 0.04     | 0.08     |           |
| PPC  |                |          | 0.40 ***  | -0.01    |          |                               | GPC            | -0.22 *** | 0.13 *   | 0.08            |           |                |          | 0.36 *** | -0.15 *  | -0.13    |           |
| SPC  |                |          | -0.21 *** |          | -0.08    |                               |                |           |          |                 |           |                |          | -0.17 *  | 0.00     | -0.13    |           |
| RISK |                |          | 0.27 **   |          |          |                               | RISK           | 0.44 ***  |          |                 |           |                |          | 0.24 **  | 0.06     | 0.07     |           |
| PCON |                |          |           | 0.43 *** | 0.30 *** |                               | PCON           |           | 0.48 *** | 0.37 ***        |           |                |          |          | 0.49 *** | 0.37 *** |           |
| NORM |                |          |           | -0.11    | -0.04    |                               | NORM           |           | -0.12 *  | -0.06           |           |                |          |          | -0.14 *  | -0.06    |           |
| PEXP |                |          | 0.29 ***  | 0.23 *** | 0.29 *** |                               | PEXP           | 0.24 ***  | 0.21 **  | 0.25 ***        |           |                |          | 0.29 *** | 0.18 **  | 0.23 **  |           |
| AGE  | 0.13 *         | 0.03     | -0.03     | -0.09    | -0.06    |                               | AGE            | 0.07      | -0.01    | -0.10 *         | -0.07     | AGE            | 0.11     | 0.07     | -0.05    | -0.09    | -0.04     |
| GEN  | 0.01           | -0.13 ** | 0.05      | 0.10     | 0.14 **  |                               | GEN            | -0.09     | 0.04     | 0.10 *          | 0.14 **   | GEN            | -0.01    | -0.16 ** | 0.06     | 0.08     | 0.10 *    |
| INC  | 0.05           | 0.08     | 0.06      | 0.17 **  | 0.07     |                               | INC            | 0.04      | 0.10 *   | 0.16 **         | 0.06      | INC            | 0.02     | 0.08     | 0.06     | 0.18 *** | 0.09      |
| EDU  | -0.03          | 0.06     | 0.05      | 0.03     | 0.00     |                               | EDU            | 0.02      | 0.01     | 0.03            | 0.00      | EDU            | -0.02    | 0.05     | 0.03     | 0.03     | -0.01     |

Note: SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; GPC: general privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. Path significances: \*p < 0.05; \*\*p < 0.01; \*\*\*p < 0.001. Values in **bold** are the hypothesized relations of the proposed model.

Overall, the structural model showed satisfactory fit (Gefen et al. 2011, Hooper et al. 2008, Zhang et al. 2022). Fit metrics included  $\chi^2=1624.083$ ,  $df=897$ ,  $p\text{-value}<0.001$ ,  $\chi^2/df=1.811$ ,  $RMSEA=0.052$ ,  $SRMR=0.053$ ,  $CFI=0.931$ ,  $NNFI=0.922$ , and  $TLI=0.922$ . Factor models (i.e., CB-SEM) are often robust against multicollinearity (Trieu et al. 2022). However, this potential issue was examined by assessing each construct’s variance inflation factor (VIF). VIF values are multiple regression equations where, one at a time, an exogenous variable is regressed on all the rest exogenous variables affecting the same endogenous construct to obtain relevant R<sup>2</sup> values (O’Brien 2007). The highest VIF value was 1.47 (Appendix G), which is under the threshold of 5 typically suggested (Hair et al. 2011).

The non-hypothesized effects of the correlates show that past experience is a powerful explanation for increased information privacy concern, distancing, and exit across both views of privacy control. In contrast to general privacy control, the nomological network of the dual privacy controls show important differences. First, the culturally-informed personal values of uncertainty avoidance and collectivism differentially affect primary and secondary privacy control. However, only collectivism has a non-negligible effect on general privacy control. Moreover, uncertainty avoidance seems to have the opposite effects on this construct, in contrast to primary privacy control. Curiously, there is a negative

association between general privacy control and information privacy concern; resembling the association of secondary privacy control on concern.

Overall, most of the hypotheses are supported. Hypothesis 1 stating the positive association between uncertainty avoidance and primary privacy control is supported ( $\beta=0.47$ ,  $p\text{-value}>0.001$ ). Collectivism positively associates with secondary privacy control (H2:  $\beta=0.31$ ,  $p\text{-value}>0.001$ ). Moreover, although not hypothesized the agentic antecedents importantly contribute to the dual privacy control orientations. The antecedents explained 49% and 36% of the variance of secondary and primary privacy control, respectively. Hypothesis 3 and 4, which examined the effects of the dual privacy controls on information privacy concern were significant and opposite. While secondary privacy control lowered one's concerns over one's information privacy (H4:  $\beta=-0.23$ ,  $p\text{-value}>0.001$ ), a primary privacy control orientation exacerbates those concerns (H3:  $\beta=0.39$ ,  $p\text{-value}>0.001$ ). As expected, information privacy concern increases one's intentions to distancing and, furthermore, to exit social networking platforms.

Intriguingly, hypotheses 6 and 8 regarding the differential associations between secondary privacy control and exit intentions, and primary privacy control and distancing intentions were small and not significant ( $\beta=-0.08$ ,  $p\text{-value}>0.059$ ;  $\beta=-0.03$ ,  $p\text{-value}>0.600$ ). Moreover, instead of the expected negative association between primary privacy control and distancing intentions, this relation was unintuitively negative.

#### Suppression Effect

While the standardized regression weight for the relation between primary privacy control and distancing is negative ( $\beta=-0.03$ ), their correlation is positive though not very significant ( $r=0.10$ ,  $p\text{-value}=0.081$ ). This incoherence in their relations has the markings of a negative suppression effect (Paulhus et al. 2004). Suppression effects occur when there are two moderately correlated variables in the model and the suppressor variable suppresses criterion-irrelevant variance (Paulhus et al. 2004). To address this finding,

it is necessary to apply a correlation analysis (Thompson and Levine 1997). In our proposed model, primary privacy control and information privacy concern are both proposed to have effects on distancing. Further analysis of the suppression effects shows a moderate correlation between predictors ( $r=0.54$ ) and points to primary privacy control as the suppressor variable. The effects of information privacy concern on distancing are higher when primary privacy control is in the model, even though the correlation between primary privacy control and distancing is very low ( $r=0.10$ ). Given the potential for other suppression effects, the relationships between secondary privacy control, information privacy concern and exiting intentions is also examined but no suppression effects were found (see Appendix H).

#### Cross Associations and Overriding Associations

Looking at alternative explanations beyond the proposed model, the full model not only challenges the propositions regarding the differential effects of primary privacy control and secondary privacy control on outcomes, but also explores non-hypothesized associations. To limit chance findings of potential relationships in the exploration of the full model, a simply look at their statistical significance is not enough (Wasserstein and Lazar 2016). Rather, one has to focus on the new paths with coefficients close to, or higher than, the lowest absolute value of significant proposed paths in the model ( $\beta=0.13$ ) (Table 6). In this way, non-hypothesized paths are harder to reject than the least effective hypothesized path.

One such relation is SNS self-efficacy that even after including all overriding associations in the saturated model, its overriding effects on exit ( $\beta=-0.16$ ,  $p\text{-value}<0.01$ ) and distancing ( $\beta=-0.24$ ,  $p\text{-value}<0.001$ ) have only reduced in about 0.03 units, on average. These unexpected findings could be the result of the general measurement of SNS self-efficacy used in this study as it highlights that those users not confident in handling the full set of available features of Facebook are likely to leave without even thinking about privacy issues in the first place, but the powerful overriding effects of SNS self-efficacy cannot be discounted altogether. Additionally, the effect of SNS regulation on primary privacy control



remains negative but less significant and smaller ( $\beta=-0.15$ ,  $p\text{-value}<0.05$ ). Interestingly, this relation could be attributed to the makings of CMV earlier discussed. Moreover, the effects of the suppression effects found between primary privacy control and information privacy concern on distancing grow larger while the association between secondary privacy control, information privacy concern, and exit intentions also increase but without reaching significance. It is worth noting that this last relationship seems also to be affected by CMV. These chance findings could be statistical anomalies but are nonetheless worthy of discussion.

#### Common-Factor vs. Composite Perspectives

A composite nature of secondary and primary privacy control as capturing heterogenous strategies, as some have argued about secondary and primary control (Hall et al. 2006b), is tested because it could help relate this study findings with prior literature. Specifically, secondary privacy control is a lynchpin construct in this study as there is reason to believe it is a radically different perspective of privacy control. Rothbaum et al. (1982) also paid special attention to secondary control as a counter theory to the then prevailing concept of uncontrollability, and conceptualized it as having at least four interrelated aspects: interpretive, predictive, illusory, and vicarious. Several empirical operationalizations of secondary control have attempted to distinctly capture these four dimensions (e.g., Grootenhuis et al. 1996, Hall et al. 2006b, Seginer et al. 1993, Thompson et al. 1998). However, these studies did not find strong evidence that the aspects can be discriminated empirically (Seginer et al. 1993), nor could they distinguish the outcomes nomology of these four aspects (Grootenhuis and Last 2001).

Nonetheless, a re-examination of the nature of secondary privacy control as a composite construct is in place. Given the difficulties in modeling a single composite in an otherwise common factor model (Diamantopoulos 2011), the entire model was re-estimated with all constructs being composites and using Partial Least Squares Path Modeling (PLS-PM). In contrast to CB-SEM, the estimation of

composite models is based on weighted sums of items. This view does not assume the covariance between items in a composite to be explained by a common-factor and so composites are proxies of the concept investigated (Henseler et al. 2016). While research in information systems did not explicitly consider privacy control a composite, estimation of construct scores or the use employing PLS-PM suggest agreement in this direction (Benitez-Amado et al. 2017, Dinev and Hart 2004, Xu et. al 2012).

Secondary and primary privacy control were composed of all items on the onset; eight and five respectively, though only three and four proved usable for the common factor representation. The proposed model results of the composite view are shown in Table 8 (see Appendix I for more details). Compared to the common-factor model, the composite model effects did not change in valence or significance. This suggests that the choice of items for the common factor model was valid. When comparing the variance explained of both models, the common-factor view showed an increase of about 15% ( $R^2=0.05$ ), on average. The hypothesized antecedent-to-mediator paths varied 7% ( $\beta=0.02$ ), the mediation paths -6% ( $\beta=-0.01$ ), and the mediator- to-outcome paths in less than 2% ( $\beta<0.00$ ), on average and in relation to the common factor model.

**Table 8:** Structural Results of the Composite Proposed Model

|                       | PPC      | SPC      | PCON      | DIST     | EXIT      |
|-----------------------|----------|----------|-----------|----------|-----------|
| <i>R</i> <sup>2</sup> | 0.26     | 0.41     | 0.43      | 0.35     | 0.32      |
| SEFF                  | 0.23 *** | 0.21 *** |           | -0.14 *  | -0.23 *** |
| REG                   | -0.16 ** | 0.45 *** |           |          |           |
| UNA                   | 0.41 *** |          |           |          |           |
| COL                   |          | 0.24 *** |           |          |           |
| PPC                   |          |          | 0.36 ***  | -0.09    |           |
| SPC                   |          |          | -0.17 *** |          | -0.07     |
| RISK                  |          |          | 0.27 ***  |          |           |
| PCON                  |          |          |           | 0.46 *** | 0.32 ***  |
| NORM                  |          |          |           | -0.12 *  | -0.08     |
| PEXP                  |          |          | 0.21 ***  | 0.20 *** | 0.24 ***  |
| AGE                   | 0.11     | 0.06     | -0.03     | -0.08    | -0.06     |
| GEN                   | -0.02    | -0.13 ** | 0.05      | 0.09     | 0.14 **   |
| INC                   | 0.04     | 0.08     | 0.06      | 0.16 **  | 0.06      |
| EDU                   | -0.01    | 0.08     | 0.04      | 0.03     | 0.00      |

NOTES: SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; GPC: general privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. Path significances: \*p < 0.05; \*\*p < 0.01; \*\*\*p < 0.001.

However, there were some changes in the correlates of the endogenous constructs, specifically, the association of age on primary privacy control lost significance, and the association between SNS normative benefits and exit intentions became significant. However, none of these relations drastically changed:  $\beta=-0.02$  and  $\beta=+0.01$  for the first and the second, respectively. Once again, the relationship between primary privacy control and distancing is the result of suppression. We conclude that a composite measurement of secondary privacy control has no discernable advantages over a common-factor perspective.

## **Discussion**

After a conceptual review of secondary control in other fields of study, this notion was adapted to the privacy domain to reconcile prior findings in the relation between control and concern and to advance our understanding of the origins and outcomes of privacy control. Social networking platforms are among the most suitable environments for social interactions. Specifically, the flexibility in the ways users are allowed to construct and modify the impression about themselves to others, the culturally diverse population, and the ongoing privacy threats to users made of Facebook an ideal environment to empirically test the nomology of dual privacy controls.

Importantly, this study reports that secondary privacy control and primary have opposing effects on information privacy concern. Generally, the dual privacy controls are associated with a sense of agency, but the culturally-informed personal values differentially affect one's sense of privacy control. A secondary privacy control orientation comes about uniquely from a saliency in the value of collectivism and primary privacy control from uncertainty avoidance. Intriguingly, the findings of this study suggest striking empirical similarity between secondary privacy control and general privacy control, in contrast to their opposite conceptual representations of control. Additionally, the challenges in finding the effect of the dual privacy controls on outcomes are considered. Overall, there are several theoretical and practical ramifications worth discussing.

## Theoretical Contributions

The ultimate theoretical contribution of this study is the conception of privacy control as a dual process. Secondary privacy control, or the understanding of control as a form of acceptance and adaptation to privacy threats in which users, out of their lack of ability, need for time or choice to follow the preferences of one's social network, seem not protect their privacy. In a contrasting stance to secondary privacy control, this study includes the most common meaning of control into primary privacy control, or personally choosing to achieve privacy protection by using one's ability, refining it through permanent learning, or heavily relying on one's choice.

The reconceptualization of privacy control as two distinct concepts—secondary and primary privacy control—facilitates the cohesive reconciliation of mixed findings in the information systems literature (H4 and H3). The raise of a natural resistance to keep using social networking services versus the unrestricted use of these platforms also reflect this dual phenomenon (Edison Research 2019, 2022, MarketingLand 2019). More specifically, secondary privacy control now explains ( $\beta=-0.23$ ,  $p$ -value $<0.001$ ) why privacy control is often associated with lowered information privacy concern in the literature (Dinev and Hart 2004, Xu et al. 2012). In contrast, primary privacy control explains ( $\beta=0.39$ ,  $p$ -value $<0.001$ ) why perceptions of privacy control are associated with more privacy concern in the literature (Wang et al. 2016, Miltgen and Peyrad-Guillard 2014). These associations remain stable even after the inclusion of cross- and over-riding effects which is a signal of their explanatory strength.

Prior studies in the information privacy literature identified agentic roots of privacy control perceptions, and this study replicates these relationships with general privacy control and largely confirm their relationship with the dual privacy controls. However, we note that SNS regulation had a significantly negative association on primary privacy control in the proposed and saturated models. It is surmised that users with faith in government and industry regulations do not, by and large, see a need to adopt a hypervigilant primary stance on managing their privacy. Instead, their sense of privacy control

is of a mixed nature: primary in their being alert to changes in the privacy climate, although they defer to higher authorities to take the first step; and secondary in that during this wait-and-see period, they rely on the hope that desirable privacy outcomes will prevail.

Beyond agency, and based on the extensive literature on dual controls, the newly introduced culturally informed values are important determinants of dual privacy controls (H2 and H1). At their essence, both uncertainty avoidance and collectivism reflect people's culturally informed, but ultimately personal, choices of how to deal with uncertainty. People who hang onto the value of collectivism are inclined to underplay personal threats and adopt the long-term view of secondary privacy control. They often imitate what their family or closer group of peers do in their online social interaction and so follow their group's goals. In contrast, people who value uncertainty avoidance seek to deal immediately and directly with privacy threats through primary privacy control. These clear differences in the relationship between these two values and dual privacy controls again underscore the key differences between secondary and primary control. Value-based factors such as collectivism and uncertainty avoidance are seen elsewhere in information systems literature (Hwang 2005, Srite and Karahanna 2006), and this study contributes by demonstrating that they play an important role in privacy matters as well. This study is also in accord with the broader dual controls literature in calling for secondary approaches to managing privacy control to not be seen simply as passive or maladaptive. Instead, these secondary approaches should be recognized as a healthy, value-based preference and alternative to acting immediately and possibly futilely. By adopting these secondary approaches, some users thus avoid surrendering and losing hope of better outcomes.

The associations between information privacy concern and outcomes are positive and significant (H7 and H5), whereas the results suggest that the dual privacy controls do not directly impact protective intentions (H8 and H6). Specifically, the association between primary privacy control and distancing intentions is blurred by the makings of suppression effects (see "Suppression Effects"). And even when

those with a secondary privacy control orientation display lowered exit intentions regardless of their concern, this association is low and insignificant ( $\beta=-0.08$ ,  $p\text{-value}=0.600$ ). And although our observations do not confirm enhanced distancing intentions among primary privacy control-oriented users in our context, it would not be easy to disconfirm this association in other contexts or upon behaviors. Thus, researchers investigating users in contexts in which privacy issues are salient should not disregard the potential relationship between privacy control orientations and key outcomes.

### **Managerial Contributions**

Managers, designers of user experience, and policy makers should consider the dual nature of privacy control in social networking services when designing interventions. Service providers are increasingly giving users more privacy management settings and tools to enhance their privacy control. Although these tools could benefit users with primary privacy control orientations who are inclined to use them, these privacy tools may at best have a palliative effect on users oriented toward secondary privacy control who are not inclined to investigate or alter their environment. Counter-intuitively, providing more privacy management settings might only further increase the vigilance and concern of users under primary privacy control while lowering the concern of users who are more inclined toward secondary privacy control despite the unlikelihood they would use these tools to secure their privacy. Thus, rather than assuming that privacy settings and tools are enough, service providers might better protect their users by reducing privacy exposure more directly through conservative privacy defaults and design, and rely less on all users making sense of a dizzying array of privacy options.

Practitioners should also note that the roots of the dual privacy controls are both agentic and value-based. Although our study examined several decision-making factors, it is very possible a service provider is operating in a market in which one of these factors is more prevalent among users. For example, a firm could potentially operate in a largely collectivist culture and so expect greater secondary privacy control orientations. Conversely, a domain-specific group of tech savvy users might have the

abilities and inclination to adopt a more primary privacy control orientation. An understanding of the psychological makeup of their user base should guide providers in how they differentially help users manage privacy issues and so reduce protective intentions that could possibly limit the vitality of their network. Moreover, in an age of increased data, service providers could even attain the personalization of privacy protective measures.

Overall, this reconceptualization of privacy control yielded important support from this empirical study of Facebook users. However, the last set of results regarding the relation between dual privacy controls and outcomes has left questions still unresolved. Perhaps the major one relates to whether behaviors, in contrast to intentions, are affected by the dual privacy controls, thus, motivating the second study in this manuscript.



## Chapter 4: Study 2

The relation between intentions and behaviors is blurry at best, as Sheeran (2011) discovered in a meta-analysis of meta-analyses. Some studies even found that measuring intentions can change subsequent behaviors (Morwitz and Fitzsimons 2004). However, we could not measure distancing and exit behaviors in a cross-sectional way as these behaviors can only be observed over long periods of time. Moreover, some behaviors like exit can be reversed later if a user rejoins. Thus, this second study is complementary to Study 1 in that it takes advantage of a privacy-related event that naturally induce privacy protection of smartphone users in social networking services by raising awareness about how companies collect their data and how users can protect themselves by simply upgrading their mobile devices. It is also more causal in nature as participants provide data about their privacy perceptions before the privacy-related event and their upgrading behavior two months after the event.

### **Context: Smartphone Social Networking Services Apps**

The invention of the telegraph, and every information technology developed since then, has afforded a steady increase in the amount and speed of information shared with others (Jepsen 2018). Parallely, the nature of privacy challenges present with old technologies have not only changed but also increased with more modern devices (Freeman 2012). Intelligent technologies such as the most widely used smartphones are at the closest end of this chain and so represent the richest and fastest point for the collection of one's personal and transactional information. In truth, smartphones are so embedded in people's life that they use it to achieve a variety of goals, from simply navigating the internet to even finding one's life partner (Jung et al. 2019).

More broadly, except from some parts of the world, the adoption of smartphones is above the 74% of the total of mobile connections in 2021 and it is expected to increase to above 82% by 2025 (O'Dea 2022). The most interesting and profitable feature of smartphone devices is their capability to host apps – software programs limited to perform a specific function. For companies, apps are the means



through which companies offer their services, collect data, and communicate directly with users. For users, apps are the most common way to access one's favorite activities. They allowed companies and researchers to get insights from people's everyday social behavior (Raento et al. 2009). Offering an app is a common strategy companies use to increase their market share in their domain of influence and so the apps market keeps growing (Technavio 2022).

One of the most common activities on smartphones is the use of social networking services. Facebook, for example, maintains the Facebook App which, thanks to the smartphones' convenient size, grants immediate access to one's social network platform. As mobile applications are the mobile version of the original website platforms, their amount of data collected and the privacy breaches extend to both realms. Thus, privacy issues in mobile social networking apps have also been of major concern. Recent reports on the smartphone market show that the collection and use of users' data through mobile applications, especially by social networking platforms such as Facebook has been deeply criticized (Confessore and Kang 2018). Interestingly, motivated by the huge amount of data specifically collected by Facebook through their mobile app (Clover 2020), Apple, Inc, a smartphone producing company, has slowly implemented a series of measures to counteract privacy breaches through their app store (Apple 2022a). In a first attempt to raise privacy awareness among users, Apple, Inc has launched a feature in their app store called App Privacy that informs users about the app's privacy practices before they download an app from the App store (Apple 2022b).

### **The App Tracking Transparency Feature - ATT**

Every mobile user is assigned an identifier for advertisements (IDFA) number that not only allows apps to track users' activity and provide personalized advertisements to them, but, more importantly, depersonalize users. Data collection regulations are not new to Apple's privacy policy. Before the enforcement of the ATT feature, companies followed the Limit Ad Tracking feature (LAT) through which the user's IDFA was transformed into zeros if users chose not to share their data (Specktor 2021).

However, the depersonalized IDFA was still accessible to companies that did not always abide by their users' choice. Thus, a subsequent step in this stream of privacy protection implementations was the release of Apple's App Tracking Transparency feature – ATT. A feature that since the release of iOS 14.5 effectively enforces app developers to include a function asking for their users' consent to the collection and use of their data across third party apps for advertising and data sharing with brokers (Campbell 2021). This release was publicly stipulated to target the Facebook app's information overreach (Clover 2020).

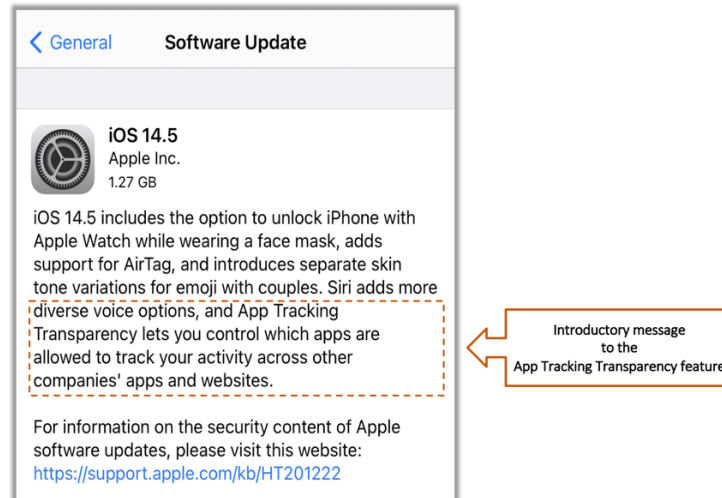
Fundamentally, the ATT feature transfers the decision to smartphone users to allow a particular app to track their activity on their app by showing them a permission-request prompt message. The prompt message only appears to those users who upgrade their iPhones to iOS 14.5 and it is shown at any time after users launch the application (Apple 2022c). If iPhone users had their LAT toggled off prior to upgrading to iOS 14.5 or after manually upgrading switch off the ATT privacy setting: “*Allow Apps to Request to Track*”, they do not receive the prompt message (Specktor 2021). Consequently, those not receiving the message automatically deny all apps to track them. If after upgrading to iOS 14.5, iPhone users toggle the ATT feature on, they receive the prompt message after launching the app and at any time during their use (Ha 2021). However, it is still possible that users have set their settings to not automatically update apps whenever the iOS system is upgraded, in which case, users do not receive the prompt message either.

Although the ATT feature was already released with an upgrade of iOS 14.0, many technical and social challenges including Facebook's complaints (Nikas and Isaac 2021) delayed its implementation. It was not early than the end of April 2021 that the ATT feature was finally released within the iOS 14.5 upgrade to the public as the major change in Apple's privacy policy.

## Exogenous Variation from a Privacy-Related Event

Apple.Inc's serious initiative to privacy protection effectively puts privacy control on the hand of iPhone users. Such important step, changes the way organizations and people engage in information transactions regarding privacy. Thus, Apple.Inc has released several short videos intended to enhance the awareness of this upgrade among their users (Bhatia 2021, Miller 2021). The ATT feature is the most important technical aspect of this new privacy policy. However, it is the impact of the message, accompanying the ATT introduction, on iPhone users, the main focus of Study 2.

Apple.Inc regularly sends, alongside their iOS system upgrades, highlights listing or explaining the latest changes in functionality of their devices. The iOS 14.5 version for iPhone users was released on April 27<sup>th</sup> (Ha 2021). For this upgrade specifically, the highlights included the ATT feature (Figure 2) which occupied about half the space dedicated for the highlights, reflecting the importance of this message. Moreover, the message was written in a *personal* tone and with an emphasis on *privacy control*. Such strategic framing explaining the intend of including the ATT feature in the new upgrade was likely to have a motivational effect on users to take control of their most valuable information. Consequently, the message acts as a reminder to users that they can execute their right to disclose information about themselves (Dinev and Hart 2004). As a result, the declaration sets the grounds for a quasi-natural experiment in which users are given the means to effectively exert control over their privacy. This eye-opening event is used to identity the causal effects of users' dual privacy controls on protective behaviors; specifically, on upgrading behavior.



**Figure 2:** Software Update Message on iPhone

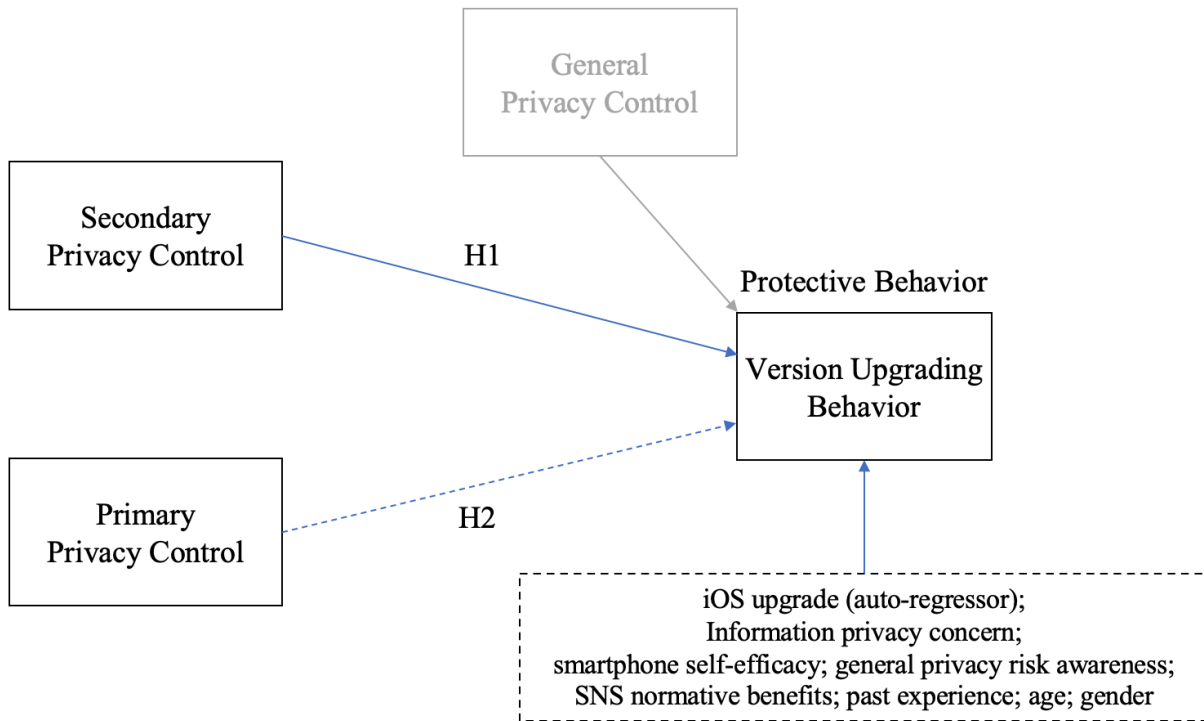
## Theory Development

The framework of Study 1 has facilitated our understanding of the complex ways in which social network users attempt to gain control, or a feel of control, over their privacy. Moreover, Study 1 allowed us to discover the culturally-informed personal value antecedents of both, secondary and primary privacy control. However, even when Study 1 displayed the arguments for the association between the dual controls and protective intentions, the effects of suppression (Paulhus et al. 2004) deterred these findings. In Study 2, the idea that intentions accounts for only a small portion of the variance explained by behaviors in the privacy context is entertained (Bélanger and Crossler 2019, Sheeran 2011). As a consequence, the main goal of Study 2 is to gain further understanding of the effects of the dual privacy controls on protective behaviors, in contrast to intentions, in the context of smartphone social networking service apps. Moreover, by using a lagged-design, Study 2 reduces the impact of common method bias.

## Theoretical Framework

The following complementary framework (Figure 3) is focused on the effects of the secondary and primary privacy control on smartphone users upgrading, a form of privacy protective behavior. This framework also includes the effects of the well-known information privacy concern and the potential

autoregressive effect of iOS upgrading as an explanation for users keeping up with smartphone updates. Additionally, smartphone self-efficacy and other correlates are also measured as directly affecting one's upgrading behavior.



**Notes:** Negative associations use dashed lines; Correlates are in dashed boxes, and are positioned below the constructs they are associated with.

**Figure 3:** Conceptual Framework

### Dual Privacy Controls and Upgrading Behavior

In contrast to examining distancing and exit behaviors in the social networking app context, the external event explained above constrain the outcome to the iOS 14.5 version upgrading. In the face of the awareness generated among users regarding the implementation of the ATT feature and its benefits in giving control back to users, not upgrading can be interpreted as the adaptation to privacy threatening situations. Adaptation that often happens in correspondence to their lack of ability as individuals, but powerful as part of their more powerful social group that decides the adequate time to act on privacy protection. Secondary control strategies are attempts to resist challenging situations and not giving up

faith to adversity (Thompson et al. 2020). The internalization of the challenging situation enables secondary control-oriented individuals to match the environment exigencies (Rothbaum et al. 1982). Similarly, secondary privacy control-oriented individuals, dependent on their group's will, internalize the unstoppable nature of privacy issues and so avoid fighting against them.

*H1: Secondary privacy control negatively affect smartphone upgrading behavior*

Contrary, the implementation of new means to further protect one's privacy with the release of the iOS 14.5, represents another opportunity to individuals with a primary privacy control-orientation to explore meaningful ways to shield their private information from others. A primary control orientation entails the permanent, and even incessant, search for changing the environment to fulfil one's needs (Thompson et al. 2020) reflected in a proactive behavior (Hall et al. 2006a) and the alertness to new opportunities (Yu 2001). Thus, upgrading represents a display of one's primary privacy control orientation.

*H2: Primary privacy control positively affect smartphone upgrading behavior*

Additionally, the model also considers the effects of one's willingness to upgrade their device to keep up-to-day with technological advances, information privacy concern, smartphone self-efficacy, general privacy risk awareness, SNS normative benefits, past experience with privacy issues, age and gender, all as correlates of upgrading behavior.

## **Empirical Validation of Study 2**

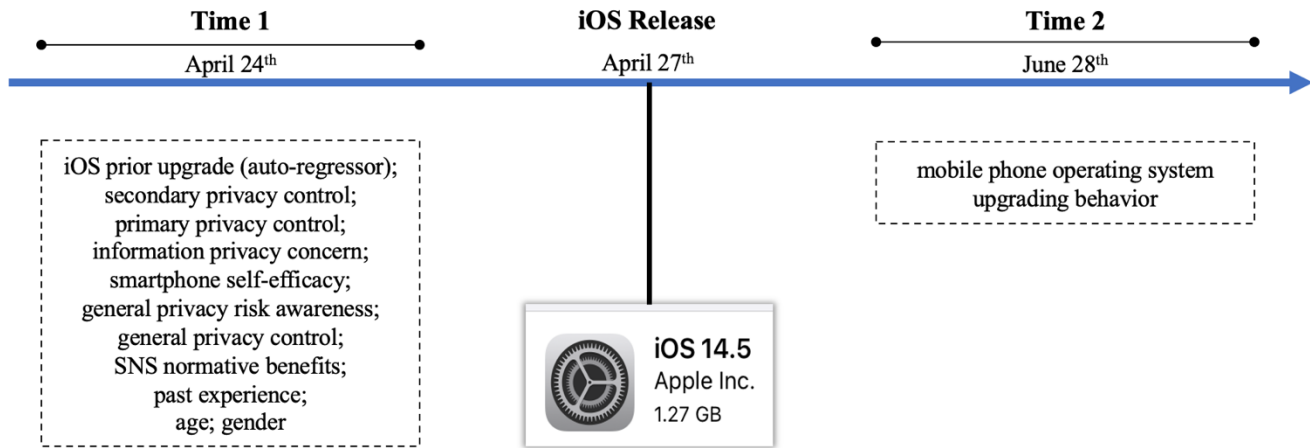
### **Study Design and Deployment**

The introduction of the App Tracking Transparency feature within this the iOS 14.5 upgrade is ideal to study privacy behaviors as it motivates users to think about the value of their privacy. This major event in the information privacy domain influences all iPhone users. Additionally, researchers cannot choose when or how the exogenous event will take place. Moreover, iOS upgrading is not mandatory among users allowing them to decide on this matter (Huang et al. 2021). All these characteristics set the necessary conditions for a quasi-natural experiment.

In this second study, the main concern is with the reasons motivating smartphone users to upgrade their iOS system. Specifically, whether the dual privacy controls, proposed in Study 1, explain users' upgrading behavior. Following recent study design advances in the information systems literature (Liu et al. 2020), the release of the iOS 14.5 upgrade is used as an exogenous event believed to have influenced the way smartphone users interact with Facebook on their smartphone devices as there is a close relation between the iOS 14.5 upgrade and the possibility to protect one's privacy.

### Data Collection

Through a contracted market research company, the questionnaires were sent to survey individuals at two points in time. Data were collected at two points in time and only from randomly chosen participants in North America who were iPhones users and had the Facebook app installed in their phones (Figure 4). None of the participants in the first or second wave were part of the sample of Study 1. Additionally, participants were informed about the anonymity of their responses, and that their responses would be used in aggregate, and solely for research purposes. The first data collection used Surveycake.com and happened from April 24th to May 6<sup>th</sup> of 2021. Although this period overlaps with the release of the iOS upgrade, April 27th, whether users upgraded was confirmed by offering guidelines to participants to provide their iOS version at the time of the survey. Moreover, the adoption rate of past iOS versions was only about 5-10% worldwide during the first 10 days of release (Ha 2021). Thus, the likelihood of the participants upgrading their iOS system to the 14.5 software version at the time of the survey was low. In this first wave, there was a total of 746 answers out of 20000 sent requests, a 3.73% response rate. This first questionnaire was expected to last 15 minutes, and for the most part asked for perceptions of the dual privacy controls, smartphone self-efficacy, information privacy concern and constructs included as correlates coming from Study 1 (Appendix J).



**Figure 4:** Lagged Quasi-Natural Experimental Design

After six weeks and a half, the first-wave list of respondents was used to choose only those that fulfilled the criteria, Facebook users on iPhone, and sent back to the marketing company for a follow-up questionnaire to a total of 397 participants. Again, the waiting time prior to closing the survey was based on past iOS adoption experiences (Balasubramanian 2021). This follow-up questionnaire was deployed on SurveyMoonbear.heroapp.com and was substantially shorter, 8 minutes: It mainly included upgrading behavior (see Appendix K for the full list of items). Data was collected data from June 28th to July 13th of 2021. A first reminder was sent to 166 participants on June 30<sup>th</sup> and a second to 111 participants on July 6th. Each time a reminder was released, it was only released to those who did not answer the survey. Only when both waves of data were collected for this two-wave lagged design, the participants received a small reward for their participation.

## Definition of Variables

### Criterion and Auto-Regressor

The dependent variable was measured in the second wave and it is a behavioral outcome. Participants were specifically asked to access their iPhone settings and report their iOS version: “*On the same settings page (‘Settings’ > ‘General’ > ‘About’) tell us your ‘Software Version’*”. In this way, it was possible to



know if they upgraded their iOS systems to 14.5 or any other version above. Additionally, the auto-regressor controlled for trait-like upgrading behavior of participants. This variable was obtained in the first wave as respondents had to answer: *“On your iPhone, please access ‘Settings’ > ‘General’ > ‘About’ and tell us which of the following options matches the information under ‘Software Version’.”* We then provided them the following options: *“13.7 or below, 14.0~14.4, and 14.4 or above.”* Both these variables were transformed to their binary forms.

Given that Apple.Inc releases not only major versions as 14.4 but also subversions as 14.4.1, the option corresponding to “14.0~14.4” in the auto-regressor did not include subversion while the option “14.4 or above” included subversions since 14.5 was not released by the time of this data collection. Consequently, to run a suitable analysis, the dependent and auto-regressor variables were transformed by assigning each individual to an upgrading group with the value of “1” and to a not upgrading group - “0”. For example, for the criterion variable those who upgraded reported a value of 14.5 or above and so they were placed in the upgrading group. For the auto-regressor, those who chose either 13.7 or below, or 14.0~14.4, were assigned the value of “0” and so they were accounted within the not upgrading group.

The inclusion of the auto-regressor plays an important role as it accounts for the general explanation of users upgrading their iOS system because they always do. This explanation is also understood as users’ willingness to go further in their intentions to be up-to-day with smartphone technology advances. Thus, if the surveyed users constantly upgrade their iOS system and yet the variables of interest have a salient effect, it can be concluded that the external event has had an impact on how users perceive their chances to control their privacy in a primary or secondary form.

## Predictors

The independent constructs of this study were measured in the first wave. The same items used to measure secondary privacy control, primary privacy control, general privacy control, information privacy

concern, and general privacy risk awareness (see “Measurement Items” on p. 28) in Study 1 were used in this study. While a context modification was necessary to match with the Facebook app in iPhones, items corresponding to smartphone self-efficacy also come from SNS self-efficacy in Study 1. The reason to use the same items as in Study 1 was that the final goal of Study 2 is to unveil the effects of the dual privacy controls on behaviors.

#### Correlates

Potential explanations or effects on upgrading to iOS 14.5 were ruled out by fixing the effect of constructs that could potentially motivate users to upgrade their iOS system. Among them, the effects of SNS normative benefits and past experience with privacy issues. Additionally, demographic characteristics such as the gender and age of participants were also considered.

#### Data Analysis

There were 299 complete and matched responses for both waves: A response rate of 75.3%. However, after scrutinizing the data for duplicate or monotonic responses, a working sample of 285 participants was left. In this sample, 59.6% were female and 40.4% male. Respondents were mostly within the age range of 25-34 years old. The sample demographic characteristics fairly reflected the population of interest. About 98.5% of Facebook users interact through Facebook on their mobile device (Statista 2022b), and Apple.Inc, in average, has the largest market share (Statista 2021). Moreover, the majority of users are males between 25 to 34 years old. Following recent literature on information systems adoption applying logistic regression analysis (Chen et al. 2020, Steinhouser et al. 2020), a comprehensive summary of variables and their description appear in Table 9. Broadly, there are one dependent variable, five predictor constructs, one autoregressive variable, and four correlates.

**Table 9:** Data Descriptives

|                                | Short Name | Description                                 | Mean | Sd   | Min. | Max. |
|--------------------------------|------------|---|------|------|------|------|
| Upgrade to iOS 14.5            | PUPG       | 1: Upgraded to iOS 14.5 or above            | 0.79 | 0.41 | 0    | 1    |
| Upgrade iOS (autoregressor)    | iOSupg     | 1: Upgraded iOS                             | 0.65 | 0.48 | 0    | 1    |
| Secondary Privacy Control      | SPC        | Average of 3-item variables                 | 4.00 | 1.36 | 1    | 7    |
| Primary Privacy Control        | PPC        | Average of 4-item variables                 | 5.84 | 0.94 | 1    | 7    |
| General Privacy Control        | GPC        | Average of 3-item variables                 | 4.03 | 1.42 | 1    | 7    |
| Information Privacy Concern    | PCON       | Average of 7-item variables                 | 5.36 | 1.28 | 1    | 7    |
| Smartphone Self-efficacy       | iSEFF      | Average of 4-item variables                 | 6.06 | 0.90 | 1    | 7    |
| General Privacy Risk Awareness | GPR        | Average of 4-item variables                 | 5.90 | 1.07 | 2    | 7    |
| SNS Normative Benefits         | NORM       | Average of 2-item variables                 | 4.89 | 1.37 | 1    | 7    |
| Past Experience                | PEXP       | Average of 2-item variables                 | 3.56 | 1.56 | 1    | 7    |
| Age                            | AGE        | <18, 18-24, 25-34, 35-44, 45-54, 55-64, ≥65 | 3.94 | 1.92 | 3    | 7    |
| Gender                         | GEN        | 1: Female and 2: Male                       | 1.39 | 0.48 | 1    | 2    |

NOTES: Items following a 7-pt scale used the values: 1 strongly disagree, 7 strongly agree, and 4 neutral.

### Logistic Regression Model

As the dependent variable is binary, multiple logistic regression analysis is the most suitable statistical technique. The focus is on the effects of secondary and primary privacy control on the adoption iOS 14.5 version. Thus, the most important regression coefficients in Equation 1 are  $\beta_2$  and  $\beta_3$ . An alternative model examining the effect of general privacy control on upgrading to iOS 14.5, also called the general privacy control model, replaces secondary and primary privacy control with the general privacy control construct and it corresponds to the way researchers currently think of privacy control (Equation 2). Below the equations to be tested:

$$PUPG_i = \beta_0 + \beta_1 * iOSupg + \beta_2 * SPC + \beta_3 * PPC + \beta_4 * PCON + \beta_x * Correlates + \varepsilon_i \quad \dots (1)$$

$$PUPG_i = \beta_0 + \beta_1 * iOSupg + \beta_2 * GPC + \beta_3 * PCON + \beta_x * Correlates + \varepsilon_i \quad \dots (2)$$

### Results

Logistic regression analysis is a commonly used method when outcomes are dichotomous (Chen et al 2020, Steinhouser et al. 2020). Hypothesis 1 is supported. Secondary privacy control has a significant negative effect on the individual's likelihood of upgrading their iOS system to 14.5 version (Table 10). Specifically, secondary privacy control-oriented individuals are 0.71 less likely to upgrade their iPhone devices (*odds-ratio*=0.71, *p-value*<0.05). However, H2 is not supported. Although the effect of primary

privacy control on upgrading behavior is not significant, it is still positive, meaning that primary privacy control-oriented individuals are 0.08 more likely to upgrade their iPhone devices (*odds-ratio*=1.08, *p-value*=0.730). Past experience with privacy issues is a powerful explanation for users to upgrade their iOS system (*odds-ratio*=1.38, *p-value*<0.01). Surprisingly, information privacy concern has a negative but insignificant effect on upgrading.

**Table 10:** Logistic Regression Dual Privacy Controls and General Privacy Control Models

|   | Outcome = PUPG Odds Ratio (RSE) |                               |
|---|---------------------------------|-------------------------------|
|   | Proposed Model                  | General Privacy Control Model |
| Intercept                               | 49.50 (2.49)                    | 24.24 (2.32)                  |
| Upgrade iOS (auto-regressor)            | 6.91*** (0.36)                  | 6.63*** (0.36)                |
| Secondary Privacy Control (SPC)         | 0.71* (0.22)                    |                               |
| Primary Privacy Control (PPC)           | 1.08 (0.16)                     |                               |
| Information Privacy Concern (PCON)      | 0.73 (0.19)                     | 0.76 (0.20)                   |
| General Privacy Control (GPC)           |                                 | 0.79 (0.17)                   |
| <b>Correlates</b>                       |                                 |                               |
| Smartphone Self-efficacy (iSEFF)        | 0.71 (0.20)                     | 0.79 (0.19)                   |
| General Privacy Risk Awareness (RISK)   | 0.98 (0.20)                     | 1.01 (0.19)                   |
| SNS Normative Benefits (NORM)           | 1.12 (0.14)                     | 1.07 (0.14)                   |
| Past Experience (EXP)                   | 1.38* (0.12)                    | 1.31* (0.12)                  |
| Age (AGE)                               | 1.08 (0.16)                     | 1.12 (0.16)                   |
| Gender (GEN)                            | 0.57 (0.36)                     | 0.60 (0.34)                   |
| <i>Wald Test Statistic</i> ( $\chi^2$ ) | 45.7 ( <i>df</i> =10)           | 74.9 ( <i>df</i> =10)         |
| <i>p-value</i>                          | 0.000                           | 0.000                         |
| <i>Observations</i>                     | 285                             | 285                           |

**NOTES:** \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$ . Robust standard errors are in parentheses (RSE) to avoid the influence of heteroskedasticity. Odds ratios higher than 1 indicate a positive effect on the outcome variable, and vice versa.

The alternative model shows no significant effects, except for the relation between past experience and upgrading (*odds ratio*=1.31, *p-value*<0.05). However, the effect of general privacy control on upgrading is negative (*odds ratio*=0.79, *p-value*=0.184), and not positive as the theoretical notion suggests. This finding further supports the notion that privacy control, in the information systems literature, has been seen more as adapting and adjusting oneself to privacy issues, and less as one's ability to protect from privacy threats. Moreover, this model has a higher Walt test statistic, which in comparison with the proposed model corresponds to a poorer fit.

## **Discussion**

Apple.Inc's release of a function that returns control to their iPhone users allowed for a quasi-natural experiment in which the message accompanying the release of iOS version 14.5 containing the ATT feature acted as a reminder to users regarding the protection of their privacy. Social network apps facilitate the reaching of one's closest social circle. In a similar way to social networking on the web, SNS apps afford great flexibility in the ways users build their reputation to others. More important to this study, these platforms are not free from privacy threats, all the opposite, they are perhaps the principal source of threat to one's privacy as our smartphones tap into a wide range of activities in our daily life. Study 2 is a complement to Study 1. Study 1 has shown some unavoidable difficulties in the effects of the dual privacy controls on intentions. We could not measure distancing and exit behaviors in a cross-sectional way as these behaviors can only be observed over long periods of time. Moreover, some behaviors like exit can be reversed later if a user rejoins. Thus, overcoming these challenges required measuring actual behaviors at different times. Moreover, the nature of cross-sectional studies is prohibitive as causal claims can be harshly questioned. This quasi-natural experiment contributes to theory and management.

## **Theoretical Contribution**

This study shows that taking a secondary stance on control can also limit one's adoption of positive outcomes. Secondary control is best known for its positive impact on people's reluctance to relinquish control (Rothbaum et al. 1982). While accepting and adjusting to privacy threats bring peace-of-mind to users and affords them a wide range of possibilities in their interactions, the internalization of current privacy circumstances as the new normal also blinds them from seizing opportunities that require their minimal effort to better protect their privacy. Intriguingly, gaining any type of control seem to have a negative side. Attempting to change the environment, a primary control-orientation, drags people to believe they have control over objectively uncontrollable outcomes (Langer et al. 1977), and attempting

to change the self, a secondary privacy control-orientation, precludes people from inverting efforts in any available attempt to personally improve their privacy condition. The implications of this discovery could inspire new research in the information systems literature as well as in the psychology literature.

### **Managerial Contribution**

Individuals who delay the adoption of organizational implementations are likely to produce disruptions in the platform's operating systems and even force a change in their business model. Interestingly, it was found that secondary privacy control-oriented individuals do not upgrade their mobile phone operating system, even when such action was beneficial to their privacy. These users have come to understand that their goal is to accept and adapt to circumstances as they come to exist in the privacy domain. Thus, service providers can be better off if they consider the dual nature of privacy control and device strategies that motivate secondary privacy control-oriented users into accepting newly released implementations.



## Chapter 5: Alternative Views of Secondary Privacy Control

Although secondary control has now been developed and applied as a counterpart of primary control for almost three decades, it is worth noting other competing perspectives that offer similar explanations. Specifically, this chapter includes a through comparison of secondary privacy control with *privacy coping*, *privacy accommodation*, and *primary appraisal*.

### Literature Review of Alternative Concepts

#### Secondary Privacy Control and Privacy Escape-Avoidance Coping

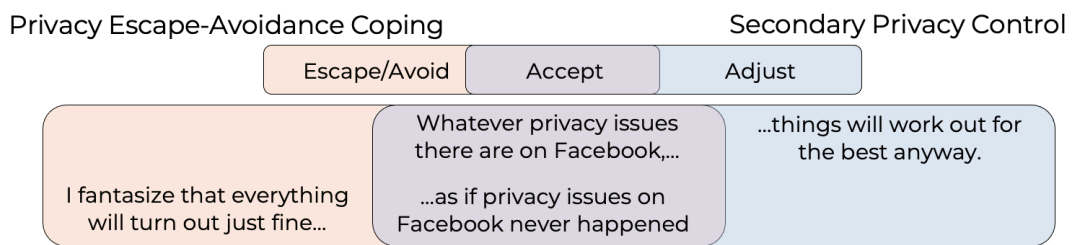
There are theoretical explanations that can help disentangle secondary privacy control from privacy coping. The most relevant coping framework (Lazarus and Folkman 1984, p.171) broadly defines control as an overarching concept consisting of appraisal and coping. These authors write: “*disaggregating the concept of control with respect to its appraisal and coping functions*”. However, coping is so expansive in Lazarus and Folkman (1984) and Folkman et al. (1986) that even taking concrete steps to change the environment –framed as primary control in this study– corresponds to many coping strategies (McCrae et al. 1984). Thus, their framework is impressively inclusive but blurs the lines between being in control, being out of control, and what we otherwise think of as coping with a situation that one cannot influence.

Alternatively, using Rothbaum et al.’s (1982) perspective, it is possible to distinguish between being able to change one’s environment from changing one’s self. When comparing secondary privacy control to coping, the only coping strategy that in any way resembles secondary control is escape-avoidance (Folkman et al. 1986). Escape-avoidance is recently found in prominent IS studies on privacy (e.g., Liang et al. 2019), where it is operationalized as wishful thinking.

This dissertation recognizes that secondary privacy control bears surface resemblance to wishful thinking. Indeed, secondary control is also about accepting a new situation (Morling and Evered 2006). However, those who engage in escape-avoidance strategies such as wishful thinking tend to avoid new information and resist revisiting their beliefs (Folkman et al. 1986). In terms of privacy, wishful-thinking

oriented individuals might accept conditions of lowered privacy but fail to adjust to the new standard. Rather, they are prone to fantasizing how they can escape this situation. For example, if we adapt Liang et al.'s (2019) Privacy Wishful Thinking items to our Facebook context, they would read as: *“I fantasize that all of a sudden privacy issues on Facebook will disappear by themselves.”*, *“I fantasize that I would somehow come across a magical solution for privacy issues on Facebook.”*, *“I fantasize that privacy issues on Facebook will go away or somehow I will be over with.”*, *“I fantasize that everything will turn out just fine as if privacy issues on Facebook never happened.”*

In contrast, secondary privacy control-oriented users attempt to both accept and adjust to the new privacy conditions. By and large, this adjustment is hopeful in nature and foresees improved outcomes: *“It is better to accept any privacy issues of using Facebook rather than trying to fight them.”*, *“When it comes to privacy issues on Facebook, I think it’s better to just wait and see how things turn out.”*, *“Whatever privacy issues there are on Facebook, things will work out for the best anyway.”* Thus, Figure 5 shows that while secondary privacy control and privacy wishful thinking strategies overlap in the acceptance of privacy issues, they differ in whether they adjust, or not, to these challenges.



**Figure 5:** Secondary Privacy Control vs. Privacy Escape-Avoidance Coping

Coping is often related to negative psychological conditions and secondary control with adaptive psychological conditions. Coping strategies (e.g., wishful thinking) are many times classified as extreme psychological condition of emotional unstable individuals (Bolger 1990). This argument must be taken



with care because some studies investigating “lowering aspirations”, a secondary control strategy, find they are detrimental to one’s well-being (Wrosch et al. 2002). But in more recent rebuttals to this approach, there has been a warning call in how secondary control is interpreted and operationalized (Morling and Evered 2006). These authors explain that measuring secondary control as uniquely acceptance or adjustment constrains the full nature of secondary control to only serve the purpose of gaining primary control.

Finally, the field of information systems is itself increasingly aware of people’s need to accept and adjust to the growing complexity of information technologies in everyday life. For example, the literature of technostress recognizes that a positive psychological response to technological stressors is reflected by efforts to both directly control and indirectly accept and adjust to some optimal amount of stress in stressful situations (Califf et al. 2020). Such studies are among the first in our discipline to recognize that adaptation is a healthy response that happens alongside efforts to directly control outcomes.

It is also possible to look at this issue empirically. Study 2 includes the conceptualization and measurement of privacy wishful thinking, the prominent privacy escape-avoidance coping strategy used in information systems studies (Liang et al. 2019), to compare it against secondary privacy control. Although Study 2 has different goals than the earlier study (Study 1), it is designed to additionally replicate the proposed model from Study 1. Table 11 shows a near-replication of Study 1 using data from Study 2. Specifically, it displays the results of two models, one using Secondary Privacy Control (SPC) and the other replacing it with Privacy Wishful Thinking (WISH). The nomological networks of secondary privacy control and privacy wishful thinking are different, and at times contrary to each other. For instance, smartphone self-efficacy decreases one’s secondary privacy control ( $\beta=-0.14$ ,  $p$ -value=0.062) but does not affect privacy wishful thinking ( $\beta=0.00$ ,  $p$ -value=0.997). In turn, secondary privacy control has a powerful negative effect on information privacy concern ( $\beta=-0.32$ ,  $p$ -value<0.001),

in contrast to privacy wishful thinking which does not have an effect ( $\beta=0.01, p\text{-value}=0.887$ ). Similarly, the effects of secondary privacy control on distancing ( $\beta=0.01, p\text{-value}=0.896$ ) and exit intentions ( $\beta=-0.05, p\text{-value}=0.560$ ) are not significant, but, privacy wishful thinking has a positive significant effect on distancing ( $\beta=0.32, p\text{-value}>0.001$ ) and exit ( $\beta=0.18, p\text{-value}>0.01$ ). Thus, secondary privacy control materializes in a different form than privacy escape-avoidance coping strategies (i.e., privacy wishful thinking) and also has different consequences on outcomes.

**Table 11:** Secondary Privacy Control vs. Privacy Escape-Avoidance Models

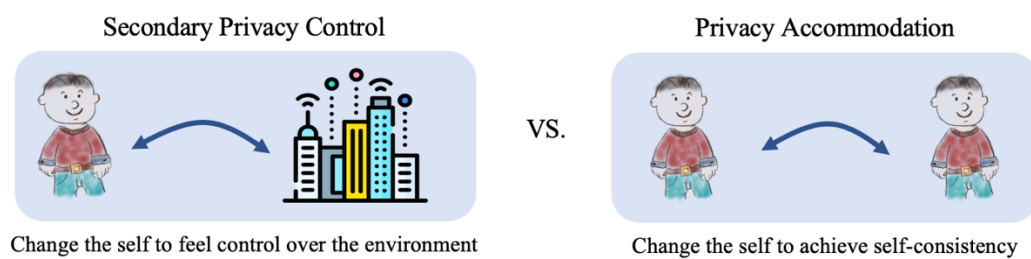
| Secondary Privacy Control Model |         |          |          |         |         | Privacy Escape-Avoidance Model |         |          |         |         |         |
|---------------------------------|---------|----------|----------|---------|---------|--------------------------------|---------|----------|---------|---------|---------|
|                                 | PPC     | SPC      | PCON     | DIST    | EXIT    |                                | PPC     | WISH     | PCON    | DIST    | EXIT    |
| <i>R</i> <sup>2</sup>           | 0.24    | 0.09     | 0.39     | 0.28    | 0.25    | <i>R</i> <sup>2</sup>          | 0.24    | 0.08     | 0.30    | 0.35    | 0.27    |
| iSEFF                           | 0.37*** | -0.14    | -0.10    | 0.01    | -0.09   | iSEFF                          | 0.37*** | 0.00     | -0.07*  | 0.02    | -0.08   |
| PPC                             |         |          | 0.23**   | -0.01   | -0.01   | PPC                            |         |          | 0.20    | 0.01    | -0.02   |
| SPC                             |         |          | -0.32*** | 0.01    | -0.05   | WISH                           |         |          | 0.01    | 0.32*** | 0.18**  |
| RISK                            |         |          | 0.30***  | 0.01    | 0.09    | RISK                           |         |          | 0.37*** | 0.00    | 0.08    |
| PCON                            |         |          |          | 0.18    | 0.13    | PCON                           |         |          |         | 0.18*   | 0.15*   |
| NORM                            |         |          |          | -0.07   | -0.06   | NORM                           |         |          |         | -0.15   | -0.12   |
| EXP                             |         |          | 0.37***  | 0.40*** | 0.35*** | EXP                            |         |          | 0.32*** | 0.36*** | 0.31*** |
| AGE                             | 0.24*** | -0.26*** | 0.02     | -0.14*  | -0.16*  | AGE                            | 0.24*** | -0.27*** | 0.09    | -0.08   | -0.11   |
| GEN                             | -0.19** | 0.01     | 0.06     | 0.12*   | 0.15*   | GEN                            | -0.19** | 0.10     | 0.06    | 0.10    | 0.14*   |

NOTES: SEFF: iPhone self-efficacy; RISK: general privacy risk awareness; PPC: primary privacy control; SPC: secondary privacy control; WISH: wishful thinking; PCON: information privacy concern; NORM: SNS normative benefit; PEXP: prior experience; AGE: age; GEN: gender. Path significances: \* $p < 0.05$ ; \*\* $p < 0.01$ ; \*\*\* $p < 0.001$ .

## Secondary Privacy Control and Privacy Accommodation

In contrast to secondary control that arises from the need to control (Rothbaum et al. 1982), accommodation is the result of the need to “achieve consistency between actual and intended courses of personal development” (Brandtstadter and Renner 1990) (Figure 6). Secondary privacy control-oriented individuals are motivated to change the way they approach privacy issues in order to fit the requirements of the new environment without losing control. However, privacy accommodation-oriented individuals might attempt to adjust themselves to fit their ideal selves and achieve consistency in the way they want to keep their privacy. The accommodation focus on self-performance is evidenced in its most common operationalization (Brandtstadter and Renner 1990): “In general, I am not upset very long about an

opportunity passed up", "I can adapt quite easily to changes in a situation", "After a serious disappointment, I soon turn to new tasks", "I usually recognize quite easily my own limitations". For example, the item "Even if everything goes wrong, I still can find something positive about the situation" from accommodation clearly focuses on one's doing. Likewise, "Whatever privacy issues there are on Facebook, things will work out for the best anyway" from secondary privacy control has a focus on how people expect other powerful agents to change the individual's environment.



**Figure 6:** Secondary Privacy Control vs. Privacy Accommodation

Additionally, while accommodation and assimilation are compared against secondary and primary control, the first two are considered coping mechanisms (Brandtstadter and Renner 1990, Rothermund and Brandtstadter 2003). As a consequence, if privacy accommodation were to be used as a substitute for secondary privacy control, it would again have been not easy to clearly delimitate the boundaries of control and coping strategies.

### **Secondary Privacy Control and Privacy Primary Appraisal**

From the lens of coping theory, control is a process comprising two phases –appraisal and coping–and the coping literature aims at “disaggregating the concept of control with respect to its appraisal and coping functions, ...” (Lazarus and Folkman 1984, p. 171). These authors conceive primary appraisal as: “consist[ing] of the judgment that an encounter is irrelevant, benign-positive, or stressful.” (p. 54), and secondary appraisal as: “[...] a judgment concerning what might and can be done.” (p. 54). They also discuss appraisal as a necessary antecedent of coping: “Appraisal proved to be a potent predictor of

*whether coping was oriented toward emotion-regulation (emotion-focused coping) or doing something to relieve the problem (problem-focused coping).*” (p. 44). As a consequence, people must perceive an encounter as a threat (e.g., primary appraisal) to think what they might or can do about it (e.g., secondary appraisal) to finally do it (e.g., emotion-focused coping or problem-focused coping). They must identify a threat which leads people to re-evaluate the potential effectiveness of their strategies and, if needed, finally resort to coping mechanisms either to change their environment or to change themselves.

Recent work in the information systems literature (Liang et al. 2019) has operationalized primary appraisal as a sort of concern: *“The malicious nature of the problem [IT security breach] threatened me”*, *“The threat [IT security breach] was fearful”*, *“The threat [IT security breach] made me anxious”*. In contrast, secondary privacy control is operationalized in this study as the recognition of a threat and a expected useful strategy: *“It is better to accept any privacy issues of using Facebook rather than trying to fight them”*, *“When it comes to privacy issues on Facebook, I think it’s better to just wait and see how things turn out”*, *“Whatever privacy issues there are on Facebook, things will work out for the best anyway”*. Thus, while primary appraisal is captured by individuals’ recognition of the threat, secondary privacy control-oriented individuals, beyond recognizing the threat, have a strategy to use when required.

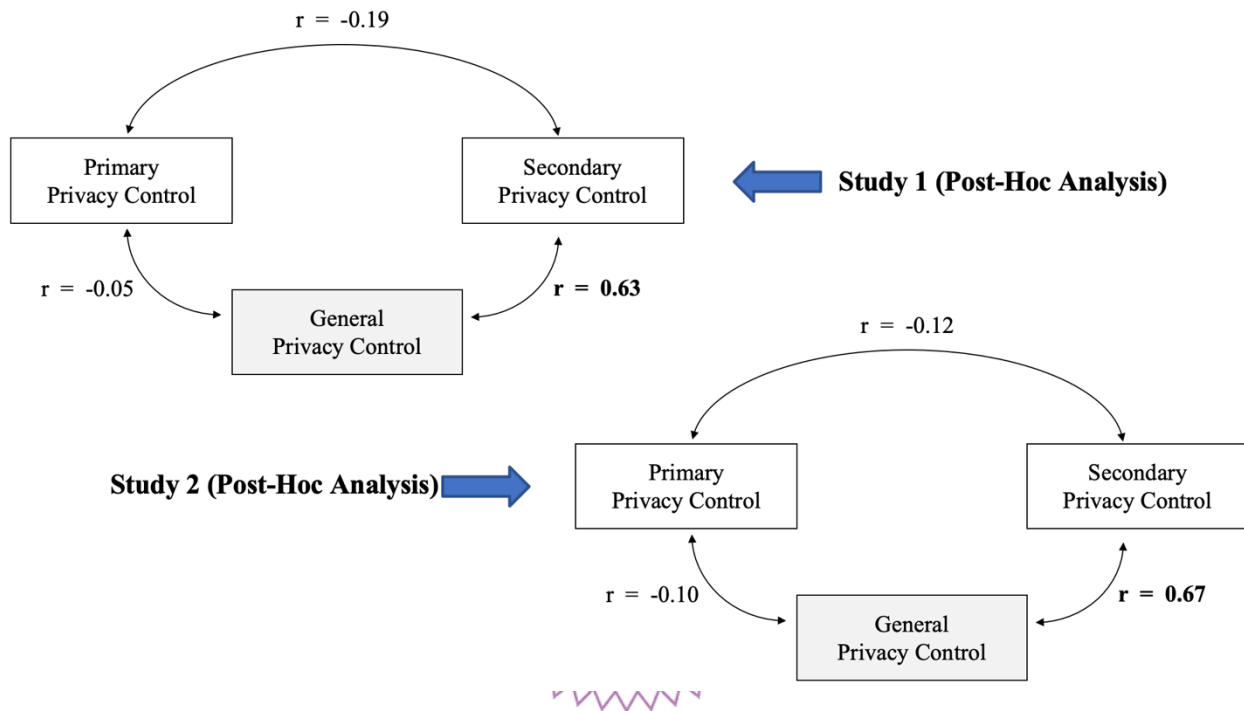
For example: *“When it comes to privacy issues on Facebook [perhaps primary appraisal], I think it’s better to just wait and see how things turn out [strategy]”* is made of the recognition of privacy issues on Facebook plus the strategy of observing and waiting for the best moment to act on privacy issues. Thus, there is agreement with thinking that secondary privacy control also captures part or perhaps all of primary appraisal perceptions, but also this research shows that secondary privacy control includes a strategy, not narratively or operationally considered in primary appraisal.

### **Post Hoc Empirical Comparisons with Secondary Privacy Control**

Additionally, this dissertation includes some post hoc analysis useful to see clearer differences and similarities between prior conceptualizations in relation to secondary privacy control.

## Secondary Privacy Control vs. General Privacy Control

Using data from Study 1 and 2, a closer look at the relationship between dual privacy control constructs and the general privacy control construct found in Xu et al. (2012) is offered. Figure 7 shows the correlation between these concepts.



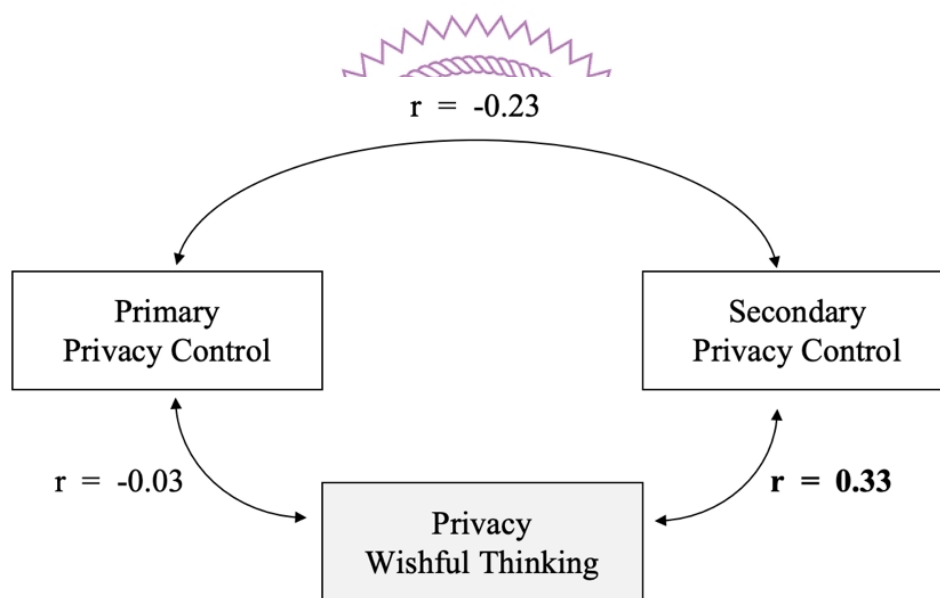
**Figure 7:** Correlation of Privacy Control Constructs

In both empirical studies there is a considerable overlap between secondary privacy control and general privacy control ( $r_{Study1}=0.63$   $r_{Study2}=0.67$ ). Moreover, the correlation between primary privacy control and general privacy control in both studies is small and negative ( $r_{Study1}=-0.05$   $r_{Study2}=-0.10$ ) just as between primary privacy control and secondary privacy control ( $r_{Study1}=-0.19$   $r_{Study2}=-0.12$ ). These results bring to mind prior structural equation modelling analysis in Study 1 where general privacy control and secondary privacy control have negative significant effects on information privacy concern; even when conceptually, secondary privacy control and general privacy control represent opposite notions. Overall, it is suggested in this manuscript that the most common way in which researchers have measured privacy

control represents secondary privacy control or the idea of users gaining a feeling of control by accepting and adjusting to privacy issues.

### Secondary Privacy Control vs. Privacy Wishful Thinking

The second wave of Study 2 also includes the measurements of wishful thinking (Liang et al. 2019) for the sake of comparing it with our principal constructs. After running a CFA analysis to ensure the reliability and validity of the privacy wishful thinking items and construct, a correlation table was built to grasp an idea of their commonalities and differences. Figure 8 shows that secondary privacy control and privacy wishful thinking are mildly correlated ( $r_{Study2-secondwave}=0.33$ ). The remaining variance (0.67) suggests these two constructs are different as it is theoretically argued.



**Figure 8:** Correlation of Dual Privacy Controls and Privacy Wishful Thinking

### Secondary Privacy Control vs. Primary Privacy Control

#### Cross-Lagged Panel Model Analysis

As a complementary statistical technique, we use the Cross-Lagged Panel Model (CLPM) analysis to compare the potential relationship between the two privacy controls in two different times. CLPM

analysis involves including measurements of the same variable in at least two points in time and estimating their effects using multivariable analysis such as structural equation modeling (Duncan 1969). This methodology is popular among researchers because not only it can significantly address issues of causality (Zablan et al. 2016), but also reciprocal causality (Allison et al. 2017). Thus, we used data from our Study 2 to estimate this model, shown in the figure below.

#### Long-Term Nature of Secondary and Primary Privacy Controls

This dissertation views the two privacy control constructs similarly to how developmental psychologists and biologists view healthy psychological and biological development – as the maintenance of equilibrium or homeostasis (Piaget 1970, Cannon 1929). Secondary and primary privacy controls are mechanisms that users can simultaneously use to maintain an equilibrium in the concern over privacy; they might rely more on one at certain times but are free to avail both. This reasoning is echoed by Rothbaum et al. (1982) (p. 8): *“Neither process [primary and secondary control] is thought to exist in pure form, often both processes are intertwined, as when persons negotiate and compromise [...] the difference between primary and secondary control should be thought of as a difference in emphasis”*. A visualization of the distribution of respondents based on their secondary and primary privacy control orientations in Figure 9 shows that both controls appear in individuals in simultaneous ways.





We observe that the autoregressive effects of each privacy control at Time 1 upon itself at Time 2 are far more important than the cross-lagged effects between primary privacy control and secondary privacy control measured across the two times ( $\beta_{Time1}=-0.14, p\text{-value}=0.090$ ;  $\beta_{Time2}=-0.11, p\text{-value}=0.029$ ). These results provide further evidence that these two privacy control constructs represent parallel, mechanisms that people simultaneously avail to protect themselves. If there are cross-effects over time, they are likely very minimal. While Study 2 does not have long term data, some measurements can be reused to get some preliminary evidence of whether secondary privacy control and primary privacy control are states (i.e., short-term, temporary) or orientations (i.e., long-term, chronic). The above post-hoc analysis, reveals that there is a strong tendency in people to maintain one's privacy orientation for a reasonable period of time (about 4 months between waves in Study 2) indicating that the dual privacy controls are relatively stable orientations rather than short-term states.

### **Secondary Privacy Control as a Form of Privacy Concern**

Theoretically, the difference between any type of concern and secondary privacy control is that the latter includes a potential strategy. For example, the information privacy concern item: *“When I give my preferences or information to Facebook for the use of its services, I am concerned it may use my information for other purposes”* expresses the worry of users when they provide their own information to Facebook. Similarly, the general privacy risk awareness item: *“In general, it could be risky for people to put personal information on Facebook”* shows how worried users are when they provide information to Facebook, but in a more general sense for all people. In contrast, the secondary privacy control item: *“When it comes to privacy issues on Facebook [perhaps primary appraisal], I think it's better to just wait and see how things turn out [strategy]”* includes a strategy (“wait and see”) to overcome those concerns. Moreover, the mainstream information systems privacy research suggests (Dinev and Hart 2004) and applies (Xu et al. 2012) the separation of both notions: One as related to fairness and the other to control. This study recognizes that one of the advantages of separating both concepts is the richness

brought to privacy studies; for example, the proposition of actionable antecedents of privacy such as agency (Xu et al. 2012).

In order to see the difference between control and concern, this post-hoc analysis (table below) considers the nomological network of the secondary privacy control, and general privacy risk awareness as exemplars of control- and concern-like constructs. Using the collected data from Study 1 and 2, it is possible to show that secondary privacy control is negatively associated with exit intentions, and that general privacy risk awareness is positively associated with this same outcome. Thus, secondary privacy control does not behave like erosion of concern, lessened concern, or even information privacy concern but rather it is an antecedent of concern because it includes a strategy to reduce concern.

**Table 12:** Secondary Control as a Form of Concern

|                       | Study 1  |          |          |          |           | Study 2 |          |           |          |          |
|-----------------------|----------|----------|----------|----------|-----------|---------|----------|-----------|----------|----------|
|                       | PPC      | SPC      | PCON     | DIST     | EXIT      | PPC     | SPC      | PCON      | DIST     | EXIT     |
| <i>R</i> <sup>2</sup> | 0.37     | 0.52     | 0.47     | 0.43     | 0.36      | 0.24    | 0.09     | 0.39      | 0.28     | 0.25     |
| SEFF                  | 0.26 *** | 0.16 **  | -0.06    | -0.16 ** | -0.24 *** | iSEFF   | 0.37 *** | -0.14     | -0.10    | 0.01     |
| REG                   | -0.15 *  | 0.48 *** | -0.09    | 0.05     | 0.08      | PPC     |          | 0.23 **   | -0.01    | -0.01    |
| UNA                   | 0.50 *** | -0.16 ** | 0.10     | 0.07     | -0.04     | SPC     |          | -0.32 *** | 0.01     | -0.05    |
| COL                   | -0.11    | 0.36 *** | 0.01     | 0.04     | 0.08      | RISK    |          | 0.30 ***  | 0.01     | 0.09     |
| PPC                   |          |          | 0.36 *** | -0.15 *  | -0.13     | PCON    |          |           | 0.18     | 0.13     |
| SPC                   |          |          | -0.17 *  | 0.00     | -0.13     | NORM    |          |           | -0.07    | -0.06    |
| RISK                  |          |          | 0.24 **  | 0.06     | 0.07      | PEXP    |          | 0.37 ***  | 0.40 *** | 0.35 *** |
| PCON                  |          |          | 0.49 *** | 0.37 *** |           | AGE     | 0.24 *** | -0.26 *** | 0.02     | -0.14 *  |
| NORM                  |          |          | -0.14 *  | -0.06    |           | GEN     | -0.19 ** | 0.01      | 0.06     | 0.12 *   |
| EXP                   |          |          | 0.29 *** | 0.18 **  | 0.23 **   |         |          |           |          |          |
| AGE                   | 0.11     | 0.07     | -0.05    | -0.09    | -0.04     |         |          |           |          |          |
| GEN                   | -0.01    | -0.16 ** | 0.06     | 0.08     | 0.10 *    |         |          |           |          |          |
| INC                   | 0.02     | 0.08     | 0.06     | 0.18 *** | 0.09      |         |          |           |          |          |
| EDU                   | -0.02    | 0.05     | 0.03     | 0.03     | -0.01     |         |          |           |          |          |

NOTES: SEFF: SNS self-efficacy; iSEFF: iPhone self-efficacy; REG: SNS regulation; COL: collectivism; UNA: uncertainty avoidance; PPC: primary privacy control; SPC: secondary privacy control; RISK: general privacy risk awareness; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefits; EXP: prior experience with privacy threats; GEN: gender; AGE: age range; INC: income range; EDU: education level. **The constructs in Study 2 are collected in two waves, first independent constructs and in a second wave the dependent constructs.**

## Discussion

Overall, secondary privacy control is conceptually and empirically different from privacy escape-avoidance coping. At least theoretically and operationally, secondary privacy control found to be different from privacy accommodation and privacy primary appraisal. Moreover, in both studies,

secondary privacy control is strongly correlated to the common notion of general privacy control often used in privacy research. Interestingly, this study also gives initial insights regarding the long-term nature of both privacy controls.

### **Theoretical Contributions**

While secondary privacy control is about accepting and adjusting to the new privacy conditions, privacy escape-avoidance coping is about accepting and escaping-avoiding them. The most interesting takeaway from these empirical differences is that secondary privacy control is dependent in part on one's abilities (self-efficacy) and can mitigate concern. In contrast, coping mechanisms like wishful thinking are momentary escapes and do not effectively lower one's enduring privacy concern. From these findings, we can further appreciate why secondary control, in general, is seen as a positive adjustment whereas coping strategies like wishful thinking are maladjustments that do not deal with concern and stressors. Also, secondary privacy control is different from privacy accommodation in the underlying motivation: while privacy accommodation arises from the need to achieve consistency between the current and the ideal self, secondary privacy control arises from the need to achieve control in dealing with the environment. Finally, even when the dual privacy controls are found to be long-term orientation, further examination with longitudinal data (Mulder and Hamaker 2020) is required to confirm these findings.

Most conceptualizations of privacy control have commonly highlighted the user's ability to deal with challenging privacy issues on information system platforms (Dinev and Hart 2004, Xu et al. 2012). This general privacy control notion largely corresponds to the theoretical understanding of primary privacy control, but mostly overlaps with the operationalization of secondary privacy control or accepting and adjusting the self to privacy challenges. This startling mismatch suggests that while researchers have been conceptualizing privacy control as personally taking steps to protect one's privacy, they have actually been measuring some sort of unknown mixture between their conceptualization and people's attempts to change their selves to adapt to the new realities of privacy. Given the general privacy control

measurements leave the strategies users use to take control over their privacy unrevealed, it is not easy to learn about the true nature of privacy control. The reconceptualization proposed in this manuscript promises to solve this problem by including privacy control strategies in a cohesive way and within the framework of secondary and primary privacy control, solidly-grounded in seminal thinking regarding the psychology of control (Rothbaum et al. 1982). It is believed that thinking about privacy control as the expected results of strategies users have can facilitate the development of further theoretical insights regarding how people attempt to protect their privacy.

General privacy control only weakly correlated to primary privacy control, thus, it is very possible that one or the other of the dual privacy control orientations can be more salient in different contexts, and so the sense of general privacy control could very well correlate more strongly to primary privacy control in some settings. Wherever researchers are focusing on explaining the relationship between privacy control and privacy concern, or other outcomes, it is strongly advised to model both aspects of privacy control to fully capture how users balance these two approaches in a given research context. Nonetheless, the general privacy control construct might still serve other purposes, such as a parsimonious statistical control-variable in studies where privacy control is not a focal concept.

### **Managerial Contributions**

Clearly distinguishing the concept of secondary privacy control from its potential confounding notions provides social network service management and policy regulators with a more detailed understanding of how secondary privacy control-oriented users *do not* approach privacy issues when protecting their privacy. Practitioners armed with this knowledge and data lakes could profile users and infer their motivations, being those control, coping, accommodation or primary appraisal, to more specifically design policies and features accordingly. Thus, disentangling the nature of secondary privacy control is beneficial to organizations as they are given the tools and guidelines to be even more selective about the strategies they attempt to put in practice.

## Chapter 6: Repositioning Privacy Control

### Overall Contributions

The ultimate theoretical contribution of this manuscript is the conception of privacy control as a dual process and its implications. Secondary privacy control represents a form of control where one accepts and adapts to lowered privacy conditions in which users, out of their lack of ability, need for time, or choice to follow the preferences of one's social network, seem not to protect their privacy. Nonetheless, these users keep hope alive that the situation will change and rely on powerful others to bring about this change. Thus, this is not a helpless orientation but a hopeful one. It is in stark contrast to primary privacy control, wherein users seek to achieve privacy protection by using their own learning, ability, and efforts. This dissertation takes on two major questions: what is the nature and antecedent explanations for varying perceptions of privacy control, and to what degree does it go beyond mitigating concern and affect intentions and behaviors?

### Overall Theoretical Contributions

General privacy control, as a holistic measure of privacy control, has been alternately found to decrease (Dinev and Hart 2004, Xu et al. 2012) or increase (Wang et al. 2016, Miltgen and Peyrat-Guillard 2014) individual concern about one's information privacy. Moreover, the unrestricted use of social network platforms by some and the resistance to use them by others also reflect this dual phenomenon (Edison Research 2019, 2022). This overall study proposed and found that such divergent effects can be reconciled if researchers and practitioners conceptualize privacy control as having a dual nature. Secondary privacy control, which entails accepting and adjusting to new privacy conditions, reduces one's information privacy concern while primary privacy control, which entails personally taking steps to protect one's privacy, increases it.

Second, while this manuscript replicates the effects of agentic antecedents on privacy control, it also shows that SNS regulations lowers one's primary privacy control. We surmise that users with faith

in government and industry regulations do not adopt extreme vigilance to manage their privacy. Users might rely on primary privacy control when they are alert to changes in the privacy climate, but avail secondary privacy control during the wait-and-see period when they rely on the hope that desirable privacy outcomes will prevail. The dual privacy control also arises from one's culturally-informed personal values. Uncertainty avoidance and collectivism reflect people's ultimately choices of how to deal with uncertainty. Collectivists are inclined to underplay personal threats and adopt the long-term view of secondary privacy control, but people who value uncertainty avoidance seek to deal immediately and directly with privacy threats through primary privacy control. These clear differences in the relationship between these two values and dual privacy controls again underscore the key differences between secondary and primary control.

Secondary privacy control adversely affects people's privacy protection by decreasing the likelihood of a user undertaking minimal steps to protect one's privacy, as they think their privacy is or will be protected, perhaps by powerful others. While accepting and adjusting to privacy threats brings peace-of-mind to users and affords them a wide range of possibilities in their interactions, the internalization of current privacy circumstances as the new normal also blinds them from seizing opportunities to better protect their privacy.

In direct contrast to secondary privacy control, privacy escape-avoidance coping is about accepting and escaping-avoiding privacy issues and so does not come from one's ability (SNS self-efficacy). From these findings, we can further appreciate why secondary control, in general, is seen as a positive adjustment whereas coping strategies like wishful thinking are maladjustments that do not deal with concerns and stressors. Secondary privacy control and privacy accommodation differ in the underlying motivation to control the environment: competence and consistency, respectively. Additionally, the dual privacy controls are found to be long-term orientations, however, further examination with longitudinal data (Mulder and Hamaker 2020) is required to confirm these findings.

Finally, the general privacy control notion found in literature seems to conceptually correspond to primary privacy control, but we unexpectedly find it empirically overlaps with secondary privacy control. The psychometrics of general privacy control do not account for the strategies adopted to control one's privacy and so a general sense of privacy control remains unknown.

By including dual privacy controls in a cohesive way, this deeper understanding of privacy control proposed in this manuscript offers to solve the paradoxical effect of privacy control on privacy concern. The framework of secondary and primary privacy control is solidly-grounded in seminal thinking regarding the psychology of control (Rothbaum et al. 1982) and so it is suggested that wherever researchers are focusing on explaining the relationship between privacy control and privacy concern, or other outcomes, it is strongly advised to model both aspects of privacy control to fully capture how users balance these two approaches in a given research context. Nonetheless, the general privacy control construct might still serve other purposes, such as a parsimonious statistical control-variable in studies where privacy control is not a focal concept.

### **Overall Managerial Contributions**

Managers, designers of user experience, and policy makers should consider the dual nature of privacy control in social networking services when designing interventions. Service providers are increasingly giving users more privacy management settings and tools to enhance their privacy control (e.g., Newcomb 2018). Although these tools could benefit users with primary privacy control orientations who are inclined to use them, these privacy tools may at best have a palliative effect on users oriented toward secondary privacy control who are not inclined to investigate or alter their environment. Counter-intuitively, providing more privacy management settings might only further increase the vigilance and concern of users under primary privacy control while lowering the concern of users who are more inclined toward secondary privacy control despite the unlikelihood they would use these tools to secure their privacy. This is partly reflected in Study 2, where users under secondary privacy control were found

to be less likely to update their phone operating system to include advertised privacy-protecting features. Thus, rather than assuming that privacy settings and tools are enough, service providers might better protect their users by reducing privacy exposure more directly through conservative privacy defaults and design, and rely less on all users making sense of a dizzying array of privacy options.

Segmenting users based on their privacy control orientation can advance security prevention policies and avoid adverse consequences to the normal development of businesses and to the subsequent outcomes. As part of governmental requirements, or at times by company initiatives, organizations invest a great amount of effort and time to figure out ways in which they can help users better protect their privacy. Both studies shed light into the motivational aspect of users' behavior. Interestingly, it was found that secondary privacy control-oriented individuals do not upgrade their mobile phone operating system, even when such action was beneficial to their privacy (Study 2). These users have come to understand that their goal is to accept and adapt to circumstances as they come to exist in the privacy domain. Thus, service providers can be better off if they devise strategies that motivate these particular users into accepting newly released implementations. For example, companies could devise features that target users' attention and provide them with the necessary means to adopt them. Failing to recognize individuals who delay the adoption of organizational implementations might provoke disruptions in the service platform's operating systems and even force a change in the organization's business model.

Practitioners should also note that the roots of the dual privacy controls are both agentic and value-based. Although our study examined several decision-making factors, it is very possible a service provider is operating in a market in which one of these factors is more prevalent among users. For example, a firm could potentially operate in a largely collectivist culture and so expect greater secondary privacy control orientations. Conversely, a domain-specific group of, say, tech savvy users might have the abilities and inclination to adopt a more primary privacy control orientation. An understanding of the psychological makeup of their user base should guide providers in how they differentially help users



manage privacy issues and so reduce protective intentions that could possibly limit the vitality of their network. Moreover, in an age of increased data, service providers could even attain the personalization of privacy protective measures.

Secondary privacy control-oriented users *do not* approach privacy issues in ways those coping, accommodating, or even appraising privacy threats do. Practitioners could profile users and infer their motivations, being those control, coping, accommodation or primary appraisal, to more specifically design policies and features accordingly. Thus, disentangling the nature of secondary privacy control is beneficial to organizations as they are given the tools and guidelines to be even more selective about the strategies they attempt to put in practice.

Overall, focusing on the dual perspective of privacy control affords businesses detailed insights about how users approach privacy issues and so protect their privacy, in contrast to the more general conceptualization of privacy control. Organizations are now given the means to develop privacy protection strategies that specifically address each type of privacy control orientation.

### **Limitations and Future Directions**

There are several important challenges future research needs to address. First, this first glimpse of how general privacy concern relates to the dual privacy control constructs needs to ascertain whether any meaning is missing in the dual perspective. As data ownership gains traction by the creation and enforcement of regulations that give control to users over their private information (Fadler and Ledger 2021), and the role of psychological ownership in affecting one's privacy control in relation to others becomes more salient (Zhang et al. 2022). It is relevant to understand the direct relation between psychological ownership and dual privacy controls, especially with secondary privacy control as both constructs seem to converge in the psychological aspect. For example, some studies in other domains of the information systems literature have proposed the dual privacy controls alongside psychological ownership as parallel routes to approaching intentions (Wang et al. 2021).

Second, although two culturally-informed personal values inform the dual privacy controls as largely compatible with the prior literature on dual control theory, they are not the only way to capture value-based antecedents. Researchers should examine other perspectives on personal values (Schwartz et al. 2012) that may yield greater insight for specific contexts. Moreover, this manuscript captures the associations of these values with the dual privacy controls through a cross-sectional study. It would be of great value to incorporate these constructs into randomized experiments and longitudinal studies to develop stronger causal and behavioral linkages.

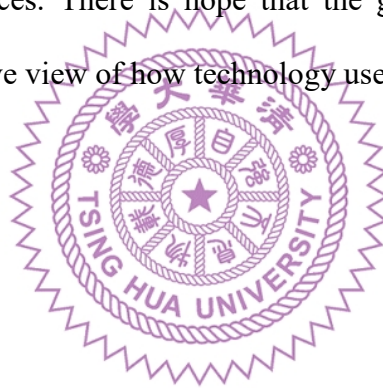
Finally, several of our demographic correlates offer an exploratory glimpse into the roles of gender, age, and socioeconomic status on the dual privacy controls, all of which are concerns that echo in the broader literature of dual controls (Hall et al. 2006a). Thus, these results suggest that much remains to know about how social identity affects privacy control and concern, beyond what this study uncovered.

## **Conclusions**

Privacy breaches in social media are increasingly implicated in influencing a wide range of social discourse, including political outcomes (Hitlin et al. 2019). Perhaps there has never been a more relevant time to investigate how the users of online services truly react and adapt to privacy threats, and this study provides just such a lens to more fully examine why people react differently to privacy threats. Privacy control has been regarded as the users' willingness to take action to change privacy outcomes. This dissertation takes on two major questions: what is the nature and antecedent explanations for varying perceptions of privacy control, and to what degree does it go beyond mitigating concern and affect intentions and behaviors? We found evidence for the dual nature of privacy control. Users not only attempt to proactively use privacy protective strategies, but they also simply attempt to accept and adjust to a deteriorating privacy environment. Understanding both privacy control orientations helps reconcile different findings about the relationship between privacy control and concern (Study 1). The two types of privacy control come from different personal values, some of which might reflect political or cultural

differences worth noting (Study 1). Moreover, the dual privacy controls can directly influence protective behaviors (Study 2).

Adopting the dual perspective of control leads to theoretical developments and practical advancements in ensuring and assuring users of privacy. These practical implications include the consideration of the users' psychological makeup in the design of privacy policies and artifacts that cater to differing approaches to privacy control. Moreover, this differentiation can be used in security prevention policies as they have important consequences on the normal development of business and on the consequent outcomes. Neglecting secondary and primary privacy control can harm our understanding and management of privacy, while recognizing its role can prove useful in understanding and designing successful social networking services. There is hope that the general frameworks proposed in this dissertation produce a more inclusive view of how technology users simultaneously combat, adjust, and struggle with privacy issues.



## References

- Abramson, L. Y., Seligman, M. E., and Teasdale, J. D. 1978. "Learned Helplessness in Humans: Critique and Reformulation," *Journal of Abnormal Psychology* (87:1), pp. 49.
- Ajzen, I. 2002. "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior," *Journal of Applied Social Psychology* (32:4), pp. 665-683.
- Al-Natour, S., Cavusoglu, H., Benbasat, I., and Aleem, U. 2020. "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research* (31:4), pp. 1037-1063.
- Allison, P. D., Williams, R., and Moral-Benito, E. 2017. "Maximum Likelihood for Cross-Lagged Panel Models with Fixed Effects," *Socius: Sociological Research for a Dynamic World* (3), pp. 1-17.
- Apple 2022a. *Privacy*. Retrieved from <https://www.apple.com/privacy/features/>
- Apple 2022b. *App Privacy Details on the App Store*. Retrieved from <https://developer.apple.com/app-store/app-privacy-details/>
- Apple 2022c. *Users Privacy and Data Use*. Retrieved from <https://developer.apple.com/app-store/user-privacy-and-data-use/>
- Specktor 2021. *Impact of Apple Limit Ad Tracking on Attribution (before iOS 14)*. Retrieved from <https://support.appsflyer.com/hc/en-us/articles/115003734626-Impact-of-Apple-iOS-Limit-Ad-Tracking-on-attribution>
- Armstrong, J. S., and Overton, T. S. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396-402.
- Babrow, A. S., and Kline, K. N. 2000. "From "Reducing" to "Coping with" Uncertainty: Reconceptualizing the Central Challenge in Breast Self-Exams," *Social Science & Medicine* (51:12), pp. 1805-1816.

- Bagozzi, R. P., and Yi, Y. 1988. "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science* (16:1), pp. 74-94.
- Balasubramanian, M. 2022. *App Tracking Transparency Opt-In Rate - Monthly Updates*. Retrieved from <https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/>
- Band, E. B., and Weisz, J. R. 1988. "How to Feel Better When It Feels Bad: Children's Perspectives on Coping with Everyday Stress," *Developmental Psychology* (24:2), pp. 247-253.
- Bandura, A. 1982. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37:2), pp. 122-147.
- Bandura, A. 2001. "Social Cognitive Theory: An Agentic Perspective. *Annual Review of Psychology* (52:1), pp. 1-26.
- Bandura, A. 2006. "Toward a Psychology of Human Agency," *Perspectives on Psychological Science* (1:2), pp. 164-180.
- Bailis, D. S., Chipperfield, J. G., and Perry, R. P. 2005. "Optimistic Social Comparisons of Older Adults Low in Primary Control: A Prospective Analysis of Hospitalization and Mortality," *Health Psychology* (24:4), pp. 393-401.
- Baumer, E. P., Adams, P., Khovanskaya, V. D., Liao, T. C., Smith, M. E., Schwanda Sosik, V., and Williams, K. 2013. "Limiting, Leaving, and (Re) lapsing: An Exploration of Facebook Non-Use Practices and Experiences," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3257-3266.
- Bechwati, N. N., and Xia, L. 2003. "Do Computers Sweat? The Impact of Perceived Effort of Online Decision Aids on Consumers' Satisfaction with the Decision Process," *Journal of Consumer Psychology* (13:1-2), pp. 139-148.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1042.

Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *The Information Society* (20:5), pp. 313-324.

Benitez-Amado, J., Henseler, J., and Castillo, A. 2017. "Development and Update of Guidelines to Perform and Report Partial Least Squares Path Modeling in Information Systems Research. Development. In the proceedings of the Twenty First Pacific Asia Conference on Information Systems, Langkawi.

Bhatia, S. 2021. *Apple Explains iOS 14.5's App Tracking Transparency in a New Video*. Retrieved from <https://www.iphonehacks.com/2021/04/apple-explain-ios-14-5-app-tracking-transparency.html>

Boiger, M. 2008. "Adaptation of International Students in Japan: The Cultural Fit of Control Orientation," published dissertation, University of Konstanz, Germany.

Bolger, N. 1990. "Coping as a Personality Process: a Prospective Study," *Journal of Personality and Social Psychology* (59:3), 525-537.

Bordia, P., Hunt, E., Paulsen, N., Tourish, D., and DiFonzo, N. 2004. "Uncertainty During Organizational Change: Is It All About Control?" *European Journal of Work and Organizational Psychology* (13:3), pp. 345-365.

Boyd, D. M., and Ellison, N. B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13:1), pp. 210-230.

Brandtstädter, J., and Renner, G. 1990. "Tenacious Goal Pursuit and Flexible Goal Adjustment: Explication and Age-Related Analysis of Assimilative and Accommodative Strategies of Coping," *Psychology and Aging* (5:1), pp. 58-67.

- Buchanan, T., Paine, C., Joinson, A. N., and Reips, U. D. 2007. "Development of Measures of Online Privacy Concern and Protection for Use on the Internet," *Journal of the American society for information science and technology* (58:2), pp. 157-165.
- Burns, A. J., Roberts, T. L., Posey, C., and Lowry, P. B. 2019. "The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking," *Information Systems Research* (30:4), pp. 1228-1247.
- Burton-Jones, A. 2009. "Minimizing Method Bias Through Programmatic Research," *MIS Quarterly* (33:3), pp. 445-471.
- Califf, C. B., Sarker, S., and Sarker, S. 2020. "The Bright and Dark Sides of Technostress: A Mixed-Methods Study Involving Healthcare IT," *MIS Quarterly* (44:2), pp. 809-856.
- Cannon, W. B. 1929. "Organization for Physiological Homeostasis," *Physiological Reviews* (9:3), pp. 399-431.
- Campbell 2021. *Twitter Politely Asks You to Protect its Targeted Ad Dollars in New iOS 14.5 Prompt*. Retrieved from <https://www.theverge.com/2021/5/14/22436944/twitter-ad-tracking-ios-14-5-app-transparency>
- Cavazza, N., Guidetti, M., and Pagliaro, S. 2015. "Who Cares for Reputation? Individual Differences and Concern for Reputation," *Current Psychology* (34:1), pp. 164-176.
- Chen, G., Gully, S. M., and Eden, D. 2001. "Validation of a New General Self-Efficacy Scale," *Organizational Research Methods* (4:1), pp. 62-83.
- Chen, H. T. 2018. "Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management," *American Behavioral Scientist*, (62:10), pp. 1392-1412.
- Chen, L., Xu, P., and Liu, D. 2020. Effect of Crowd Voting on Participation in Crowdsourcing Contests," *Journal of Management Information Systems* (37:2), pp. 510-535.

- Chipperfield, J. G., Perry, R. P., and Menec, V. H. 1999. "Primary and Secondary Control-Enhancing Strategies: Implications for Health in Later Life," *Journal of Aging and Health* (11:4), pp. 517-539.
- Chipperfield, J. G., and Perry, R. P. 2006. "Primary and Secondary Control Strategies in Later Life: Predicting Hospital Outcomes in Men and Women," *Health Psychology* (25:2), pp. 226-236.
- Clover J. 2020. *Apple Confirms Commitment to App Tracking Transparency in Letter Condemning Facebook's Data Collection [Updated]*. Retrieved from <https://www.macrumors.com/2020/11/19/apple-app-tracking-transparency-letter/>
- Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.
- Confessore and Kang 2018. *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites*. Retrieved from <https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html>
- Confessore N. 2018. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" Retrieved from: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- Costello, A., and Osborne, J. 2005. "Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most from Your Analysis," *Practical Assessment Research and Evaluation* (10:7), pp. 1-9.
- Crossler, R. E., and Bélanger, F. 2019. "Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge-Belief Gap," *Information Systems Research* (30:3), pp. 995-1006.
- Culnan, M. J. 1993. "'How Did They Get my Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341-363.



- Culnan, M. J., and Armstrong, P. K. (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.
- De Hert, P. 2008. "Identity Management of e-ID, Privacy and Security in Europe. A Human Rights View," *Information Security Technical Report* (13:2), pp. 71-75.
- DePaulo, B. M., Kashy, D. A., Kirkendol, S. E., Wyer, M. M., and Epstein, J. A. 1996. "Lying in Everyday Life," *Journal of Personality and Social Psychology* (70:5), pp. 979-995.
- Diamantopoulos, A. 2011. "Incorporating Formative Measures into Covariance-Based Structural Equation Models," *MIS Quarterly* (35:2), pp. 335-358.
- Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and their Antecedents Measurement Validity and a Regression Model," *Behaviour and Information Technology* (23:6), pp. 413-422.
- Dinev, T., and Hart, P. 2005. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce* (10:2), pp. 7-29.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.
- Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* (26:4), pp. 639-655.
- Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts," *European Journal of Information Systems* (22:3), pp. 295-316.
- Duncan, O. D. 1969. "Some Linear Models for Two-Wave, Two-Variable Panel Analysis," *Psychological Bulletin* (72:3), pp. 177-182.
- Edison Research, 2019. *The Infinite Dial 2019*. Retrieved from <https://www.edisonresearch.com/the-social-habit-2019/>

Edison Research, 2022. *The Infinite Dial 2022*. Retrieved from <https://www.edisonresearch.com/the-infinite-dial-2022/>

Ejova, A., Delfabbro, P. H., and Navarro, D. J. 2010. "The Illusion of Control: Structure, Measurement and Dependence on Reinforcement Frequency in the Context of a Laboratory Gambling Task." In *ASCS09: Proceedings of the 9th Conference of the Australasian Society for Cognitive Science*.

Endler, N. S., Speer, R. L., Johnson, J. M., and Flett, G. L. 2001. "General Self-Efficacy and Control in Relation to Anxiety and Cognitive Performance," *Current Psychology* (20:1), pp. 36-52.

Essau, C. A., and Trommsdorff, G. 1996. "Coping with University-Related Problems: A Cross-Cultural Comparison," *Journal of Cross-Cultural Psychology* (27:3), pp. 315-328.

Facebook 2020a. *How do I Control Who Can See What's on my Facebook Profile and Timeline?*

Retrieved from <https://www.facebook.com/help/167941163265974>

Facebook 2020b. *What names are allowed on Facebook?*

Retrieved from <https://www.facebook.com/help/112146705538576>

Fadler, M., and Legner, C. 2021. "Data Ownership Revisited: Clarifying Data Accountabilities in Times of Big Data and Analytics," *Journal of Business Analytics*, pp. 1-17.

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., and Gruen, R. J. 1986. "Dynamics of a Stressful Encounter: Cognitive Appraisal, Coping, and Encounter Outcomes," *Journal of Personality and Social Psychology* (50:5), pp. 992-1003.

Fornell, C., and Larcker, D. F. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics," *Journal of Marketing Research* (18:3), pp. 382-388.

Fowler 2022. *There is no Scape from Facebook even if You do not Use It*. Retrieved from:

<https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

Frankl, V. E. 1984. *Man's Search for Meaning*. New York, US: Simon and Schuster.

- Freeman, E. H. 2012. "The Telegraph and Personal Privacy: A Historical and Legal Perspective," *EDPACS* (46:6), pp. 9-20.
- Fromm, E. 1968. *The Revolution of Hope, Toward a Humanized Technology*, Vol. 38.
- Gefen, D., and Pavlou, P. 2006. "The Moderating Role of Perceived Regulatory Effectiveness of Online Marketplaces on the Role of Trust and Risk on Transaction Intentions," Paper 81 in *ICIS 2006 Proceedings*. Milwaukee, WI, USA.
- Gefen, D., and Straub, D. W. 2004. "Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services," *Omega* (32:6), pp. 407-424.
- Gefen, D., Rigdon, E. E., and Straub, D. 2011. "Editor's Comments: An Update and Extension to SEM Guidelines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.
- Gould, S. J. 1999. "A Critique of Heckhausen and Schulz's (1995) Life-Span Theory of Control from a Cross-Cultural Perspective," *Psychological Review* (103:6), pp. 597-604.
- Grootenhuis, M. A., and Last, B. F. 2001. "Children with Cancer with Different Survival Perspectives: Defensiveness, Control Strategies, and Psychological Adjustment," *Psycho-Oncology: Journal of the Psychological, Social and Behavioral Dimensions of Cancer* (10:4), pp. 305-314.
- Grootenhuis, M. A., Last, B. F., De Graaf-Nijkerk, J. H., and Van Der Wel, M. 1996. "Secondary Control Strategies Used by Parents of Children with Cancer," *Psycho-Oncology: Journal of the Psychological, Social and Behavioral Dimensions of Cancer* (5:2), pp. 91-102.
- Ha A. 2021. *Apple's App Tracking Transparency Feature Has Arrived — Here's What You Need to Know*. Retrieved from <https://techcrunch.com/2021/04/26/apples-app-tracking-transparency-feature-has-arrived-heres-what-you-need-to-know/>

- Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. "When to Use and How to Report the Results of PLS-SEM," *European Business Review* (31:1), pp. 2-24.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. 1998. "Multivariate Data Analysis Upper Saddle River, NJ: Prentice hall.
- Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed, a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139-152.
- Hall, N. C., Chipperfield, J. G., Perry, R. P., Ruthig, J. C., and Goetz, T. 2006a. "Primary and Secondary Control in Academic Development: Gender-Specific Implications for Stress and Health in College Students," *Anxiety, Stress, and Coping* (19:2), pp. 189-210.
- Hall, N. C., Perry, R. P., Ruthig, J. C., Hladkyj, S., and Chipperfield, J. G. 2006b. "Primary and Secondary Control in Achievement Settings: A Longitudinal Field Study of Academic Motivation, Emotions, and Performance," *Journal of Applied Social Psychology* (36:6), pp. 1430-1470.
- Harter J. and Arora R. 2008. *Social Time Crucial to Daily Emotional Well-Being in U.S.* Retrieved from <https://news.gallup.com/poll/107692/social-time-crucial-daily-emotional-wellbeing.aspx#:~:text=Certainly%2C%20the%20additional%20time%20spent,on%20weekends%20and%20public%20holidays.>
- Haynes, T. L., Heckhausen, J., Chipperfield, J. G., Perry, R. P., and Newall, N. E. 2009. "Primary and Secondary Control Strategies: Implications for Health and Well-Being Among Older Adults," *Journal of Social and Clinical Psychology* (28:2), pp. 165-197.
- Heckhausen, J., and Schulz, R. 1995. "A Life-Span Theory of Control," *Psychological Review* (102:2), pp. 284-304.
- Heiligenstein 2022. *Facebook Data Breacher: Full Timeline through 2022.* Retrieved from: <https://firewalltimes.com/facebook-data-breach-timeline/>

- Henseler, J., Hubona, G., and Ray, P. A. 2016. "Using PLS Path Modeling in New Technology Research: Updated Guidelines," *Industrial Management and Data Systems* (116:1), pp. 2-20.
- Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 115-135.
- Hirschman, A.O. 1970. *Exit, Voice, and Loyalty Responses to Decline in Firms, Organizations, and States*. Cambridge, US: Harvard University Press.
- Hitlin, P., Rainie, L., and Olmstead, K. 2018. *Americans are changing their relationship with Facebook*. Retrieved from <https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>
- Hitlin, P., Rainie, L., and Olmstead, K. 2019. *Facebook Algorithms and Personal Data*. Retrieved from <https://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/>
- Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications*, (9:1), pp. 50-60.
- Hogg, M. A. 2009. "Managing Self-Uncertainty Through Group Identification," *Psychological Inquiry* (20:4), pp. 221-224.
- Hofstede, G. 1980. "Motivation, Leadership, and Organization: Do American Theories Apply Abroad?" *Organizational Dynamics* (9:1), pp. 42-63.
- Hofstede, G. 1984. *Culture's consequences: International differences in work-related values*, New Delhi, India: Sage Publications.
- Holmes A. 2021. *533 Million Facebook Users' Phone Numbers and Personal Data Have Been Leaked Online*, Retrieved from <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>

- Hong, W., Chan, F. K., and Thong, J. Y. 2019. "Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective," *Journal of Business Ethics (June)*, pp. 1-26.
- Hong, W., and Thong, J. Y. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly (37:1)*, pp. 275-298.
- Hooper, D., Coughlan, J.P., and Mullen, M.R. 2008. "Structural Equation Modelling: Guidelines for Determining Model Fit," *Electronic Journal of Business Research Methods (6:1)*, pp. 53-60.
- Hwang, Y. 2005. "Investigating Enterprise Systems Adoption: Uncertainty Avoidance, Intrinsic Motivation, and the Technology Acceptance Model," *European Journal of Information Systems (14:2)*, pp. 150-161.
- Huang, N., Yan, Z., and Yin, H. 2021. "Effects of Online-Offline Service Integration on e-Healthcare Providers: A Quasi-Natural Experiment," *Production and Operations Management (30:8)*, pp. 2359-2378.
- Jepsen, T. 2018. "A New Business in the World: The Telegraph, Privacy, and the US Constitution in the Nineteenth Century," *Technology and Culture (59:1)*, pp. 95-125.
- Ji, L. J., Peng, K., and Nisbett, R. E. 2000. "Culture, Control, and Perception of Relationships in the Environment," *Journal of Personality and Social Psychology (78:5)*, pp. 943-955.
- Jiang, Z., Heng, C. S., and Choi, B. C. 2013. "Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research (24:3)*, pp. 579-595.
- Jung, J., Bapna, R., Ramaprasad, J., and Umyarov, A. 2019. "Love Unshackled: Identifying the Effect of Mobile App Adoption in Online Dating," *MIS Quarterly (43:1)*, pp. 47-72.

- Jung, J. M., and Kellaris, J. J. 2004. "Cross-National Differences in Proneness to Scarcity Effects: The Moderating Roles of Familiarity, Uncertainty Avoidance, and Need for Cognitive Closure," *Psychology & Marketing* (21:9), pp. 739-753.
- Karahanna, E., Xu, S. X., Xu, Y., and Zhang, N. A. 2018. "The Needs–Affordances–Features Perspective for the Use of Social Media," *MIS Quarterly* (42:3), pp. 737-756.
- Kim, H. W., Chan, H. C., and Kankanhalli, A. 2012. "What Motivates People to Purchase Digital Items on Virtual Community Websites? The Desire for Online Self-Presentation," *Information Systems Research* (23:4), pp. 1232-1245.
- Kelly, G. 2020. *The psychology of personal constructs*. London, UK: Routledge.
- Kuem, J., Khansa, L., and Kim, S. S. 2020. "Prominence and Engagement: Different Mechanisms Regulating Continuance and Contribution in Online Communities," *Journal of Management Information Systems* (37:1), pp. 162-190.
- Langer, E. J. 1977. "The Psychology of Chance," *Journal for the Theory of Social Behaviour* (7:2), pp. 185-207.
- Langer, D. A., Chen, E., and Luhmann, J. D. 2005. "Attributions and Coping in Children's Pain Experiences," *Journal of Pediatric Psychology* (30:7), pp. 615-622.
- Lazarus, R. S., and Folkman, S. 1984. *Stress, Appraisal, and Coping*. New York, NY: Springer Publishing Company.
- Leary, M. R., and Kowalski, R. M. 1990. "Impression Management: A Literature Review and Two-Component Model," *Psychological Bulletin* (107:1), pp. 34-47.
- Leetaru, K. 2018. *Facebook as the Ultimate Government Surveillance Tool?* Retrieved from <https://www.forbes.com/sites/kalevleetaru/2018/07/20/facebook-as-the-ultimate-government-surveillance-tool/#4b9932522909>
- Lewis, C. 1930. "Review," *The Journal of Philosophy* (27:1), pp. 14-25.

- Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. A. 2019. "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective," *MIS Quarterly* (43:2), pp. 373-394.
- Lim, K. H., Leung, K., Sia, C. L., and Lee, M. K. 2004. "Is eCommerce Boundary-Less? Effects of Individualism–Collectivism and Uncertainty Avoidance on Internet Shopping," *Journal of International Business Studies* (35:6), pp. 545-559.
- Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), pp. 114-121.
- Liu, Q. B., Liu, X., and Guo, X. 2020. "The Effects of Participating in a Physician-Driven Online Health Community in Managing Chronic Disease: Evidence from Two Natural Experiments," *MIS Quarterly* (44:1), pp. 391-419.
- Lowry, P. B., Cao, J., and Everard, A. 2011. "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *Journal of Management Information Systems* (27:4), pp. 163-200.
- Ma, M., and Agarwal, R. 2007. "Through a Glass Darkly: Information Technology Design, Identity Verification, and Knowledge Contribution in Online Communities," *Information Systems Research* (18:1), pp. 42-67.
- McCrae, R. R. 1984. "Situational Determinants of Coping Responses: Loss, Threat, and Challenge," *Journal of Personality and Social Psychology* (46:4), pp. 919-928.
- Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.



- Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp. 1865-1883.
- Manstead, A. S., and Van Eekelen, S. A. 1998. "Distinguishing Between Perceived Behavioral Control and Self-Efficacy in the Domain of Academic Achievement Intentions and Behaviors," *Journal of Applied Social Psychology* (28:15), pp. 1375-1392.
- Marakas, G., Johnson, R., and Clay, P. F. 2007. "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time," *Journal of the Association for Information Systems*, (8:1), pp. 16-46.
- Mason, R. O. 1986. "Four Ethical Issues of the Information Age," *MIS Quarterly*, (10:1), pp. 5-12.
- Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. 1995. "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM* (38:12), pp. 65-74.
- Miller, C. 2021. *Apple Debuts Humorous New 'Tracked' Ad Promoting iPhone Privacy [Video]*. Retrieved from <https://9to5mac.com/2021/05/20/apple-debuts-humorous-new-tracked-ad-promoting-iphone-privacy-video/>
- Miller, L. E., and Smith, K. L. 1983. "Handling Nonresponse Issues," *Journal of Extension* (21:5), pp. 45-50.
- Miltgen, C. L., and Peyrat-Guillard, D. 2014. "Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries," *European Journal of Information Systems* (23:2), pp. 103-125.
- Mittal, C., and Griskevicius, V. 2014. "Sense of Control Under Uncertainty Depends on People's Childhood Environment: A Life History Theory Approach," *Journal of Personality and Social Psychology* (107:4), pp. 621-637.

- Morling, B. 2000. “‘Taking’ an Aerobics Class in the US and ‘entering’ an Aerobics Class in Japan: Primary and Secondary Control in a Fitness Context” *Asian Journal of Social Psychology* (3:1), pp. 73-85.
- Morling, B., and Evered, S. 2006. “Secondary Control Reviewed and Defined,” *Psychological Bulletin* (132:2), pp. 269-296.
- Morwitz, V. G., and Fitzsimons, G. J. 2004. “The Mere-Measurement Effect: Why Does Measuring Intentions Change Actual Behavior?” *Journal of Consumer Psychology* (14:1-2), pp. 64-74.
- Mulder, J. D., and Hamaker, E. L. 2020. “Three Extensions of the Random Intercept Cross-Lagged Panel Model,” *Structural Equation Modeling: A Multidisciplinary Journal* (28:4), pp. 638-648.
- Newcomb, A. 2018. “A Timeline of Facebook's Privacy Issues — and its Responses,” Retrieved from <https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651>
- Nikas and Isaac 2021. *Facebook Takes the Gloves Off in Feud with Apple*. Retrieved from <https://www.nytimes.com/2020/12/16/technology/facebook-takes-the-gloves-off-in-feud-with-apple.html>
- O’Brien, R. M. 2007. “A Caution Regarding Rules of Thumb for Variance Inflation Factors,” *Quality and Quantity* (41:5), pp. 673-690.
- O’Dea S. 2022. *Smartphone Adoption Rate Worldwide in 2021 and 2025, by Region*. Retrieved from: <https://www.statista.com/statistics/1258906/worldwide-smartphone-adoption-rate-telecommunication-by-region/>
- Oerter, R., Oerter, R., Agostiani, H., Kim, H. O., and Wibowo, S. 1996. “The Concept of Human Nature in East Asia: Etic and Emic Characteristics,” *Culture and Psychology* (2:1), pp. 9-51.
- Orben, A. C., and Dunbar, R. I. 2017. “Social Media and Relationship Development: The Effect of Valence and Intimacy of Posts,” *Computers in Human Behavior* (73), pp. 489-498.

- Origi, G. 2018. *Reputation: What It Is and Why It Matters*. New Jersey, US: Princeton University Press.
- Paulhus, D. L., Robins, R. W., Trzesniewski, K. H., and Tracy, J. L. 2004. "Two Replicable Suppressor Situations in Personality Research," *Multivariate Behavioral Research* (39:2), pp. 303-328.
- Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where are We Now and Where Should We Go?," *MIS Quarterly* (35:4), pp. 977-988.
- Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp. 37-59.
- Piaget, J. 1970. *Piaget's Theory*. In P. H. Mussen (Ed.), *Carmichael's manual of child psychology* (3rd ed., Vol. 2). New York, US: Wiley.
- Pinsonneault, A., and Kraemer, K. 1993. "Survey Research Methodology in Management Information Systems: An Assessment," *Journal of Management Information Systems* (10:2), pp. 75-105.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.
- Pouget, A., Drugowitsch, J., and Kepecs, A. 2016. "Confidence and Certainty: Distinct Probabilistic Quantities for Different Goals," *Nature Neuroscience* (19:3), pp. 366-374.
- R Core Team 2017. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria. URL <https://www.R-project.org/>.
- Raento, M., Oulasvirta, A., and Eagle, N. 2009. "Smartphones: An Emerging Tool for Social Scientists," *Sociological Methods & Research* (37:3), pp. 426-454.

- Ray, S., Danks, N.P., Velasquez Estrada, J.M. 2020. “*seminr: Domain-Specific Language for Building PLS Structural Equation Models*,” R package version 0.7.0.
- Ray, S., Kim, S. S., and Morris, J. G. 2014. “The Central Role of Engagement in Online Communities,” *Information Systems Research*, (25:3), pp. 528-546.
- Rothbaum, F., Weisz, J. R., and Snyder, S. S. 1982. “Changing the World and Changing the Self: A Two-Process Model of Perceived Control,” *Journal of Personality and Social Psychology* (42:1), pp. 5-37.
- Rothermund, K., and Brandstädter, J. 2003. “Coping with Deficits and Losses in Later Life: from Compensatory Action to Accommodation,” *Psychology and Aging* (18:4), pp. 896-905.
- Rosseel Y. 2012. “lavaan: An R Package for Structural Equation Modeling.” *Journal of Statistical Software* (48:2), pp. 1–36. <http://www.jstatsoft.org/v48/i02/>.
- Sasaki, J. Y., and Kim, H. S. 2011. “At the Intersection of Culture and Religion: A Cultural Analysis of Religion's Implications for Secondary Control and Social Affiliation,” *Journal of Personality and Social Psychology* (101:2), pp. 401.
- Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., V., Markku., L, Jan-Erik, and Konty, M. 2012. “Refining the Theory of Basic Individual Values,” *Journal of Personality and Social Psychology* (103:4), pp. 663.
- Seginer, R., Trommsdorff, G., and Essau, C. 1993. “Adolescent Control Beliefs: Cross-Cultural Variations of Primary and Secondary Orientations,” *International Journal of Behavioral Development* (16:2), pp. 243-260.
- Sheeran, P. 2002. “Intention—Behavior Relations: A Conceptual and Empirical Review,” *European Review of Social Psychology* (12:1), pp. 1-36.

- Shipman, F. M., and Marshall, C. C. 2020. "Ownership, Privacy, and Control in the Wake of Cambridge Analytica: The Relationship Between Attitudes and Awareness," *In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-12.
- Shuper, P. A., Sorrentino, R. M., Otsubo, Y., Hodson, G., and Walker, A. M. 2004. "A Theory of Uncertainty Orientation: Implications for the Study of Individual Differences Within and Across Cultures," *Journal of Cross-Cultural Psychology* (35:4), pp. 460-480.
- Sivo, S. A., Saunders, C., Chang, Q., and Jiang, J. J. 2006. "How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research," *Journal of the Association for Information Systems* (7:6), pp. 352-414.
- Smart, B. 1994. *Michael Foucault: critical assessments*. London, UK: Routledge.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.
- Solove, D. J. 2008. *Understanding privacy*, Cambridge, MA: Harvard University Press.
- Son, J. Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.
- Sreenivasan S. 2022. *How to Use Social Media in your Career*. Retrieved from: <https://www.nytimes.com/guides/business/social-media-for-career-and-business>
- Srite, M., and Karahanna, E. 2006. "The Role of Espoused National Cultural Values in Technology Acceptance," *MIS Quarterly* (30:3), pp. 679-704.
- Statista, 2019a. Facebook Distribution of Users in the United States as of August 2019, by Age Group. Retrieved from <https://www.statista.com/statistics/187549/facebook-distribution-of-users-age-group-usa/>

Statista, 2019b. Facebook Distribution of Users in the United States as of August 2019, by Gender.

Retrieved from <https://www.statista.com/statistics/266879/facebook-users-in-the-us-by-gender/>

Statista 2021. *Share of Smartphone Unit Sales to end Users by Vendor from the First Quarter of*

*2016 to Second Quarter of 2021*. Retrieved from <https://www.statista.com/statistics/266220/global-smartphone-market-share-by-vendor-in-2007-and-2008/>

Statista 2022a. *Daily Time Spend on Social Networking by Internet Users Worldwide from 2012 to*

*2022*. Retrieved from <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/>

Statista 2022b. *Device Usage of Facebook Users Worldwide as of January 2022*. Retrieved from

<https://www.statista.com/statistics/377808/distribution-of-facebook-users-by-device/>

Steinhauser, S., Doblinger, C., and Hüsigg, S. 2020. The Relative Role of Digital Complementary

Assets and Regulation in Discontinuous Telemedicine Innovation in European Hospitals,” *Journal of Management Information Systems* (37:4), pp. 1155-1183.

Stets, J. E., and Burke, P. J. 2000. “Identity Theory and Social Identity Theory,” *Social Psychology*

*Quarterly* (63:3), pp. 224-237.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Srite, M. 2002. “Toward a Theory-Based

Measurement of Culture,” *Journal of Global Information Management* (10:1), pp. 13-23.

Swain, S. D., Weathers, D., and Niedrich, R. W. 2008. “Assessing Three Sources of Misresponse to

Reversed Likert Items,” *Journal of Marketing Research* (45:1), pp. 116-131.

Technavio 2022. *Mobile Apps Market by Platform, Application, Revenue Model, and Geography -*

*Forecast and Analysis 2021-2025*. Retrieved from: <https://www.technavio.com/report/mobile-apps-market-industry-analysis>

- Thatcher, J. B., and Perrewe, P. L. 2002. "An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy," *MIS Quarterly* (26:4), pp. 381-396.
- The Economist, 2019. *Facebook Comes Under Fresh Attack for its Data-Privacy Practices*. Retrieved from <https://www.economist.com/business/2019/01/31/facebook-comes-under-fresh-attack-for-its-data-privacy-practices>
- Thompson, D. V., Hamilton, R. W., and Banerji, I. 2020. "The Effect of Childhood Socioeconomic Status on Patience," *Organizational Behavior and Human Decision Processes* (157), pp. 85-102.
- Thompson, F. T., and Levine, D. U. 1997. "Examples of Easily Explainable Suppressor Variables in Multiple Regression Research," *Multiple Linear Regression Viewpoints* (24:1), pp. 11-13.
- Thompson, S. C., Thomas, C., Rickabaugh, C. A., Tantamjarik, P., Otsuki, T., Pan, D., Garcia, B., and Sinar, E. 1998. "Primary and Secondary Control Over Age-Related Changes in Physical Appearance," *Journal of Personality* (66:4), pp. 583-605.
- Trieu, V. H., Burton-Jones, A., Green, P., and Cockcroft, S. 2022. "Applying and Extending the Theory of Effective Use in a Business Intelligence Context," *MIS Quarterly* (46:1), pp. 645-678.
- Trommsdorff, G. 1994. "Future Time Perspective and Control Orientation: Social Conditions and Consequences," In *Psychology of Future Orientation / Z. Zalenski* (ed.). Lublin. Towarzystwo Naukowe KUL, pp. 39-62.
- Trommsdorff, G., and Essau, C. A. 1998. "Japanese and German Adolescents' Control Orientation: A Cross-Cultural Study," in Trommsdorff, Gisela, ed. and others. *Japan in Transition: Sociological and Psychological Aspects*. Lengerich:Pabst Science, pp. 198-211.
- Tyler, T. R., and Cook, F. L. 1984. "The Mass Media and Judgments of Risk: Distinguishing Impact on Personal and Societal Level Judgments," *Journal of Personality and Social Psychology* (47:4), pp. 693-708.

- van den Hoven, Jeroen, Blaauw, Martijn, Pieters, Wolter and Warnier, Martijn, "Privacy and Information Technology". *The Stanford Encyclopedia of Philosophy (Winter 2019 Edition)*, Edward N. Zalta (ed.), Retrieved from <https://plato.stanford.edu/archives/win2019/entries/it-privacy/>.
- Vasalou, A., Joinson, A. N., and Courvoisier, D. 2010. "Cultural Differences, Experience with Social Networks and the Nature of "True Commitment" in Facebook," *International Journal of Human-Computer Studies* (68:10), pp. 719-728.
- Venkatesh, V. 2000. "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research* (11:4), pp. 342-365.
- Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.
- Wang, X., Abdelhamid, M., and Sanders, G. L. 2021. "Exploring the Effects of Psychological Ownership, Gaming Motivations, and Primary/Secondary Control on Online Game Addiction," *Decision Support Systems* (14:4), pp. 113-512.
- Wang, T., Duong, T. D., and Chen, C. C. 2016. "Intention to Disclose Personal Information Via Mobile Applications: A Privacy Calculus Perspective," *International Journal of Information Management* (36:4), pp. 531-542.
- Wasserstein, R. L., and Lazar, N. A. 2016. "The ASA Statement on p-values: Context, Process, and Purpose," *The American Statistician* (70:2), pp. 129-133.
- Weisz, J. R., Rothbaum, F. M., and Blackburn, T. C. 1984. "Standing Out and Standing In: The Psychology of Control in America and Japan," *American Psychologist* (39:9), pp. 955-969.



- Weisz, J. R., McCabe, M. A., and Dennig, M. D. 1994. "Primary and Secondary Control Among Children Undergoing Medical Procedures: Adjustment as a Function of Coping Style," *Journal of Consulting and Clinical Psychology* (62:2), pp. 324-332.
- Westin A. 1967. *Privacy and Freedom*. New York, US: Ig Publishing.
- White, R. W. 1959. "Motivation Reconsidered: The Concept of Competence," *Psychological Review* (66:5), pp. 297.
- Whitley, E. A. 2009. "Informational Privacy, Consent and the "Control" of Personal Data," *Information Security Technical Report* (14:3), pp. 154-159.
- Whitman, J. Q. 2004. *The Two Western Cultures of Privacy: Dignity Versus Liberty*. 113 Yale LJ.
- Wisniewski, P., Knijnenburg, B. P., and Lipford, H. R. 2014. "Profiling Facebook Users Privacy Behaviors," *In SOUPS2014 Workshop on Privacy Personas and Segmentation*.
- Wrosch, C., Schulz, R., and Heckhausen, J. 2002. "Health Stresses and Depressive Symptomatology in the Elderly: The Importance of Health Engagement Control Strategies," *Health Psychology* (21:4), pp. 340-348.
- Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798-824.
- Xu, H., Teo, H. H., Tan, B. C., and Agarwal, R. 2012. "Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp. 1342-1363.
- Yoo, B., Donthu, N., and Lenartowicz, T. 2011. "Measuring Hofstede's Five Dimensions of Cultural Values at the Individual Level: Development and Validation of CVSCALE," *Journal of International Consumer Marketing* (23:3-4), pp. 193-210.

Yu, T. F. L. 2001. "Entrepreneurial Alertness and Discovery," *The Review of Austrian Economics* (14:1), pp. 47-63.

Zablah, A. R., Carlson, B. D., Donavan, D. T., Maxham III, J. G., and Brown, T. J. 2016. "A Cross-Lagged Test of the Association between Customer Satisfaction and Employee Job Satisfaction in a Relational Context," *Journal of Applied Psychology* (101:5), pp. 1-13.

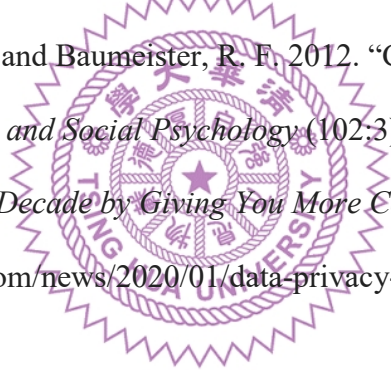
Zemba, Y., Young, M. J., and Morris, M. W. 2006. "Blaming Leaders for Organizational Accidents: Proxy Logic in Collective-Versus Individual-Agency Cultures," *Organizational Behavior and Human Decision Processes* (101:1), pp. 36-51.

Zhang, N. A., Wang, C. A., Karahanna, E., and Xu, Y. 2022. "Peer Privacy Concern: Conceptualization and Measurement," *MIS Quarterly* (46:1). pp. 491-530.

Zhou, X., He, L., Yang, Q., Lao, J., and Baumeister, R. F. 2012. "Control Deprivation and Styles of Thinking," *Journal of Personality and Social Psychology* (102:3), pp. 460-478.

Zuckerberg M. 2020. "Starting the Decade by Giving You More Control Over Your Privacy".

Retrieved from: <https://about.fb.com/news/2020/01/data-privacy-day-2020/>



# Appendices

## Appendix A: Survey Items – Study 1

**Table A1: Survey Items**

| ANTECEDENTS   |       |   |
|---|-------|---|
| <b>SNS Self-Efficacy</b><br><i>(Chen et al. 2001)</i>   | SEFF1 | I believe I can succeed at using most any feature on Facebook to which I set my mind.   |
|   | SEFF2 | I will be able to successfully overcome any challenge of using Facebook's features.   |
|   | SEFF3 | I am confident that I can perform effectively on many different features related to Facebook.   |
|   | SEFF4 | Compared to other people, I can use most features very well on Facebook.  |
| <b>SNS Regulation</b><br><i>(Gefen and Pavlou 2006)</i>   | REG1  | I am confident that the government or market can be effective in enforcing mechanisms to protect user's privacy on platforms like Facebook.     |
|   | REG2  | I believe that the government or market are effective in helping resolving privacy violation conflicts on platforms like Facebook.              |
|   | REG3  | I believe that the government or market are effective authority that assures privacy protection on platforms like Facebook.                     |
|   | REG4  | I believe that the government or market can act effectively in certifying appropriate privacy protection on platforms like Facebook.            |
| <b>Uncertainty Avoidance</b><br><i>(Yoo et al. 2011)</i>  | UNA1  | It is important to have instructions spelled out in detail.   |
|   | UNA2  | It is important to closely follow instructions and procedures.  |
|   | UNA3  | Rules/regulations are important to me.  |
| <b>Collectivism</b><br><i>(Yoo et al. 2011)</i>   | COL1* | Individuals should stick with their group even through difficulties.  |
|   | COL2  | Group success is more important than individual success.  |
|   | COL3  | Individuals should only pursue their goals after considering the welfare of the group.  |
| <b>General Privacy Risk Awareness</b><br><i>(Malhotra et al. 2004)</i>  | RISK1 | In general, it could be risky for people to put personal information on Facebook.   |
|   | RISK2 | There would be high potential for privacy loss associated with putting personal information on Facebook.  |
|   | RISK3 | People's personal information available on Facebook could be inappropriately used.  |
|   | RISK4 | Putting personal information on Facebook could bring people unexpected problems.  |
| INFORMATION PRIVACY CONCERN   |       |   |
| <b>Secondary Use</b><br><i>(Smith et al. 1996)</i>  | SUS1  | I am concerned that Facebook may sell my personal preferences and information to other companies.   |
|   | SUS2  | When I give my preferences or information to Facebook for the use of its services, I am concerned it may use my information for other purposes. |
| <b>Unauthorized Access</b><br><i>(Smith et al. 1996)</i>  | SUS3  | I am concerned that Facebook may share my preferences and information with other parties without getting my authorization.                      |
|   | UAA1  | I am concerned that Facebook may not devote enough time and effort to preventing unauthorized access to my information or posts.                |
|   | UAA2  | I am concerned that Facebook's data that contains my personal information may not be well protected from unauthorized access.                   |
| <b>Collection</b><br><i>(Smith et al. 1996)</i>   | UAA3  | I am concerned that Facebook may not take measures to prevent unauthorized access to my personal information.                                   |
|   | CLL1* | When I'm asked for personal information on Facebook, I sometimes think twice before providing it.   |
|   | CLL2* | It bothers me to put my personal information on Facebook.   |
|   | CLL3  | I am concerned that Facebook is collecting too much personal information about me.  |
| PRIVACY CONTROLS  |       |   |
| <b>Primary Privacy Control</b><br><i>(Hall et al. 2006 and Thompson et al. 1998)</i>                            | PPC1  | I like to know what key things to do to prevent my information on Facebook being seen by the wrong person.                                      |
|   | PPC2  | I like to understand how Facebook works so I can choose who sees which things about me.   |
|   | PPC3* | I can see myself having privacy problems on Facebook, so I like to have strategies to use it appropriately.                                     |
|   | PPC4  | No matter what Facebook does with my information, I like to take steps to keep my privacy safe.   |
|   | PPC5  | I like to understand how to tweak settings and preferences to make sure my privacy stays safe on Facebook.                                      |
| <b>Secondary Privacy Control</b><br><i>(Hall et al. 2006; Thompson et al. 1998 and Grootenhuis et al. 1996)</i> | SPC1* | Although there might be privacy issues with using Facebook, I assume everything will turn out just fine while I use it.                         |
|   | SPC2  | It is better to accept any privacy issues of using Facebook rather than trying to fight it.   |
|   | SPC3* | Despite any privacy issues on Facebook, I try to focus on the benefits of using it.   |
|   | SPC4  | When it comes to privacy issues on Facebook, I think it's better to just wait and see how things turn out.                                      |
|   | SPC5  | Whatever privacy issues there are on Facebook, things will work out for the best anyway.  |
|   | SPC6* | Whatever privacy issues there are on Facebook, there are other things to think about in life.   |
|   | SPC7* | Even if people find out something about me on Facebook I didn't intend them to, it could turn out to be a blessing in disguise.                 |
|   | SPC8* | Eventually, Facebook will have to take privacy seriously, so I don't have to take extra precautions right now.                                  |
| <b>General Privacy Control</b><br><i>(Xu et al. 2012)</i>   | GPC1  | How much control do you feel you have over content and information related to you on Facebook?  |
|   | GPC2  | How much control do you feel you have over the amount of your personal information collected by Facebook?                                       |
|   | GPC3  | How much control do you feel you have over who can get access to your personal information?   |
|   | GPC4  | How much control do you feel you have over how your personal information is being used by Facebook?   |

Items follow a 7-pt scale with 1 as *strongly disagree* and 7 as *strongly agree*, with 4 as *neutral*. \*Removed items after item reliability assessment (CFA).

**Table A1: Survey Items (Continuation)**

| PROTECTIVE INTENTIONS            |        |   |
|----------------------------------|--------|---|
| Distancing                       | DIST1  | In future, I plan to untag or remove mentions from photos or posts on Facebook to protect my privacy.                 |
|                                  | DIST2  | In future, I intend to request friends to take down posts or photos on Facebook to keep myself private.               |
| Intentions                       | DIST3  | In future, I plan to delete contents on my Facebook timeline to hide somethings from others.                          |
|                                  | EXIT1  | In future, I intend to deactivate my Facebook account at some point to maintain my privacy.                           |
| Exit Intentions                  | EXIT2  | In future, I plan to stop using my Facebook account at some point to maintain my privacy.                             |
|                                  | EXIT3  | In future, I will delete my Facebook account at some point, to maintain my privacy.                                   |
| CORRELATES or CONTROL CONSTRUCTS |        |   |
| Subjective Norm                  | NORM1  | I have family, friends or peers who think I should use Facebook to share my personal experiences.                     |
|                                  | NORM2  | People who are important to me think that posting personal experiences on Facebook is the right way to go.            |
| (Venkatesh et al.                | NORM3  | In general, people who are important to me support the use of Facebook to share personal experiences.                 |
| Past Experience                  | PEXP1  | How often have you experienced incidents where your personal information was used by a company without your           |
|                                  | PEXP2  | How often have you been a victim of privacy invasion involving your personal information by a company?                |
| (Xu et al. 2012)                 | PEXP3* | How often have you heard or read during the past year about misuse of personal information of consumers by a company? |

NOTES: Items follow a 7-pt scale with 1 as *strongly disagree* and 7 as *strongly agree*, with 4 as *neutral*. \*Removed items after item reliability assessment (CFA).



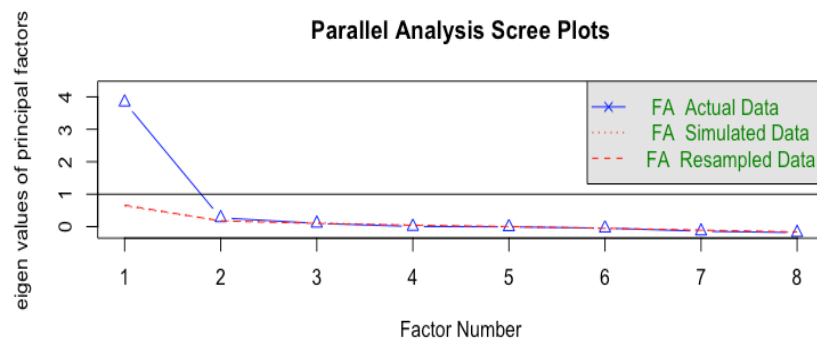
## Appendix B: Exploratory Factor Analysis of Dual Privacy Control

In order to empirically distinguish if the measures of secondary privacy control reflect the four dimensions of secondary control conceptualized by Rothbaum et al. (1982), an exploratory factor analysis (EFA) is needed. The results (Table B1, Figure B1) show that only two factors are captured, as suggested by the number of eigen values higher than 1 and the parallel analysis (Ray et al. 2014). Out of eight items adapted to measure secondary privacy control, three were simultaneously sound with theory and analysis. SPC1, SPC3, and SPC6 seemed to be part of a second factor found by the EFA. Even when SPC7 and SPC8 are part of the first factor, their communality with this factor is very low – 0.37 on average. The remaining items, SPC2, SPC4 and SPC5 all show loadings higher than 0.70 when running a second EFA only on them (Costello and Osborn 2005). Moreover, only these three items could explain about 64.1% of this factor.

**Table B1:** Exploratory Factor Analysis of Secondary Privacy Control

| Factors | Eigen_Values |             | ML1          | ML2           | Communality  | Uniqueness   |                       | ML1   | ML2   |
|---------|--------------|-------------|--------------|---------------|--------------|--------------|-----------------------|-------|-------|
| 1       | 5.258        | SPC1        | 0.088        | 0.741         | 0.660        | 0.340        | SS loadings           | 2.725 | 1.529 |
| 2       | 1.018        | <b>SPC2</b> | <b>0.634</b> | <b>-0.129</b> | <b>0.546</b> | <b>0.454</b> | Proportion Var        | 0.341 | 0.191 |
| 3       | 0.718        | SPC3        | -0.033       | 0.796         | 0.593        | 0.407        | Cumulative Var        | 0.341 | 0.532 |
| 4       | 0.681        | <b>SPC4</b> | <b>0.744</b> | <b>0.061</b>  | <b>0.628</b> | <b>0.372</b> | Proportion Explained  | 0.641 | 0.359 |
| 5       | 0.572        | <b>SPC5</b> | <b>0.898</b> | <b>0.013</b>  | <b>0.324</b> | <b>0.176</b> | Cumulative Proportion | 0.641 | 1.000 |
| 6       | 0.438        | SPC6        | 0.103        | 0.435         | 0.270        | 0.730        |                       |       |       |
| 7       | 0.407        | SPC7        | 0.633        | 0.046         | 0.448        | 0.552        |                       |       |       |
| 8       | 0.357        | SPC8        | 0.667        | -0.185        | 0.285        | 0.715        |                       |       |       |

NOTES: SPC: secondary privacy control. Values in **bold** refer to items selected.



\*Parallel analysis suggests that the number of factors = 2 and the number of components = NA

**Figure B1:** Parallel Analysis of Secondary Privacy Control

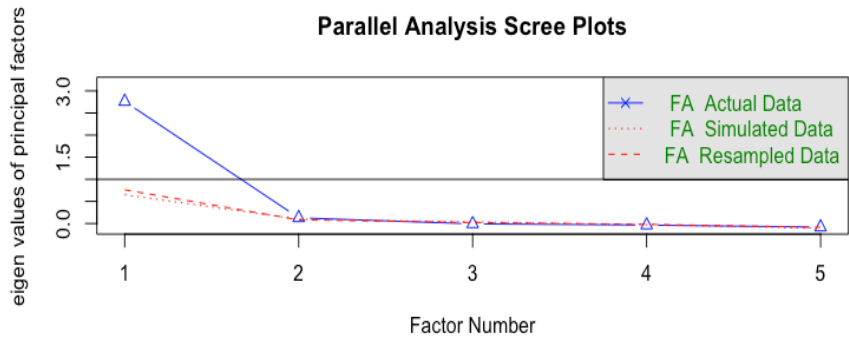
The removed items seemed not to reflect the notion of secondary privacy control. For example, item SPC6 or “*Whatever privacy issues there are on Facebook, there are other things to think about in life*” is ambiguous and could also have been understood by participants as meaning that Facebook privacy issues are not important. In contrast, all retained items conveys exactly the opposite. For example, item SPC5 or “*Whatever privacy issues there are on Facebook, things will work out for the best anyway*” clearly acknowledges the importance of privacy issues. Thus, it is concluded from this empirical and conceptual analysis that secondary privacy control is most faithfully captured by items SPC2, SPC4, and SPC5, which will be used in studies 1 and 2.

Similarly, an EFA was used to find whether primary privacy control was composed of 4 dimensions as proposed by Rothbaum et al. (1982). Table B2 and Figure B2 show that only one factor is captured, as suggested by the number of eigen values higher than 1 and the parallel analysis. Out of five items adapted to measure primary privacy control, four where simultaneously sound with theory and analysis. PPC1, PPC2, PPC4, and PPC5 all showed loadings higher than 0.70 when running a second EFA only on them (Costello and Osborn 2005). Moreover, these four items explained about 55.2 % of this factor’s variance.

**Table B2:** Exploratory Factor Analysis of Primary Privacy Control

| Factors | Eigen_Values |             | ML1          | Communality  | Uniqueness   |                | ML1   |
|---------|--------------|-------------|--------------|--------------|--------------|----------------|-------|
| 1       | 3.178        | <b>PPC1</b> | <b>0.769</b> | <b>0.591</b> | <b>0.409</b> | SS loadings    | 2.759 |
| 2       | 0.692        | <b>PPC2</b> | <b>0.811</b> | <b>0.657</b> | <b>0.343</b> | Proportion Var | 0.552 |
| 3       | 0.478        | PPC3        | 0.532        | 0.283        | 0.717        |                |       |
| 4       | 0.359        | <b>PPC4</b> | <b>0.760</b> | <b>0.577</b> | <b>0.423</b> |                |       |
| 5       | 0.293        | <b>PPC5</b> | <b>0.806</b> | <b>0.650</b> | <b>0.350</b> |                |       |

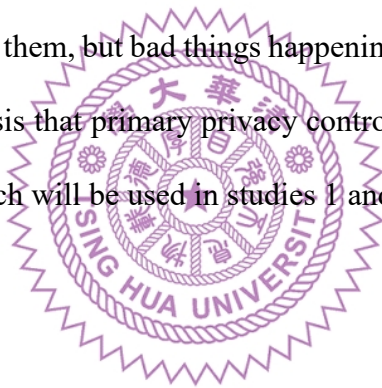
NOTES: PPC: primary privacy control. Values in **bold** refer to items selected.



\*Parallel analysis suggests that the number of factors = 1 and the number of components = NA

**Figure B2:** Parallel Analysis of Primary Privacy Control

The removed item, “*I can see myself having privacy problems on Facebook, so I like to have strategies to use it appropriately*”, might have possibly conveyed participants in this survey that they were not the ones having privacy issues, rather the rest of people, as many psychological studies have suggested. People see good things happening to them, but bad things happening to others. Thus, it is concluded from this empirical and conceptual analysis that primary privacy control is most faithfully captured by items PPC1, PPC2, SPC4, and SPC5, which will be used in studies 1 and 2.



## Appendix C: Non-Response Bias

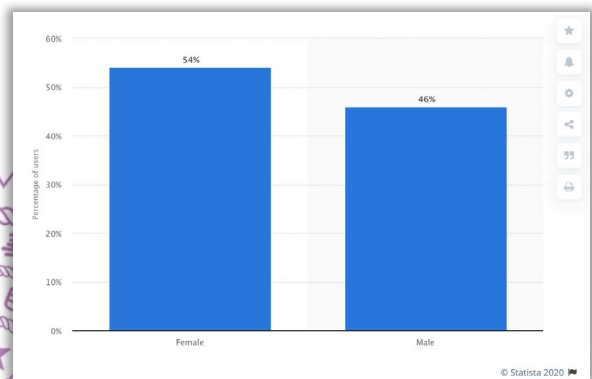
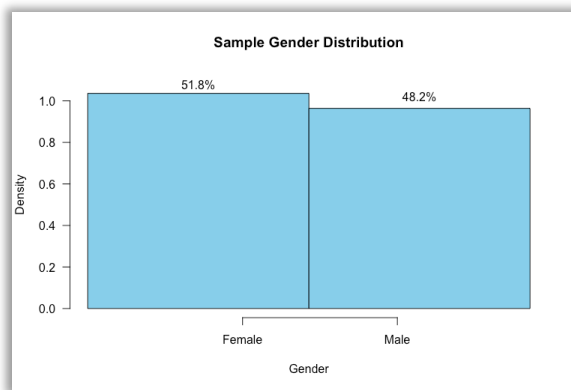
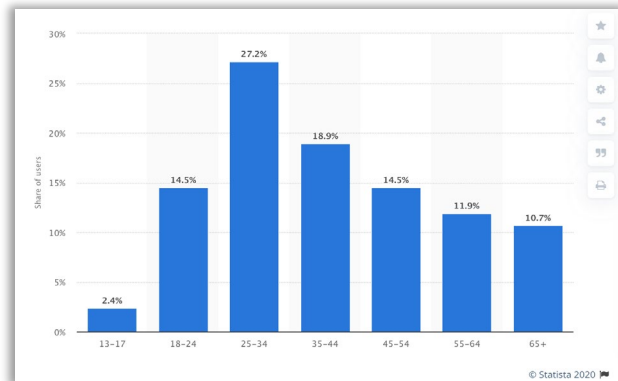
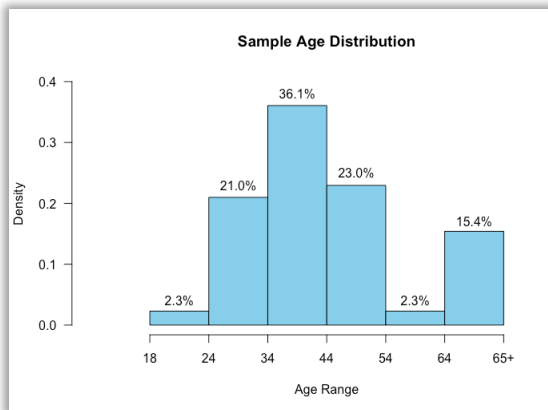
Table C1: First 50 and Last 50 Response Comparison

|       | Meanf50 | Meanl50 | sdf50 | sdl50 | t_stat | p_value |
|-------|---------|---------|-------|-------|--------|---------|
| AGE   | 4.48    | 4.36    | 0.87  | 1.21  | 0.557  | 0.579   |
| GEN   | 0.44    | 0.46    | 0.50  | 0.50  | -0.222 | 0.825   |
| INC   | 4.17    | 3.94    | 1.94  | 2.07  | 0.558  | 0.578   |
| EDU   | 4.46    | 4.68    | 1.60  | 1.72  | -0.660 | 0.511   |
| SELF1 | 5.15    | 5.18    | 1.58  | 1.59  | -0.107 | 0.915   |
| SELF2 | 4.88    | 5.14    | 1.65  | 1.65  | -0.795 | 0.429   |
| SELF3 | 5.50    | 5.44    | 1.34  | 1.47  | 0.211  | 0.833   |
| SELF4 | 4.98    | 5.32    | 1.55  | 1.27  | -1.193 | 0.236   |
| UNA1  | 5.63    | 5.56    | 1.16  | 1.28  | 0.263  | 0.793   |
| UNA2  | 5.83    | 5.66    | 0.97  | 1.41  | 0.706  | 0.482   |
| UNA3  | 5.44    | 5.32    | 1.20  | 1.49  | 0.429  | 0.669   |
| REG1  | 3.71    | 3.26    | 1.84  | 1.75  | 1.236  | 0.220   |
| REG2  | 3.29    | 2.98    | 1.57  | 1.66  | 0.954  | 0.342   |
| REG3  | 3.02    | 2.96    | 1.33  | 1.64  | 0.201  | 0.841   |
| REG4  | 3.52    | 3.30    | 1.70  | 1.64  | 0.653  | 0.515   |
| COL2  | 4.19    | 4.16    | 1.45  | 1.68  | 0.086  | 0.931   |
| COL3  | 3.92    | 4.30    | 1.37  | 1.46  | -1.341 | 0.183   |
| PPC1  | 5.67    | 5.54    | 1.19  | 1.62  | 0.440  | 0.661   |
| PPC2  | 5.48    | 5.46    | 1.20  | 1.73  | 0.063  | 0.950   |
| PPC4  | 5.94    | 5.74    | 1.00  | 1.54  | 0.751  | 0.454   |
| PPC5  | 5.69    | 5.54    | 1.15  | 1.64  | 0.513  | 0.609   |
| SPC2  | 3.52    | 3.52    | 1.79  | 1.75  | 0.002  | 0.998   |
| SPC4  | 3.83    | 3.84    | 1.72  | 1.49  | -0.021 | 0.984   |
| SPC5  | 3.48    | 3.80    | 1.56  | 1.58  | -1.013 | 0.314   |
| RISK1 | 5.67    | 5.90    | 1.49  | 1.23  | -0.845 | 0.400   |
| RISK2 | 5.63    | 5.86    | 1.51  | 1.25  | -0.842 | 0.402   |
| RISK3 | 6.04    | 6.10    | 1.35  | 1.28  | -0.219 | 0.827   |
| RISK4 | 5.83    | 5.76    | 1.49  | 1.30  | 0.259  | 0.796   |
| CLL3  | 5.40    | 5.54    | 1.48  | 1.62  | -0.459 | 0.647   |
| SUS1  | 5.31    | 5.58    | 1.52  | 1.46  | -0.890 | 0.376   |
| SUS2  | 5.46    | 5.40    | 1.22  | 1.58  | 0.204  | 0.839   |
| SUS3  | 5.44    | 5.66    | 1.41  | 1.38  | -0.789 | 0.432   |
| UAA1  | 5.44    | 5.38    | 1.35  | 1.64  | 0.189  | 0.850   |
| UAA2  | 5.56    | 5.52    | 1.41  | 1.59  | 0.139  | 0.889   |
| UAA3  | 5.50    | 5.36    | 1.40  | 1.75  | 0.437  | 0.663   |
| DIST1 | 4.08    | 4.68    | 1.93  | 1.66  | -1.642 | 0.104   |
| DIST2 | 3.71    | 3.96    | 1.90  | 1.89  | -0.656 | 0.513   |
| DIST3 | 4.04    | 4.44    | 1.98  | 1.85  | -1.029 | 0.306   |
| EXIT1 | 3.46    | 3.74    | 1.90  | 1.82  | -0.750 | 0.455   |
| EXIT2 | 3.65    | 3.80    | 2.05  | 1.84  | -0.392 | 0.696   |
| EXIT3 | 3.52    | 3.56    | 2.05  | 1.79  | -0.101 | 0.920   |
| SUB1  | 4.67    | 5.04    | 1.59  | 1.69  | -1.126 | 0.263   |
| SUB2  | 5.04    | 4.86    | 1.56  | 1.63  | 0.564  | 0.574   |
| SUB3  | 5.04    | 5.12    | 1.54  | 1.53  | -0.252 | 0.802   |
| PEXP1 | 3.25    | 4.08    | 1.41  | 1.60  | -2.721 | 0.008   |
| PEXP2 | 2.92    | 3.56    | 1.57  | 1.81  | -1.878 | 0.063   |

NOTES: MEAN: the construct mean; SD: the construct standard deviation; SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. f50: first 50 responses; l50: last 50 responses. Path significances: Item numbers go after the construct abbreviation (i.e., SPC2 is item 2 of secondary privacy control). *Italicized* values are significant.



## Appendix D: Sample vs. Population Demographics Compared



**NOTES:** Sample (light blue) and population (blue) distribution comparisons of age (top) and gender (bottom). Figures on the right taken from Statista 2019a,b

**Figure D1: Sample vs. Population Age and Gender Compared**

# Appendix E: Confirmatory Factor Analysis – CFA and Principal Component Analysis – PCA

**Table E1: Confirmatory Factor Analysis**

| ITEM          | Std.est. 1 | Std.est. 2 | se    | t-value | $\alpha = 0.05$ |       | $\alpha = 0.01$ |       | $\alpha = 0.001$ |       |
|---------------|------------|------------|-------|---------|-----------------|-------|-----------------|-------|------------------|-------|
|               |            |            |       |         | Lower           | Upper | Lower           | Upper | Lower            | Upper |
| SEFF -> SELF1 | 0.788      | 0.788      | 0.037 | 0.000   | 0.716           | 0.860 | 0.693           | 0.883 | 0.667            | 0.909 |
| SEFF -> SELF2 | 0.853      | 0.853      | 0.030 | 0.000   | 0.794           | 0.912 | 0.776           | 0.930 | 0.754            | 0.952 |
| SEFF -> SELF3 | 0.936      | 0.936      | 0.016 | 0.000   | 0.905           | 0.968 | 0.895           | 0.978 | 0.883            | 0.989 |
| SEFF -> SELF4 | 0.790      | 0.790      | 0.028 | 0.000   | 0.734           | 0.845 | 0.716           | 0.863 | 0.696            | 0.883 |
| REG -> REG1   | 0.849      | 0.849      | 0.025 | 0.000   | 0.800           | 0.898 | 0.784           | 0.913 | 0.766            | 0.931 |
| REG -> REG2   | 0.919      | 0.919      | 0.018 | 0.000   | 0.883           | 0.954 | 0.872           | 0.966 | 0.859            | 0.979 |
| REG -> REG3   | 0.921      | 0.921      | 0.014 | 0.000   | 0.894           | 0.948 | 0.886           | 0.957 | 0.876            | 0.966 |
| REG -> REG4   | 0.889      | 0.889      | 0.019 | 0.000   | 0.852           | 0.927 | 0.840           | 0.938 | 0.826            | 0.952 |
| COL -> COL1   | 0.443      |            |       |         |                 |       |                 |       |                  |       |
| COL -> COL2   | 0.815      | 0.709      | 0.054 | 0.000   | 0.603           | 0.815 | 0.569           | 0.849 | 0.530            | 0.888 |
| COL -> COL3   | 0.746      | 0.866      | 0.054 | 0.000   | 0.761           | 0.972 | 0.727           | 1.005 | 0.689            | 1.044 |
| UNA -> UNA1   | 0.757      | 0.757      | 0.057 | 0.000   | 0.645           | 0.868 | 0.610           | 0.903 | 0.569            | 0.944 |
| UNA -> UNA2   | 0.921      | 0.922      | 0.033 | 0.000   | 0.856           | 0.987 | 0.836           | 1.008 | 0.811            | 1.032 |
| UNA -> UNA3   | 0.705      | 0.705      | 0.051 | 0.000   | 0.604           | 0.805 | 0.572           | 0.837 | 0.535            | 0.874 |
| SPC -> SPC2   | 0.749      | 0.748      | 0.038 | 0.000   | 0.673           | 0.823 | 0.649           | 0.847 | 0.622            | 0.874 |
| SPC -> SPC4   | 0.778      | 0.779      | 0.034 | 0.000   | 0.713           | 0.845 | 0.692           | 0.866 | 0.668            | 0.891 |
| SPC -> SPC5   | 0.912      | 0.912      | 0.021 | 0.000   | 0.870           | 0.954 | 0.857           | 0.967 | 0.841            | 0.982 |
| PPC -> PPC1   | 0.775      | 0.776      | 0.053 | 0.000   | 0.671           | 0.881 | 0.638           | 0.914 | 0.599            | 0.952 |
| PPC -> PPC2   | 0.810      | 0.811      | 0.040 | 0.000   | 0.733           | 0.889 | 0.708           | 0.914 | 0.680            | 0.943 |
| PPC -> PPC4   | 0.764      | 0.763      | 0.044 | 0.000   | 0.676           | 0.849 | 0.649           | 0.877 | 0.617            | 0.909 |
| PPC -> PPC5   | 0.797      | 0.797      | 0.043 | 0.000   | 0.712           | 0.881 | 0.686           | 0.908 | 0.654            | 0.939 |
| RISK -> RISK1 | 0.877      | 0.877      | 0.027 | 0.000   | 0.824           | 0.929 | 0.808           | 0.946 | 0.788            | 0.965 |
| RISK -> RISK2 | 0.881      | 0.880      | 0.028 | 0.000   | 0.826           | 0.935 | 0.808           | 0.953 | 0.788            | 0.973 |
| RISK -> RISK3 | 0.848      | 0.849      | 0.034 | 0.000   | 0.782           | 0.915 | 0.761           | 0.936 | 0.737            | 0.960 |
| RISK -> RISK4 | 0.849      | 0.849      | 0.036 | 0.000   | 0.779           | 0.919 | 0.756           | 0.942 | 0.731            | 0.968 |
| PCON -> SUS1  | 0.827      | 0.838      | 0.031 | 0.000   | 0.777           | 0.900 | 0.757           | 0.919 | 0.735            | 0.942 |
| PCON -> SUS2  | 0.888      | 0.894      | 0.024 | 0.000   | 0.847           | 0.942 | 0.832           | 0.957 | 0.814            | 0.974 |
| PCON -> SUS3  | 0.845      | 0.857      | 0.033 | 0.000   | 0.792           | 0.922 | 0.772           | 0.943 | 0.748            | 0.967 |
| PCON -> UAA1  | 0.800      | 0.799      | 0.032 | 0.000   | 0.736           | 0.863 | 0.716           | 0.883 | 0.692            | 0.906 |
| PCON -> UAA2  | 0.861      | 0.862      | 0.030 | 0.000   | 0.804           | 0.920 | 0.786           | 0.938 | 0.765            | 0.960 |
| PCON -> UAA3  | 0.872      | 0.868      | 0.025 | 0.000   | 0.820           | 0.917 | 0.804           | 0.933 | 0.786            | 0.951 |
| PCON -> CLL1  | 0.632      |            |       |         |                 |       |                 |       |                  |       |
| PCON -> CLL2  | 0.648      |            |       |         |                 |       |                 |       |                  |       |
| PCON -> CLL3  | 0.789      | 0.770      | 0.031 | 0.000   | 0.710           | 0.830 | 0.691           | 0.849 | 0.669            | 0.871 |
| DIST -> DIST1 | 0.877      | 0.877      | 0.021 | 0.000   | 0.836           | 0.917 | 0.823           | 0.930 | 0.809            | 0.945 |
| DIST -> DIST2 | 0.837      | 0.836      | 0.027 | 0.000   | 0.783           | 0.890 | 0.766           | 0.907 | 0.746            | 0.926 |
| DIST -> DIST3 | 0.869      | 0.870      | 0.026 | 0.000   | 0.818           | 0.921 | 0.802           | 0.937 | 0.783            | 0.956 |
| EXIT -> EXIT1 | 0.968      | 0.968      | 0.008 | 0.000   | 0.952           | 0.985 | 0.947           | 0.990 | 0.941            | 0.996 |
| EXIT -> EXIT2 | 0.963      | 0.963      | 0.009 | 0.000   | 0.945           | 0.981 | 0.940           | 0.986 | 0.933            | 0.993 |
| EXIT -> EXIT3 | 0.948      | 0.948      | 0.013 | 0.000   | 0.922           | 0.973 | 0.914           | 0.981 | 0.905            | 0.990 |
| NORM -> NORM1 | 0.787      | 0.787      | 0.030 | 0.000   | 0.728           | 0.847 | 0.709           | 0.865 | 0.688            | 0.887 |
| NORM -> NORM2 | 0.908      | 0.908      | 0.026 | 0.000   | 0.856           | 0.959 | 0.840           | 0.976 | 0.821            | 0.995 |
| NORM -> NORM3 | 0.882      | 0.883      | 0.026 | 0.000   | 0.833           | 0.933 | 0.817           | 0.948 | 0.798            | 0.967 |
| PEXP -> PEXP1 | 0.875      | 0.858      | 0.042 | 0.000   | 0.776           | 0.941 | 0.750           | 0.967 | 0.720            | 0.997 |
| PEXP -> PEXP2 | 0.906      | 0.924      | 0.035 | 0.000   | 0.855           | 0.993 | 0.833           | 1.015 | 0.807            | 1.040 |
| PEXP -> PEXP3 | 0.515      |            |       |         |                 |       |                 |       |                  |       |
| AGE -> AGE    | 1.000      | 1.000      | 0.000 |         | 1.000           | 1.000 | 1.000           | 1.000 | 1.000            | 1.000 |
| GEN -> GEN    | 1.000      | 1.000      | 0.000 |         | 1.000           | 1.000 | 1.000           | 1.000 | 1.000            | 1.000 |
| INC -> INC    | 1.000      | 1.000      | 0.000 |         | 1.000           | 1.000 | 1.000           | 1.000 | 1.000            | 1.000 |
| EDU -> EDU    | 1.000      | 1.000      | 0.000 |         | 1.000           | 1.000 | 1.000           | 1.000 | 1.000            | 1.000 |

**Table E2: Principal Component Analysis of Distancing and Exiting Intentions**

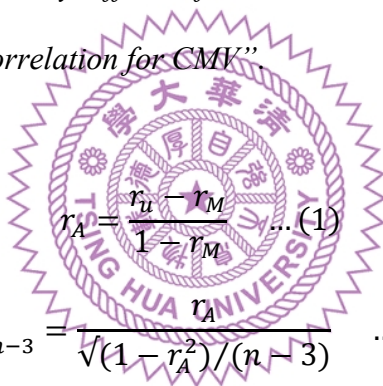
|       | RC1   | RC2   | Communality | Uniqueness |                       | RC1   | RC2   |
|-------|-------|-------|-------------|------------|-----------------------|-------|-------|
| EXIT1 | 0.913 | 0.354 | 0.960       | 0.042      |                       |       |       |
| EXIT2 | 0.891 | 0.390 | 0.950       | 0.056      | SS loadings           | 2.860 | 2.460 |
| EXIT3 | 0.888 | 0.385 | 0.940       | 0.063      | Proportion Var        | 0.480 | 0.410 |
| DIST1 | 0.356 | 0.856 | 0.860       | 0.141      | Cumulative Var        | 0.480 | 0.890 |
| DIST2 | 0.382 | 0.813 | 0.810       | 0.193      | Proportion Explained  | 0.540 | 0.460 |
| DIST3 | 0.419 | 0.801 | 0.820       | 0.183      | Cumulative Proportion | 0.540 | 1.000 |



## Appendix F: Common Method Variance

### Marker Variable Technique

It is expected that single method studies are prone to the inflation of their correlations due to common method variance - CMV (Lindell and Whitney 2001). Given that the proposed model does not include any a priori marker variable, an analysis for CMV where the second-smallest correlation between any two constructs in the correlation matrix is considered a good estimate for the influence of CMV (Malhotra et al. 2006). As provided by Malhotra et al. (2006), the first equation is used to calculate the CMV-adjusted correlation while the second equation examines whether the CMV-adjusted correlation is significantly different from zero. Specifically, these authors write: *“If the level of CMV in the data is low, then  $r_u$  correlations that were significantly different from zero to begin with will continue to be that way, even after researchers adjust that correlation for CMV”*


$$r_A = \frac{r_u - r_M}{1 - r_M} \dots (1)$$
$$t_{\frac{\alpha}{2}, n-3} = \frac{r_A}{\sqrt{(1 - r_A^2)/(n - 3)}} \dots (2)$$

**As Found in Malhotra et a. 2006**

The original correlation matrix and the CMV-adjusted correlation matrix ( $r_M=0.01$ , second smallest correlation value) are compared in terms of the increase or decrease in the number of significant correlations. (Table F1 and Table F2).

**Table F1: Original Correlation Table**

|      | SEFF         | REG          | COL          | UNA          | SPC          | PPC          | RISK         | PCON        | DIST         | EXIT         | NORM        | PEXP        | AGE          | GEN         | INC  | EDU  |
|------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|-------------|--------------|--------------|-------------|-------------|--------------|-------------|------|------|
| SEFF | 1.00         |              |              |              |              |              |              |             |              |              |             |             |              |             |      |      |
| REG  | 0.16         | 1.00         |              |              |              |              |              |             |              |              |             |             |              |             |      |      |
| COL  | <b>0.01</b>  | 0.38         | 1.00         |              |              |              |              |             |              |              |             |             |              |             |      |      |
| UNA  | 0.13         | <b>0.09</b>  | 0.16         | 1.00         |              |              |              |             |              |              |             |             |              |             |      |      |
| SPC  | 0.21         | 0.61         | 0.47         | 0.12         | 1.00         |              |              |             |              |              |             |             |              |             |      |      |
| PPC  | 0.27         | -0.12        | <b>-0.02</b> | 0.51         | <b>-0.01</b> | 1.00         |              |             |              |              |             |             |              |             |      |      |
| RISK | 0.15         | -0.21        | -0.16        | 0.41         | -0.14        | 0.29         | 1.00         |             |              |              |             |             |              |             |      |      |
| PCON | 0.13         | -0.19        | <b>-0.06</b> | 0.30         | -0.22        | 0.46         | 0.45         | 1.00        |              |              |             |             |              |             |      |      |
| DIST | -0.12        | <b>-0.09</b> | <b>0.03</b>  | <b>0.08</b>  | <b>-0.11</b> | <b>0.10</b>  | 0.16         | 0.49        | 1.00         |              |             |             |              |             |      |      |
| EXIT | -0.23        | <b>-0.10</b> | <b>0.03</b>  | <b>0.05</b>  | -0.17        | <b>0.05</b>  | 0.13         | 0.39        | 0.78         | 1.00         |             |             |              |             |      |      |
| NORM | 0.26         | 0.18         | 0.22         | 0.16         | 0.20         | <b>0.09</b>  | 0.13         | <b>0.09</b> | <b>-0.04</b> | <b>-0.03</b> | 1.00        |             |              |             |      |      |
| PEXP | <b>0.08</b>  | 0.18         | 0.25         | <b>0.08</b>  | 0.17         | <b>-0.01</b> | 0.14         | 0.31        | 0.37         | 0.36         | 0.14        | 1.00        |              |             |      |      |
| AGE  | -0.25        | <b>-0.05</b> | -0.12        | 0.13         | <b>-0.07</b> | 0.13         | 0.14         | <b>0.00</b> | <b>-0.10</b> | <b>-0.05</b> | -0.13       | -0.25       | 1.00         |             |      |      |
| GEN  | <b>-0.04</b> | <b>0.05</b>  | 0.17         | <b>-0.01</b> | <b>-0.07</b> | <b>-0.05</b> | <b>0.04</b>  | <b>0.09</b> | 0.17         | 0.20         | <b>0.02</b> | <b>0.05</b> | <b>0.02</b>  | 1.00        |      |      |
| INC  | <b>0.04</b>  | <b>-0.05</b> | <b>0.01</b>  | <b>0.01</b>  | <b>0.06</b>  | <b>0.04</b>  | <b>-0.08</b> | <b>0.08</b> | 0.21         | <b>0.09</b>  | 0.17        | <b>0.03</b> | <b>-0.03</b> | <b>0.09</b> | 1.00 |      |
| EDU  | <b>-0.04</b> | <b>-0.07</b> | <b>0.08</b>  | <b>-0.01</b> | <b>0.04</b>  | <b>-0.04</b> | <b>0.04</b>  | <b>0.09</b> | 0.15         | <b>0.09</b>  | 0.19        | <b>0.09</b> | -0.15        | <b>0.09</b> | 0.33 | 1.00 |

NOTES: SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. Values in **bold** are NOT significant correlations.

**Table F2: CMV-Adjusted Correlation Table**

|      | SEFF         | REG          | COL          | UNA          | SPC          | PPC          | RISK         | PCON        | DIST         | EXIT         | NORM        | PEXP        | AGE          | GEN         | INC  | EDU  |
|------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|-------------|--------------|--------------|-------------|-------------|--------------|-------------|------|------|
| SEFF | 1.00         |              |              |              |              |              |              |             |              |              |             |             |              |             |      |      |
| REG  | 0.16         | 1.00         |              |              |              |              |              |             |              |              |             |             |              |             |      |      |
| COL  | <b>0.01</b>  | 0.38         | 1.00         |              |              |              |              |             |              |              |             |             |              |             |      |      |
| UNA  | 0.13         | <b>0.09</b>  | 0.16         | 1.00         |              |              |              |             |              |              |             |             |              |             |      |      |
| SPC  | 0.21         | 0.61         | 0.47         | <b>0.12</b>  | 1.00         |              |              |             |              |              |             |             |              |             |      |      |
| PPC  | 0.27         | <b>-0.12</b> | <b>-0.02</b> | 0.51         | <b>-0.01</b> | 1.00         |              |             |              |              |             |             |              |             |      |      |
| RISK | 0.15         | -0.21        | -0.16        | 0.41         | -0.14        | 0.29         | 1.00         |             |              |              |             |             |              |             |      |      |
| PCON | 0.13         | -0.19        | <b>-0.06</b> | 0.30         | -0.22        | 0.46         | 0.45         | 1.00        |              |              |             |             |              |             |      |      |
| DIST | <b>-0.12</b> | <b>-0.09</b> | <b>0.03</b>  | <b>0.08</b>  | <b>-0.11</b> | <b>0.10</b>  | 0.16         | 0.49        | 1.00         |              |             |             |              |             |      |      |
| EXIT | -0.23        | <b>-0.10</b> | <b>0.03</b>  | <b>0.05</b>  | -0.17        | <b>0.05</b>  | 0.13         | 0.39        | 0.78         | 1.00         |             |             |              |             |      |      |
| NORM | 0.26         | 0.18         | 0.22         | 0.16         | 0.20         | <b>0.09</b>  | 0.13         | <b>0.09</b> | <b>-0.04</b> | <b>-0.03</b> | 1.00        |             |              |             |      |      |
| PEXP | <b>0.08</b>  | 0.18         | 0.25         | <b>0.08</b>  | 0.17         | <b>-0.01</b> | 0.14         | 0.31        | 0.37         | 0.36         | 0.14        | 1.00        |              |             |      |      |
| AGE  | -0.25        | <b>-0.05</b> | <b>-0.12</b> | 0.13         | <b>-0.07</b> | 0.13         | 0.14         | <b>0.00</b> | <b>-0.10</b> | <b>-0.05</b> | -0.13       | -0.25       | 1.00         |             |      |      |
| GEN  | <b>-0.04</b> | <b>0.05</b>  | 0.17         | <b>-0.01</b> | <b>-0.07</b> | <b>-0.05</b> | <b>0.04</b>  | <b>0.09</b> | 0.17         | 0.20         | <b>0.02</b> | <b>0.05</b> | <b>0.02</b>  | 1.00        |      |      |
| INC  | <b>0.04</b>  | <b>-0.05</b> | <b>0.01</b>  | <b>0.01</b>  | <b>0.06</b>  | <b>0.04</b>  | <b>-0.08</b> | <b>0.08</b> | 0.21         | <b>0.09</b>  | 0.17        | <b>0.03</b> | <b>-0.03</b> | <b>0.09</b> | 1.00 |      |
| EDU  | <b>-0.04</b> | <b>-0.07</b> | <b>0.08</b>  | <b>-0.01</b> | <b>0.04</b>  | <b>-0.04</b> | <b>0.04</b>  | <b>0.09</b> | 0.15         | <b>0.09</b>  | 0.19        | <b>0.09</b> | -0.15        | <b>0.09</b> | 0.33 | 1.00 |

NOTES: SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. Values in **bold** are NOT significant correlations. Values in **blue** are correlations that **BECAME NOT** significant.

As it can be seen from Table F3, common method variance affected some of the associations. Hypothesis 1 described the reasoning behind those users valuing uncertainty avoidance not likely to accept and adjust to the environment; a secondary privacy control orientation. The extraction of CMV made this hypothesis clearer as the correlation between these two constructs became insignificant ( $r=0.12$ ,  $p$ -value=0.053).

Interestingly, the correlations between SNS regulations and primary privacy control and SNS self-efficacy and distancing intentions became insignificant as well ( $r=-0.12$ ,  $p\text{-value}=0.053$ ). Additionally, one correlation regarding the association of age and collectivism also became insignificant. While common method variance has an effect on some of the associations, it does not affect the main hypothesis of the proposed model in this manuscript.

**Table F3:** Original and CMV-Adjusted Proposed Models

|       | Proposed Model |          |           |          |           |       | CMV-Adjusted Proposed Model |           |           |           |           |
|-------|----------------|----------|-----------|----------|-----------|-------|-----------------------------|-----------|-----------|-----------|-----------|
| $R^2$ | PPC            | SPC      | PCON      | DIST     | EXIT      | $R^2$ | PPC                         | SPC       | PCON      | DIST      | EXIT      |
| SEFF  | 0.27 ***       | 0.13 *   |           | -0.18 ** | -0.28 *** | SEFF  | 0.27 ***                    | 0.13 **   |           | -0.18 *** | -0.28 *** |
| REG   | -0.20 **       | 0.49 *** |           |          |           | REG   | -0.20 ***                   | 0.49 ***  |           |           |           |
| UNA   | 0.47 ***       |          |           |          |           | UNA   | 0.47 ***                    |           |           |           |           |
| COL   |                | 0.31 *** |           |          |           | COL   |                             | 0.31 ***  |           |           |           |
| PPC   |                |          | 0.39 ***  | -0.03    |           | PPC   |                             |           | 0.39 ***  | -0.03     |           |
| SPC   |                |          | -0.23 *** |          | -0.08     | SPC   |                             |           | -0.23 *** |           | -0.08 *   |
| RISK  |                |          | 0.27 **   |          |           | RISK  |                             |           | 0.27 ***  |           |           |
| PCON  |                |          |           | 0.44 *** | 0.30 ***  | PCON  |                             |           |           | 0.44 ***  | 0.30 ***  |
| NORM  |                |          |           | -0.11    | -0.04     | NORM  |                             |           |           | -0.11 *   | -0.04     |
| PEXP  |                |          | 0.29 ***  | 0.23 *** | 0.29 ***  | PEXP  |                             |           | 0.29 ***  | 0.23 ***  | 0.29 ***  |
| AGE   | 0.13 *         | 0.03     | -0.03     | -0.09    | -0.05     | AGE   | 0.13 **                     | 0.03      | -0.03     | -0.09     | -0.05     |
| GEN   | -0.03          | -0.15 ** | 0.06      | 0.10     | 0.14 **   | GEN   | -0.03                       | -0.15 *** | 0.06      | 0.10 *    | 0.14 **   |
| INC   | 0.03           | 0.08     | 0.07      | 0.17 **  | 0.07      | INC   | 0.03                        | 0.08      | 0.07      | 0.17 ***  | 0.07      |
| EDU   | -0.03          | 0.05     | 0.05      | 0.03     | 0.00      | EDU   | -0.03                       | 0.05      | 0.05      | 0.03      | 0.00      |

**NOTES:** SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. Path significances: \* $p < 0.05$ ; \*\* $p < 0.01$ ; \*\*\* $p < 0.001$ . Red stars represent an increase in significance. Boxed path estimations represent a change in significance.

The estimated paths on Table F3 above confirms that the levels of common method variance are controllable. Relationships with red stars only show an increase in significance, in contrast to a switch to significance. However, it is worth to note that the effects of the hypothesized relation between secondary privacy control and exit intentions (H8) became significant. Nonetheless, the direction and coefficient are the same.

### Common Method Factor Technique

Following the literature on common method factor analysis (Podsakoff et al. 2003), a factor was created using all the observable variables in the proposed model. After the CFA estimation, the item loadings on

their own construct, and the ones loading on the common factor were used to calculate the average influence of common method variance (Table F4 above).

**Table F4: Common Method Factor Technique**

|       | FACTOR | CMF    | FACTOR <sup>2</sup> | CMF <sup>2</sup> | ERROR |
|-------|--------|--------|---------------------|------------------|-------|
| SELF1 | 0.790  | 0.002  | 0.624               | 0.000            | 0.376 |
| SELF2 | 0.850  | 0.081  | 0.722               | 0.007            | 0.272 |
| SELF3 | 0.936  | 0.044  | 0.875               | 0.002            | 0.123 |
| SELF4 | 0.786  | 0.074  | 0.617               | 0.005            | 0.377 |
| REG1  | 0.841  | -0.136 | 0.706               | 0.019            | 0.275 |
| REG2  | 0.893  | -0.218 | 0.798               | 0.047            | 0.155 |
| REG3  | 0.892  | -0.226 | 0.796               | 0.051            | 0.153 |
| REG4  | 0.870  | -0.184 | 0.757               | 0.034            | 0.209 |
| COL2  | 0.723  | -0.001 | 0.523               | 0.000            | 0.477 |
| COL3  | 0.847  | -0.085 | 0.717               | 0.007            | 0.276 |
| UNA1  | 0.685  | 0.320  | 0.470               | 0.103            | 0.428 |
| UNA2  | 0.871  | 0.304  | 0.758               | 0.093            | 0.149 |
| UNA3  | 0.676  | 0.211  | 0.456               | 0.045            | 0.499 |
| PPC1  | 0.663  | 0.403  | 0.439               | 0.162            | 0.398 |
| PPC2  | 0.724  | 0.391  | 0.524               | 0.153            | 0.324 |
| PPC4  | 0.614  | 0.443  | 0.378               | 0.196            | 0.426 |
| PPC5  | 0.666  | 0.431  | 0.444               | 0.186            | 0.370 |
| SPC2  | 0.708  | -0.225 | 0.501               | 0.051            | 0.448 |
| SPC4  | 0.754  | -0.190 | 0.568               | 0.036            | 0.396 |
| SPC5  | 0.882  | -0.255 | 0.778               | 0.065            | 0.157 |
| SUS1  | 0.422  | 0.759  | 0.178               | 0.576            | 0.246 |
| SUS2  | 0.496  | 0.751  | 0.246               | 0.565            | 0.190 |
| SUS3  | 0.537  | 0.800  | 0.288               | 0.640            | 0.072 |
| UAA1  | -0.051 | 0.752  | 0.003               | 0.565            | 0.432 |
| UAA2  | 0.022  | 0.855  | 0.000               | 0.730            | 0.269 |
| UAA3  | -0.025 | 0.896  | 0.001               | 0.802            | 0.197 |
| CLL3  | 0.124  | 0.921  | 0.015               | 0.849            | 0.136 |
| RISK1 | 0.729  | 0.479  | 0.532               | 0.229            | 0.239 |
| RISK2 | 0.694  | 0.536  | 0.481               | 0.287            | 0.232 |
| RISK3 | 0.733  | 0.438  | 0.537               | 0.192            | 0.270 |
| RISK4 | 0.759  | 0.409  | 0.576               | 0.167            | 0.257 |
| EXIT1 | 0.897  | 0.364  | 0.804               | 0.133            | 0.063 |
| EXIT2 | 0.903  | 0.339  | 0.815               | 0.115            | 0.070 |
| EXIT3 | 0.883  | 0.346  | 0.779               | 0.120            | 0.101 |
| DIST1 | 0.761  | 0.434  | 0.580               | 0.189            | 0.232 |
| DIST2 | 0.772  | 0.342  | 0.597               | 0.117            | 0.287 |
| DIST3 | 0.747  | 0.438  | 0.558               | 0.192            | 0.250 |

**Note:** SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. FACTOR: item loading on its respective factor; CMF: item loading on the common method factor; ERROR: item variance error = 1 - (FACTOR<sup>2</sup> + CMF<sup>2</sup>).

**Table F4: Common Method Factor Technique (Continuation)**

|                | <b>FACTOR</b> | <b>CMF</b> | <b>FACTOR<sup>2</sup></b> | <b>CMF<sup>2</sup></b> | <b>ERROR</b> |
|----------------|---------------|------------|---------------------------|------------------------|--------------|
| <b>NORM1</b>   | 0.756         | 0.253      | 0.571                     | 0.064                  | 0.365        |
| <b>NORM2</b>   | 0.896         | 0.145      | 0.803                     | 0.021                  | 0.176        |
| <b>NORM3</b>   | 0.877         | 0.115      | 0.769                     | 0.013                  | 0.217        |
| <b>PEXP1</b>   | 0.836         | 0.232      | 0.698                     | 0.054                  | 0.248        |
| <b>PEXP2</b>   | 0.875         | 0.264      | 0.766                     | 0.070                  | 0.164        |
| <b>GEN</b>     | -1.000        | 0.028      | 0.999                     | 0.001                  | 0.000        |
| <b>AGE</b>     | 0.999         | 0.033      | 0.999                     | 0.001                  | 0.000        |
| <b>INC</b>     | 0.997         | 0.083      | 0.993                     | 0.007                  | 0.000        |
| <b>EDU</b>     | 0.996         | 0.087      | 0.992                     | 0.008                  | 0.000        |
| <b>AVERAGE</b> |               |            | 0.588                     | 0.173                  | 0.239        |

**Note:** SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. FACTOR: item loading on its respective factor; CMF: item loading on the common method factor; ERROR: item variance error = 1 - (FACTOR<sup>2</sup> + CMF<sup>2</sup>).





## Appendix G: Variance Inflation Factor Values

**Table G1: Variance Inflation Factors**

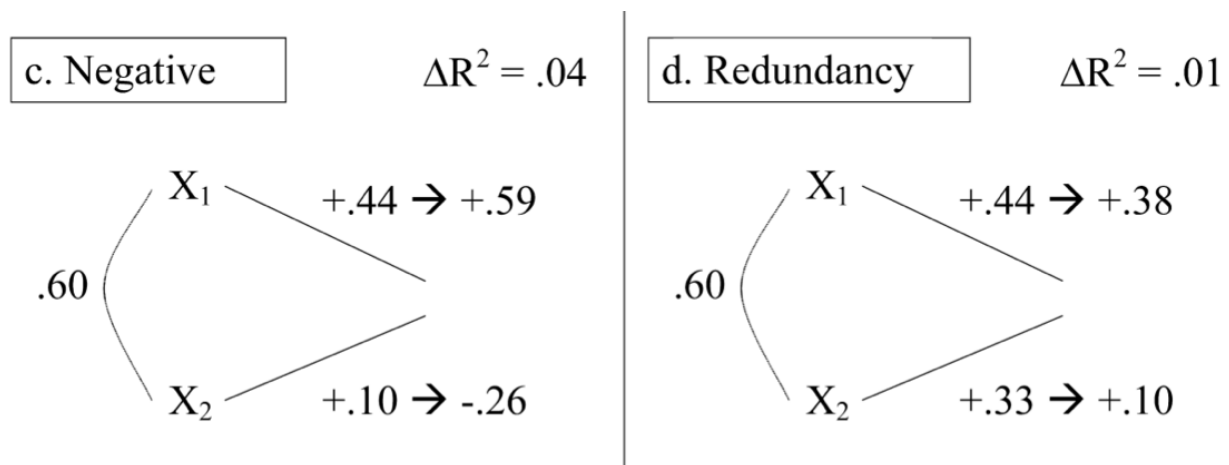
| PPC  |      | SPC  |      | PCON |      | DIST |      | EXIT |      |
|------|------|------|------|------|------|------|------|------|------|
| SEFF | 1.13 | SEFF | 1.11 | PPC  | 1.12 | SEFF | 1.26 | SEFF | 1.22 |
| REG  | 1.04 | REG  | 1.21 | SPC  | 1.07 | PPC  | 1.46 | SPC  | 1.23 |
| UNA  | 1.05 | COL  | 1.23 | RISK | 1.20 | PCON | 1.47 | PCON | 1.28 |
| AGE  | 1.13 | AGE  | 1.11 | PEXP | 1.15 | NORM | 1.15 | NORM | 1.17 |
| GEN  | 1.02 | GEN  | 1.04 | AGE  | 1.14 | PEXP | 1.23 | PEXP | 1.27 |
| INC  | 1.13 | INC  | 1.13 | GEN  | 1.03 | AGE  | 1.22 | AGE  | 1.18 |
| EDU  | 1.16 | EDU  | 1.17 | INC  | 1.15 | GEN  | 1.03 | GEN  | 1.03 |
|      |      |      |      | EDU  | 1.17 | INC  | 1.14 | INC  | 1.15 |
|      |      |      |      |      |      | EDU  | 1.20 | EDU  | 1.20 |

**Note:** SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education.



## Appendix H: Suppression Effects

Figure H1 is borrowed from Paulhus et al. (2004) and includes two types of suppression effects. Figure H2 shows the makings of suppression effect in the proposed model. Primary privacy control is a suppressor construct of information privacy concern of its effects on distancing. This type of suppression is called a negative suppression and is caused by a high existing correlation between both constructs affecting the endogenous construct. Similarly, secondary privacy control is the suppressor construct of the effects of information privacy control on exiting intentions. This type of suppression is better known as a redundancy suppression.



**Figure H1:** Types of Suppression Effects (Paulhus et al. 2004)

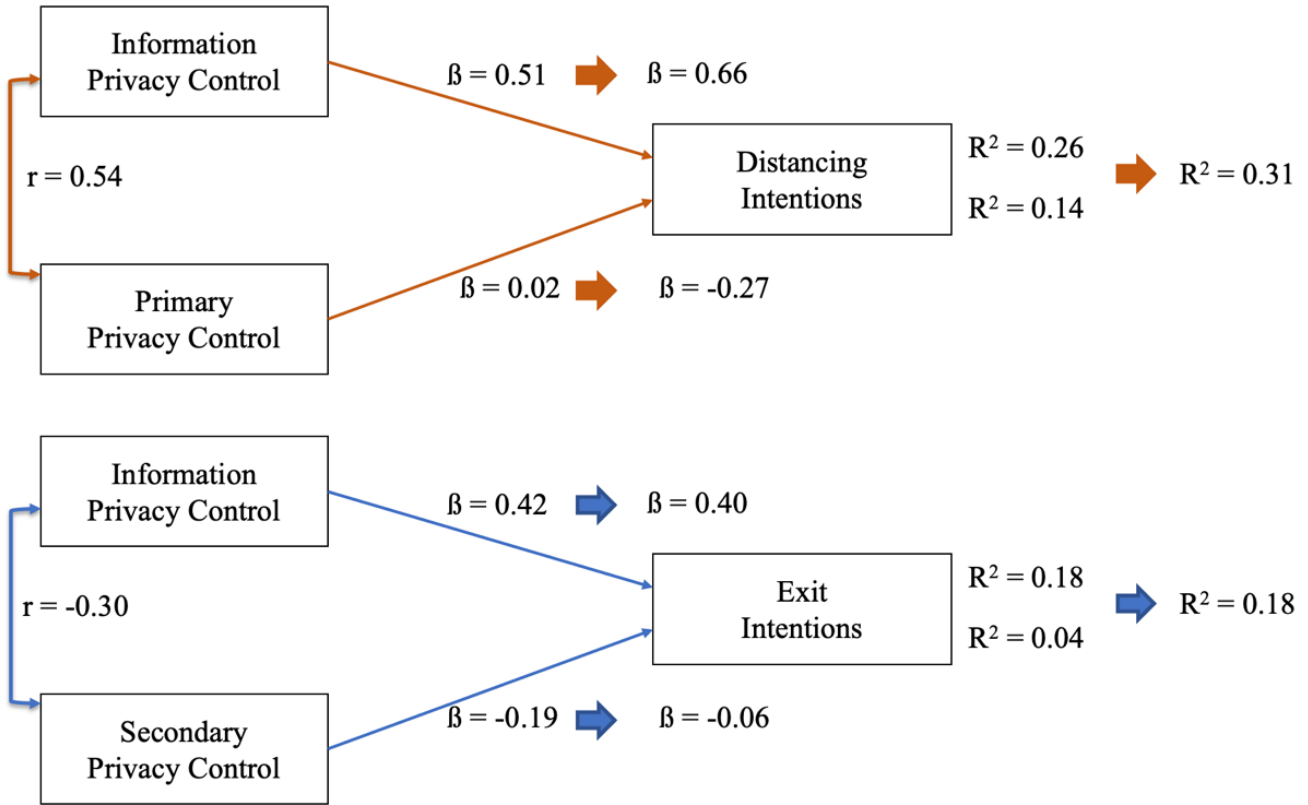
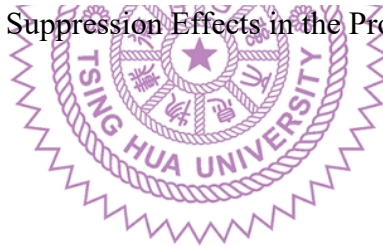


Figure H2: Suppression Effects in the Proposed Model



## **Appendix I: Composite Model Analysis**

### **Assessing the Measurement Model**

The role of secondary privacy control is central to this study, but there are still open questions as how to appropriately measure it within larger causal models. The four postulated aspects of secondary control, namely, interpretive, predictive, illusory, and vicarious, represent different clusters of strategies used by individuals to gain secondary control. But Rothbaum et al. (1982) explicitly recognize that there is much overlap among them. Studies using items from each of the four aspects traditionally construct secondary control by simply composing them together into averages that represent a single construct score (Hall et al. 2006a; Seginer et al. 1993). Hall et al. (2006) suggest that composing is the most appropriate approach given how the four aspects are believed to work together: “... *the composite measure used in this study represents an attempt to provide a better, real-world approximation of the large repertoire of heterogeneous techniques important for adaptation and development in achievement settings*”

Similarly, recent operationalizations of general privacy control in information systems (Dinev and Hart 2004, Xu et. al 2012) have also favored composite modeling either by estimating factor scores or by employing Partial Least Squares Path Modeling (PLS-PM). PLS-PM is a particularly useful technique to test complex theoretical models with pure composite constructs (Benitez-Amado et al. 2017) using weighted sums of items (Henseler et al. 2016).

Thus, PLS-PM is used to facilitate comparison of our results with earlier empirical studies in information systems that favored composite modeling of privacy control, and empirical studies in other fields that used composite modeling of secondary control. For our analysis, we used the SEMinR package (Ray et al. 2020) on the R statistical platform (R Core Team 2017).

### **Measurement Quality**

The quality assessment of the composite measurements of constructs follows recent advances in composite measurement using PLS-PM (Henseler et al. 2016), which require to determine: (a) adequate

face (convergent) validity, or whether each item makes sense in relation to the construct it represents, (b) adequate item contribution to the composite, as indicated by the sign, magnitude, and significance of each item's weight, and (c) item multicollinearity issues.

The meaning and contribution of each measurement to their respective construct was addressed in previous discussion of Operationalizing Secondary Control. Second, most items' weights were positive, and significantly different from zero suggesting adequate contribution of items to composites (Table I1). However, item weights corresponding to SNS normative benefits (NORM) showed diverging directions and not corresponding values, Thus, this construct was considered as a single-item construct using NORM3.



**Table I1: Item Weights and their Significance**

|               | Original Est. | Bootstrap Mean | Bootstrap SD | T Stat. | 2.5% CI | 97.5% CI |
|---------------|---------------|----------------|--------------|---------|---------|----------|
| SELF1 -> SEFF | 0.264         | 0.262          | 0.025        | 10.570  | 0.214   | 0.310    |
| SELF2 -> SEFF | 0.271         | 0.272          | 0.022        | 12.226  | 0.227   | 0.312    |
| SELF3 -> SEFF | 0.335         | 0.333          | 0.019        | 17.375  | 0.299   | 0.373    |
| SELF4 -> SEFF | 0.257         | 0.260          | 0.025        | 10.133  | 0.209   | 0.312    |
| REG1 -> REG   | 0.248         | 0.246          | 0.013        | 19.794  | 0.223   | 0.270    |
| REG2 -> REG   | 0.285         | 0.285          | 0.012        | 23.656  | 0.262   | 0.309    |
| REG3 -> REG   | 0.297         | 0.297          | 0.013        | 23.665  | 0.277   | 0.326    |
| REG4 -> REG   | 0.253         | 0.254          | 0.011        | 23.280  | 0.233   | 0.274    |
| COL2 -> COL   | 0.591         | 0.594          | 0.048        | 12.270  | 0.510   | 0.689    |
| COL3 -> COL   | 0.521         | 0.518          | 0.049        | 10.742  | 0.427   | 0.606    |
| UNA1 -> UNA   | 0.368         | 0.374          | 0.047        | 7.861   | 0.281   | 0.474    |
| UNA2 -> UNA   | 0.432         | 0.430          | 0.032        | 13.383  | 0.368   | 0.493    |
| UNA3 -> UNA   | 0.353         | 0.348          | 0.040        | 8.855   | 0.262   | 0.420    |
| SPC1 -> SPC   | 0.207         | 0.204          | 0.014        | 14.382  | 0.177   | 0.233    |
| SPC2 -> SPC   | 0.189         | 0.189          | 0.013        | 14.421  | 0.164   | 0.218    |
| SPC3 -> SPC   | 0.173         | 0.172          | 0.018        | 9.862   | 0.137   | 0.206    |
| SPC4 -> SPC   | 0.173         | 0.173          | 0.012        | 14.865  | 0.150   | 0.195    |
| SPC5 -> SPC   | 0.225         | 0.223          | 0.012        | 18.782  | 0.202   | 0.247    |
| SPC6 -> SPC   | 0.067         | 0.070          | 0.020        | 3.401   | 0.031   | 0.107    |
| SPC7 -> SPC   | 0.161         | 0.161          | 0.015        | 10.656  | 0.131   | 0.191    |
| SPC8 -> SPC   | 0.135         | 0.135          | 0.021        | 6.390   | 0.092   | 0.177    |
| PPC1 -> PPC   | 0.240         | 0.241          | 0.020        | 12.185  | 0.204   | 0.282    |
| PPC2 -> PPC   | 0.245         | 0.247          | 0.021        | 11.467  | 0.207   | 0.289    |
| PPC3 -> PPC   | 0.231         | 0.230          | 0.027        | 8.626   | 0.173   | 0.285    |
| PPC4 -> PPC   | 0.275         | 0.274          | 0.020        | 13.490  | 0.239   | 0.320    |
| PPC5 -> PPC   | 0.263         | 0.264          | 0.017        | 15.263  | 0.233   | 0.300    |
| RISK1 -> RISK | 0.287         | 0.288          | 0.016        | 18.414  | 0.261   | 0.323    |
| RISK2 -> RISK | 0.322         | 0.323          | 0.024        | 13.298  | 0.287   | 0.375    |
| RISK3 -> RISK | 0.261         | 0.262          | 0.020        | 13.117  | 0.222   | 0.300    |
| RISK4 -> RISK | 0.240         | 0.239          | 0.015        | 15.921  | 0.208   | 0.265    |
| SUS1 -> PCON  | 0.162         | 0.162          | 0.006        | 25.067  | 0.149   | 0.175    |
| SUS2 -> PCON  | 0.174         | 0.175          | 0.006        | 26.794  | 0.162   | 0.187    |
| SUS3 -> PCON  | 0.160         | 0.161          | 0.006        | 25.848  | 0.148   | 0.174    |
| UAA1 -> PCON  | 0.153         | 0.152          | 0.008        | 19.787  | 0.137   | 0.167    |
| UAA2 -> PCON  | 0.165         | 0.165          | 0.006        | 29.613  | 0.155   | 0.177    |
| UAA3 -> PCON  | 0.168         | 0.167          | 0.007        | 24.046  | 0.154   | 0.180    |
| CLL3 -> PCON  | 0.174         | 0.174          | 0.008        | 21.538  | 0.159   | 0.191    |
| DIST1 -> DIST | 0.374         | 0.374          | 0.012        | 30.414  | 0.352   | 0.397    |
| DIST2 -> DIST | 0.358         | 0.357          | 0.015        | 23.725  | 0.331   | 0.388    |
| DIST3 -> DIST | 0.368         | 0.368          | 0.013        | 27.398  | 0.342   | 0.396    |
| EXIT1 -> EXIT | 0.341         | 0.342          | 0.006        | 60.655  | 0.331   | 0.353    |
| EXIT2 -> EXIT | 0.342         | 0.343          | 0.006        | 54.100  | 0.332   | 0.357    |
| EXIT3 -> EXIT | 0.344         | 0.342          | 0.006        | 53.252  | 0.330   | 0.355    |
| NORM1 -> NORM | 1.343         | 0.328          | 0.755        | 1.779   | -1.229  | 1.419    |
| NORM2 -> NORM | -0.124        | 0.273          | 0.242        | -0.511  | -0.329  | 0.663    |
| NORM3 -> NORM | -1.104        | 0.250          | 0.663        | -1.666  | -1.097  | 1.263    |
| PEXP1 -> PEXP | 0.490         | 0.487          | 0.029        | 17.084  | 0.433   | 0.545    |
| PEXP2 -> PEXP | 0.566         | 0.568          | 0.029        | 19.286  | 0.515   | 0.622    |
| AGE -> AGE    | 1.000         | 1.000          | 0.000        | NA      | 1.000   | 1.000    |
| GEN -> GEN    | 1.000         | 1.000          | 0.000        | NA      | 1.000   | 1.000    |
| INC -> INC    | 1.000         | 1.000          | 0.000        | NA      | 1.000   | 1.000    |
| EDU -> EDU    | 1.000         | 1.000          | 0.000        | NA      | 1.000   | 1.000    |

NOTES: SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education.

Finally, multicollinearity between items is assessed with the variance inflation factor (VIF), which is conservatively suggested to be not higher than 5 and more liberally expected to be below 10 (Hair et al. 2011). With few exceptions, all items had small VIF values relative to other items in the construct (Table I2). However, items measuring intention to exit presented VIF values as high as 10.08, although from a conceptual perspective these items represent very different actions, namely, to delete, to stop, and to deactivate the Facebook account. We might have to contend that intention to exit behaves only like a common factor where all items are symptomatic of an underlying concept, rather than as a pure composite, where each item should contribute a distinct meaning. Similarly, one item of information privacy concern, SUS2, had a VIF value of 5.5, but all items of this construct were retained because they have been developed and refined in multiple prior studies and believe this moderately high VIF might be specific to the sample in this study.

**Table I2: Item Variance Inflation Factor Results**

| SEFF       | REG       | UNA       | COL       | SPC       | PPC       | RISK       | PCON      | DIST       | EXIT        | PEXP       |
|------------|-----------|-----------|-----------|-----------|-----------|------------|-----------|------------|-------------|------------|
| SELF1 2.40 | REG1 3.45 | UNA1 2.00 | COL2 1.61 | SPC1 2.12 | PPC1 2.09 | RISK1 3.37 | SUS1 3.50 | DIST1 3.02 | EXIT1 10.08 | PEXP1 2.69 |
| SELF2 3.12 | REG2 4.80 | UNA2 2.55 | COL3 1.61 | SPC2 2.01 | PPC2 2.33 | RISK2 3.34 | SUS2 5.50 | DIST2 2.50 | EXIT2 8.96  | PEXP2 2.69 |
| SELF3 3.92 | REG3 4.75 | UNA3 1.74 |           | SPC3 1.83 | PPC3 1.34 | RISK3 3.00 | SUS3 4.64 | DIST3 2.71 | EXIT3 7.40  |            |
| SELF4 2.36 | REG4 4.19 |           |           | SPC4 2.30 | PPC4 2.04 | RISK4 3.06 | UAA1 3.18 |            |             |            |
|            |           |           |           | SPC5 3.21 | PPC5 2.25 |            | UAA2 4.03 |            |             |            |
|            |           |           |           | SPC6 1.36 |           |            | UAA3 4.31 |            |             |            |
|            |           |           |           | SPC7 1.76 |           |            | CLL3 2.33 |            |             |            |
|            |           |           |           | SPC8 1.33 |           |            |           |            |             |            |

**NOTES:** SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education.

In a composite view, estimating reliability is not necessary because the dimensions of a composite are not expected to cause the construct rather to materially compose it (Benitez-Amado et al. 2017; Henseler et al. 2016). The discriminant validity of each composite was confirmed using the HTMT parameter which makes use of the items' weights instead of loadings (Henseler et al. 2015). HTMT should be significantly smaller than 1.0 because this parameter is an estimation of the correlation between both

constructs (Henseler et al 2015). The HTMT values were all significantly lower than 1.0, which led us to conclude that they are sufficiently different from each other.

### **Common Method Bias in a Composite View - Procedural techniques**

The cross-sectional nature of this study required us to consider the potential influence of common method variance (CMV) in our results. CMV happens as a consequence of measuring variables with a single method (Malhotra et al. 2006) and is attributed to a wide range of different sources (Podsakoff et al. 2003). From the composite measurement perspective, where items are considered material dimensions of the composites they form, procedural controls is the best way to control for CMV because the effects of method variance should be modeled at the construct level rather than at the item level. There are various conceptual and empirical problems to attain proper procedural control (see Podsakoff et al. 2003). The method to rule CMV issues at the study design stage was to separate the commonalities between the predictors and criterion variables (Johnson et al. 2011; Podsakoff et al. 2003). Specifically, we made sure that items for primary privacy control do not contain words such as “worry” because this term conflates with what information privacy concern means. Similarly, phrases such as “*I know what to do*” in the primary privacy control were avoided because they could potentially be measuring SNS self-efficacy.

Self-efficacy and control are recognized as very similar concepts (Ajzen 2002, Bandura 2006, Chen 2018, Compeau and Higgins 1995, Endler 2001). Their commonality seems to be due to their agentic nature (Ajzen 2002). Even Bandura entitled one of his books as: “*Self-Efficacy: The Exercise of Control*” (Bandura 1997) and researchers have questioned their empirical separation (Manstead et al. 1998). In the information systems literature, a well-regarded paper introducing the notion of computer self-efficacy, Compeau and Higgins (1995, p. 191) reads: “*The concept of self-efficacy, while representing a unique perception, is similar to a number of other motivational constructs such as effort-performance expectancy (Porter and Lawler, 1968), locus of control, and self-esteem.*” Consequently, one of the challenges of this and other studies (e.g., Endler et al. 2001) including self-efficacy and control



within the same framework is the right operationalization of both constructs to rule multicollinearity. One way to deal with this issue is the interplay between general and specific operationalizations. For example, in examining the influence of general self-efficacy and perceived control on anxiety and cognitive performance, Endler et al. (2001) operationalize self-efficacy in a general form: *“If I can't do a job the first time, I keep trying until I can”*, and perceptions of control in a specific form: *“How much choice were you given when performing this activity?”* and obtain low correlations between them.

In addition, items were carefully adjusted to avoid similarities among composites and gain proximity separation between constructs. Specifically, we positioned construct measurements in the survey instrument in such a way that two constructs with a causal relationship between them were not together on the same page.

### Structural Results

Before examining the results of the hypothesized paths, the variance inflation factors (VIF) at the construct level were estimated (Table I3). No construct had a value higher than 1.50 in relation to other exogenous constructs, a value not higher than the most conservative threshold of 5 (Hair et al. 2011).

**Table I3:** Composites Variance Inflation Factor Results

| PPC  |      | SPC  |      | PCON |      | DIST |      | EXIT |      |
|------|------|------|------|------|------|------|------|------|------|
| SEFF | 1.12 | SEFF | 1.10 | PPC  | 1.27 | SEFF | 1.20 | SEFF | 1.21 |
| REG  | 1.05 | REG  | 1.15 | SPC  | 1.08 | PPC  | 1.51 | SPC  | 1.32 |
| UNA  | 1.05 | COL  | 1.15 | RISK | 1.33 | PCON | 1.50 | PCON | 1.26 |
| AGE  | 1.12 | AGE  | 1.10 | PEXP | 1.13 | NORM | 1.10 | NORM | 1.17 |
| GEN  | 1.02 | GEN  | 1.03 | AGE  | 1.13 | PEXP | 1.17 | PEXP | 1.20 |
| INC  | 1.13 | INC  | 1.13 | GEN  | 1.03 | AGE  | 1.21 | AGE  | 1.17 |
| EDU  | 1.16 | EDU  | 1.17 | INC  | 1.16 | GEN  | 1.03 | GEN  | 1.03 |
|      |      |      |      | EDU  | 1.17 | INC  | 1.14 | INC  | 1.14 |
|      |      |      |      |      |      | EDU  | 1.18 | EDU  | 1.18 |

**NOTES:** SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefits; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education.

Table I4 shows the proposed model, the general privacy control model and the saturated model that were also estimated using the common factor perspective. Overall, the results are comparable (see “Common-Factor vs. Composite Perspectives” for more details).

**Table I4:** Structural Results of Proposed and Alternative Models – Composite Perspective

|                       | Proposed Model |          |           |          |           | General Privacy Control Model |          |           |           |           | Saturated Model       |          |          |          |          |           |       |
|-----------------------|----------------|----------|-----------|----------|-----------|-------------------------------|----------|-----------|-----------|-----------|-----------------------|----------|----------|----------|----------|-----------|-------|
|                       | PPC            | SPC      | PCON      | DIST     | EXIT      | GPC                           | PCON     | DIST      | EXIT      | PPC       | SPC                   | PCON     | DIST     | EXIT     |          |           |       |
| <i>R</i> <sup>2</sup> | 0.26           | 0.41     | 0.43      | 0.35     | 0.32      | <i>R</i> <sup>2</sup>         | 0.38     | 0.33      | 0.36      | 0.32      | <i>R</i> <sup>2</sup> | 0.26     | 0.42     | 0.45     | 0.36     | 0.34      |       |
| SEFF                  | 0.23 ***       | 0.21 *** |           | -0.14 *  | -0.23 *** | SEFF                          | 0.18 *** |           | -0.19 *** | -0.27 *** | SEFF                  | 0.23 *** | 0.23 *** | -0.02    | -0.14 *  | -0.21 *** |       |
| REG                   | -0.16 **       | 0.45 *** |           |          |           | REG                           | 0.52 *** |           |           |           | REG                   | -0.15 *  | 0.45 *** | -0.11    | 0.07     | 0.08      |       |
| UNA                   | 0.41 ***       |          |           |          |           | UNA                           | -0.05    |           |           |           | UNA                   | 0.41 *** | -0.09    | 0.13 *   | 0.04     | -0.03     |       |
| COL                   |                | 0.24 *** |           |          |           | COL                           | 0.14 *   |           |           |           | COL                   | -0.03    | 0.26 *** | 0.00     | 0.04     | 0.07      |       |
| PPC                   |                |          | 0.36 ***  | -0.09    |           | GPC                           |          | -0.19 *** | 0.11      | 0.07      | PPC                   |          |          | 0.32 *** | -0.12    | -0.11     |       |
| SPC                   |                |          | -0.17 *** |          | -0.07     | RISK                          |          | 0.41 ***  |           |           | SPC                   |          |          | -0.13 *  | -0.04    | -0.13     |       |
| RISK                  |                |          | 0.27 ***  |          |           | PCON                          |          |           | 0.45 ***  | 0.37 ***  | RISK                  |          |          | 0.23 **  | 0.05     | 0.05      |       |
| PCON                  |                |          |           | 0.46 *** | 0.32 ***  | NORM                          |          |           | -0.12 *   | -0.10     | PCON                  |          |          |          | 0.45 *** | 0.37 ***  |       |
| NORM                  |                |          |           | -0.12 *  | -0.08     | PEXP                          |          |           | 0.22 ***  | 0.19 ***  | 0.23 ***              | NORM     |          |          | -0.13 *  | -0.09     |       |
| PEXP                  |                |          | 0.21 ***  | 0.20 *** | 0.24 ***  | AGE                           | 0.06     | 0.00      | -0.10     | -0.07     | PEXP                  |          |          | 0.22 *** | 0.18 *** | 0.22 ***  |       |
| AGE                   | 0.11           | 0.06     | -0.03     | -0.08    | -0.06     | GEN                           | -0.02    | -0.13 **  | 0.05      | 0.09      | 0.14 **               | AGE      | 0.11 *   | 0.08     | -0.04    | -0.08     | -0.04 |
| GEN                   | -0.02          | -0.13 ** | 0.05      | 0.09     | 0.14 **   | INC                           | 0.04     | 0.09 *    | 0.15 *    | 0.06      | GEN                   | -0.01    | -0.13 ** | 0.06     | 0.08     | 0.12 **   |       |
| INC                   | 0.04           | 0.08     | 0.06      | 0.16 **  | 0.06      | EDU                           | 0.02     | 0.01      | 0.03      | 0.00      | INC                   | 0.04     | 0.09     | 0.05     | 0.17 *** | 0.08      |       |
| EDU                   | -0.01          | 0.08     | 0.04      | 0.03     | 0.00      |                               |          |           |           |           | EDU                   | 0.00     | 0.08     | 0.03     | 0.03     | 0.00      |       |

NOTES: SEFF: SNS self-efficacy; REG: SNS regulations; RISK: general privacy risk awareness; SPC: secondary privacy control; PPC: primary privacy control; GPC: general privacy control; PCON: information privacy concern; DIST: distancing intentions; EXIT: exit intentions; NORM: SNS normative benefit; PEXP: past experience with privacy issues; AGE: age; GEN: gender; INC: income; EDU: education. Path significances: \*p < 0.05; \*\*p < 0.01; \*\*\*p < 0.001.



## Appendix J: Survey Items – Study 2 – First Wave

| ANTECEDENTS  |   |
|--|---|
| <b>iPhone Self-Efficacy</b><br>(Chen et al. 2001)  | <b>ISEFF1</b> I believe I can succeed at using most any feature on the iPhone to which I set my mind.   |
|  | <b>ISEFF2</b> I will be able to successfully overcome any challenge of using the iPhone's features.   |
|  | <b>ISEFF3</b> I am confident that I can perform effectively on many different features related to the iPhone.   |
|  | <b>ISEFF4</b> Compared to other people, I can use most features very well on the iPhone.  |
| <b>General Privacy Risk Awareness</b><br>(Malhotra et al. 2004)  | <b>RISK1</b> In general, it could be risky for people to put personal information on Facebook.  |
|  | <b>RISK2</b> There would be high potential for privacy loss associated with putting personal information on Facebook.                                       |
|  | <b>RISK3</b> People's personal information available on Facebook could be inappropriately used.   |
|  | <b>RISK4</b> Putting personal information on Facebook could bring people unexpected problems.   |
| INFORMATION PRIVACY CONCERN  |   |
| <b>Secondary Use</b><br>(Smith et al. 1996)  | <b>SUS1</b> I am concerned that Facebook may sell my personal preferences and information to other companies.   |
|  | <b>SUS2</b> When I give my preferences or information to Facebook for the use of its services, I am concerned it may use my information for other purposes. |
|  | <b>SUS3</b> I am concerned that Facebook may share my preferences and information with other parties without getting my authorization.                      |
| <b>Unauthorized Access</b><br>(Smith et al. 1996)  | <b>UAA1</b> I am concerned that Facebook may not devote enough time and effort to preventing unauthorized access to my information or posts.                |
|  | <b>UAA2</b> I am concerned that Facebook's data that contains my personal information may not be well protected from unauthorized access.                   |
|  | <b>UAA3</b> I am concerned that Facebook may not take measures to prevent unauthorized access to my personal information.                                   |
| <b>Collection</b><br>(Smith et al. 1996)   | <b>CLL1*</b> When I'm asked for personal information on Facebook, I sometimes think twice before providing it.  |
|  | <b>CLL2*</b> It bothers me to put my personal information on Facebook.  |
|  | <b>CLL3</b> I am concerned that Facebook is collecting too much personal information about me.  |
| PRIVACY CONTROLS   |   |
| <b>Primary Privacy Control</b><br>(Hall et al. 2006 and Thompson et al. 1998)                            | <b>PPC1</b> I like to know what key things to do to prevent my information on Facebook being seen by the wrong person.                                      |
|  | <b>PPC2</b> I like to understand how Facebook works so I can choose who sees which things about me.   |
|  | <b>PPC3*</b> I can see myself having privacy problems on Facebook, so I like to have strategies to use it appropriately.                                    |
|  | <b>PPC4</b> No matter what Facebook does with my information, I like to take steps to keep my privacy safe.   |
|  | <b>PPC5</b> I like to understand how to tweak settings and preferences to make sure my privacy stays safe on Facebook.                                      |
| <b>Secondary Privacy Control</b><br>(Hall et al. 2006; Thompson et al. 1998 and Grootenhuis et al. 1996) | <b>SPC1*</b> Although there might be privacy issues with using Facebook, I assume everything will turn out just fine while I use it.                        |
|  | <b>SPC2</b> It is better to accept any privacy issues of using Facebook rather than trying to fight it.   |
|  | <b>SPC3*</b> Despite any privacy issues on Facebook, I try to focus on the benefits of using it.  |
|  | <b>SPC4</b> When it comes to privacy issues on Facebook, I think it's better to just wait and see how things turn out.                                      |
|  | <b>SPC5</b> Whatever privacy issues there are on Facebook, things will work out for the best anyway.  |
|  | <b>SPC6*</b> Whatever privacy issues there are on Facebook, there are other things to think about in life.  |
|  | <b>SPC7*</b> Even if people find out something about me on Facebook I didn't intend them to, it could turn out to be a blessing in disguise.                |
|  | <b>SPC8*</b> Eventually, Facebook will have to take privacy seriously, so I don't have to take extra precautions right now.                                 |
| <b>General Privacy Control</b><br>(Xu et al. 2012)   | <b>GPC1</b> How much control do you feel you have over content and information related to you on Facebook?  |
|  | <b>GPC2</b> How much control do you feel you have over the amount of your personal information collected by Facebook?                                       |
|  | <b>GPC3</b> How much control do you feel you have over who can get access to your personal information?   |
|  | <b>GPC4</b> How much control do you feel you have over how your personal information is being used by Facebook?   |
| CORRELATES or CONTROL CONSTRUCTS   |   |
| <b>Subjective Norm</b><br>(Venkatesh et al. 2003)  | <b>NORM1</b> I have family, friends or peers who think I should use Facebook to share my personal experiences.  |
|  | <b>NORM2</b> People who are important to me think that posting personal experiences on Facebook is the right way to go.                                     |
|  | <b>NORM3</b> In general, people who are important to me support the use of Facebook to share personal experiences.  |
| <b>Past Experience</b><br>(Xu et al. 2012)   | <b>PEXP1</b> How often have you experienced incidents where your personal information was used by a company without your authorization?                     |
|  | <b>PEXP2</b> How often have you been a victim of privacy invasion involving your personal information by a company?   |
|  | <b>PEXP3*</b> How often have you heard or read during the past year about misuse of personal information of consumers by a company?                         |
| <b>Upgrading Autoregressor</b>   | <b>iOSupg</b> On the same settings page ("Settings" > "General" > "About") tell us your "Software Version"  |

Items follow a 7-pt scale with 1 as *strongly disagree* and 7 as *strongly agree*, with 4 as *neutral*. \*Removed items after item reliability assessment (CFA). Upgrading autoregressor is transformed into a dichotomous variable.

## Appendix K: Survey Items – Study 2 – Second Wave

### PRIVACY CONTROLS AND COPING

|  |              |   |
|--|--------------|---|
| <b>Primary Privacy Control</b><br>(Hall et al. 2006 and Thompson et al. 1998)                            | <b>PPC1</b>  | I like to know what key things to do to prevent my information on Facebook being seen by the wrong person.                      |
|  | <b>PPC2</b>  | I like to understand how Facebook works so I can choose who sees which things about me.   |
|  | <b>PPC3*</b> | I can see myself having privacy problems on Facebook, so I like to have strategies to use it appropriately.                     |
|  | <b>PPC4</b>  | No matter what Facebook does with my information, I like to take steps to keep my privacy safe.                                 |
|  | <b>PPC5</b>  | I like to understand how to tweak settings and preferences to make sure my privacy stays safe on Facebook.                      |
| <b>Secondary Privacy Control</b><br>(Hall et al. 2006; Thompson et al. 1998 and Grootenhuis et al. 1996) | <b>SPC1*</b> | Although there might be privacy issues with using Facebook, I assume everything will turn out just fine while I use it.         |
|  | <b>SPC2</b>  | It is better to accept any privacy issues of using Facebook rather than trying to fight it.                                     |
|  | <b>SPC3*</b> | Despite any privacy issues on Facebook, I try to focus on the benefits of using it.   |
|  | <b>SPC4</b>  | When it comes to privacy issues on Facebook, I think it's better to just wait and see how things turn out.                      |
|  | <b>SPC5</b>  | Whatever privacy issues there are on Facebook, things will work out for the best anyway.  |
|  | <b>SPC6*</b> | Whatever privacy issues there are on Facebook, there are other things to think about in life.                                   |
|  | <b>SPC7*</b> | Even if people find out something about me on Facebook I didn't intend them to, it could turn out to be a blessing in disguise. |
|  | <b>SPC8*</b> | Eventually, Facebook will have to take privacy seriously, so I don't have to take extra precautions right now.                  |
| <b>General Privacy Control</b><br>(Xu et al. 2012)   | <b>GPC1</b>  | How much control do you feel you have over content and information related to you on Facebook?                                  |
|  | <b>GPC2</b>  | How much control do you feel you have over the amount of your personal information collected by Facebook?                       |
|  | <b>GPC3</b>  | How much control do you feel you have over who can get access to your personal information?                                     |
|  | <b>GPC4</b>  | How much control do you feel you have over how your personal information is being used by Facebook?                             |
| <b>Privacy Wishful Thinking</b><br>(Liang et al. 2019)   | <b>WISH1</b> | I fantasize that privacy issues on Facebook will go away or somehow I will be over with.  |
|  | <b>WISH2</b> | I fantasize that I would somehow come across a magical solution for privacy issues on Facebook.                                 |
|  | <b>WISH3</b> | I fantasize that all of a sudden privacy issues on Facebook will disappear by themselves.                                       |
|  | <b>WISH4</b> | I fantasize that everything will turn out just fine as if privacy issues on Facebook never happened.                            |
| <b>PROTECTIVE INTENTIONS</b>   |              |   |
| <b>Distancing Intentions</b><br>(Wisniewski et al. 2014)   | <b>DIST1</b> | In future, I plan to untag or remove mentions from photos or posts on Facebook to protect my privacy.                           |
|  | <b>DIST2</b> | In future, I intend to request friends to take down posts or photos on Facebook to keep myself private.                         |
|  | <b>DIST3</b> | In future, I plan to delete contents on my Facebook timeline to hide somethings from others.                                    |
| <b>Exit Intentions</b><br>(Baumer et al. 2013)   | <b>EXIT1</b> | In future, I intend to deactivate my Facebook account at some point to maintain my privacy.                                     |
|  | <b>EXIT2</b> | In future, I plan to stop using my Facebook account at some point to maintain my privacy.                                       |
|  | <b>EXIT3</b> | In future, I will delete my Facebook account at some point, to maintain my privacy.   |
| <b>Upgrading Behavior</b>  | <b>PUPG</b>  | On the same settings page ("Settings" > "General" > "About") tell us your "Software Version"                                    |

Items follow a 7-pt scale with 1 as *strongly disagree* and 7 as *strongly agree*, with 4 as *neutral*. \*Removed items after item reliability assessment (CFA). Upgrading behavior is transformed into a dichotomous outcome.