

8-13-2019

Explaining the Privacy Paradox through Identifying Boundary Conditions of the Relationship between Privacy Concerns and Disclosure Behaviors

Tawfiq Alashoor
Georgia State University

Follow this and additional works at: https://scholarworks.gsu.edu/cis_diss

Recommended Citation

Alashoor, Tawfiq, "Explaining the Privacy Paradox through Identifying Boundary Conditions of the Relationship between Privacy Concerns and Disclosure Behaviors." Dissertation, Georgia State University, 2019.
https://scholarworks.gsu.edu/cis_diss/70

This Dissertation is brought to you for free and open access by the Department of Computer Information Systems at ScholarWorks @ Georgia State University. It has been accepted for inclusion in Computer Information Systems Dissertations by an authorized administrator of ScholarWorks @ Georgia State University. For more information, please contact scholarworks@gsu.edu.

*EXPLAINING THE PRIVACY PARADOX THROUGH IDENTIFYING BOUNDARY CONDITIONS OF
THE RELATIONSHIP BETWEEN PRIVACY CONCERNS AND DISCLOSURE BEHAVIORS*

BY

TAWFIQ MAHDI A. ALASHOOR

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree

Of

Doctor of Philosophy

In the Robinson College of Business

Of

Georgia State University

GEORGIA STATE UNIVERSITY
ROBINSON COLLEGE OF BUSINESS
2019

Copyright by
Tawfiq Mahdi A. Alashoor
2019

ACCEPTANCE

This dissertation was prepared under the direction of the *TAWFIQ MAHDI A. ALASHOOR'S* Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business Administration in the J. Mack Robinson College of Business of Georgia State University.

Richard Phillips, Dean

DISSERTATION COMMITTEE

Dr. Mark Keil (Chair)
Dr. Richard Baskerville
Dr. Likoebe Mohau Maruping
Dr. Zhenhui (Jack) Jiang

ABSTRACT

*EXPLAINING THE PRIVACY PARADOX THROUGH IDENTIFYING BOUNDARY CONDITIONS OF
THE RELATIONSHIP BETWEEN PRIVACY CONCERNS AND DISCLOSURE BEHAVIORS*

BY

TAWFIQ MAHDI A. ALASHOOR

June 6th, 2019

Committee Chair: *Dr. Mark Keil*

Major Academic Unit: *Computer Information Systems*

The privacy paradox phenomenon suggests that individuals tend to make privacy decisions (i.e., disclosure of personal information) that contradict their dispositional privacy concerns. Despite the emerging research attempting to explain this phenomenon, it remains unclear why the privacy paradox exists. In order to explain why it exists and to be able to predict occurrences of privacy paradoxical decisions, this dissertation emphasizes the need to identify boundary conditions of the relationship between privacy concerns and disclosure behaviors. Across three empirical research studies varying in their contexts, this dissertation presents a total of seven boundary conditions (i.e., cognitive absorption, cognitive resource depletion, positive mood state, privacy control, convenience, empathic concern, and social nudging) that can explain why privacy concerns sometimes do not predict disclosure behaviors (i.e., the privacy paradox). The approach of identifying the boundary conditions advances privacy theories by establishing a theoretically sounder causal link between privacy concerns and disclosure behaviors while contributing to enhancing privacy policies, organizational privacy practices, and individuals' privacy decisions.

Acknowledgments

The Ph.D. program is the journey of my life. My decision to pursue a Ph.D. degree was the best decision I have made in my life, and it will likely continue to be. The positive influence the Ph.D. program had on me is instrumental and will be long-lasting. It extremely impacted my personal philosophy of life, how I perceive reality, how I behave and make decisions, and how I judge humans' behaviors and decisions. I am grateful for such an amazing evolution in my cognitive ability, knowledge, and personality, and I am thankful for everyone who was involved in this journey.

Before acknowledging those who contributed to my Ph.D. journey, I would like to commend the department of Computer Information Systems (CIS) at Georgia State University. The CIS Ph.D. program provided me with the scientific toolkit that I wanted to acquire. I would also like to acknowledge the family-friendly culture of the CIS department. It uplifted me when I was depleted, depressed, or frustrated. Thank you, CIS department family, for your support.

First and foremost, I would like to express my special and sincere gratitude to my advisor, Dr. Mark Keil. I could write pages after pages, but words cannot describe how much I appreciate this gentleman and how much he influenced me, both personally and professionally. On a personal level, Mark taught me how to assess situations through deliberate thinking and how to identify the available choices before making a decision. He also taught me how to be transparent about the choices I make and to always have rational reasons for my choices. Mark's continued guidance helped me in learning to have integrity in everything I do as well as how to preemptively think how to address any possible miscommunication, misunderstanding, or ethical dilemma. He taught me how to have an optimistic attitude and how to apply positive frames when communicating with people. Mark taught me to put myself in other people's shoes in order to understand their perspectives. He taught me and taught me to the point that I unintentionally imitated his way of saying hi, his hand wave, his laugh, his personality, and his way of caring about others. His mentorship was, for the most part, indirect and therefore I vicariously learned from him. I am significantly influenced by Mark's persona and I am very proud to acknowledge that.

At the professional level, Mark had a tremendous impact on my writing style in particular and my research skills in general. Mark's knowledge of experimental design is sharp. It is incredible how meticulous he is when it comes to designing an experiment. His expertise in this regard is reflected in my dissertation work and other projects. He taught me how to manage co-authorship issues as he connected me with well-recognized scholars in our field. He also inspired me to aim high and to invest in high-quality research ideas. Mark enhanced my professional communication style. For instance, I would always send a thank you note to people contributing to my work, even if it was an extremely minor contribution. I learned this polite behavior from him. He was generous in sharing insightful tips about the review process and how to communicate with gatekeepers. I am indebted to Mark and I feel so lucky to have had the chance to work with as well as learn from such an amazing scholar, mentor, and friend.

I would also like to thank my dissertation committee: Dr. Richard Baskerville, Dr. Likoebe Maruping, and Dr. Zhenhui (Jack) Jiang. I worked with Richard beginning in my first year in the Ph.D. program. To me, he is that scholar who would bring wisdom to the table. His radical research ideas and theoretical explanations fascinated me and continue to do so. I learned from Richard how to see the forest for the trees. Likoebe was instrumental in motivating me to rise to the challenge as he was so generous in spending the time to talk with me about my personal life and research work with positive energy. I learned from Likoebe how to pause a few seconds to process my thoughts before speaking. I met Jack (thanks to Mark who introduced me to him) in my second year. Jack improved my experimental design skills as his advice and guidance brought rigor to my dissertation and other projects. I am grateful for having a group of well-established scholars serving on my dissertation committee, and I cannot thank them enough for taking on this task.

My sincere thanks go Dr. Balasubramaniam Ramesh who had faith in me and accepted me into the Ph.D. program. A special thank you goes to Dr. Arun Rai, who not only taught me theory development, but also enhanced my scholarly thoughts and was always there to cheer me up when I was frustrated. A number of distinguished faculty members contributed to my research knowledge including Dr. Detmar Straub, Dr. Lisa Lambert, Dr. Edward Rigdon, Dr. Pierre Nguimkeu, and Dr. Leigh Ann Liu.

I would also like to thank Dr. Daniel Robey, Dr. Lars Mathiassen, Dr. Tamer Cavusgil, Dr. Satish Nargundkar, Dr. J.P. Shim, Dr. Veda Storey, Dr. Greg Gimpel, Dr. Kurt Schmitz, and Dr. Shuguang Hong for taking the time to give me advice and discuss academia-related issues with me during my Ph.D. program.

My special thanks also go to my fellow CIS Ph.D. students: Kambiz Saffarizadeh, Maheshwar Boodraj, Vitali Mindel, Hyung Koo Lee, Tianjie Deng, Amrita George, Joshua Madden, Zirun Qi, Jessica Pye, Arun Aryal, Christine Abdalla Mikhaeil, Youyou Tao, Neetu Singh, Alan Yang, Pengcheng Wang, Yanran Liu, Zhitao Yin, Hyoungyong Choi, Junyoung Park, Yukun Yang, Khaleed Mahmood Fuad, Xiaocong Cui, Sophia Zhang, Jeremy Lee, Wei Joe Zhang, and Yumeng Miao. Also, my special thanks go to my other fellow Ph.D. students in the Robinson College of Business: Elizabeth Napier, Artemis Boulamatsi, Roberto Felipe Mora, Yimai Lewis, Yen-Hung Steven Liu, Jingting Liu Holmes, Derek Stotler, Tanja Darden, AJ Corner, Jenny Wang, Greg Hardt, Ania Zabinski, François Neville, Sarah Ku, Elena Poliakova, Rumela Sengupta, Ayan Ghosh Dastidar, Vic Lee, and James Wilhelm. The Ph.D. journey would not be as enjoyable if it was not for this group of smart and caring individuals.

My heartfelt thanks go to my family, especially my mom and Ruqayah, for their continuous emotional support during the Ph.D. program. I am also grateful for having a wonderful group of close friends who were geographically far away but were emotionally close to support me and to always bring laughter into my life. Murtada Alramadan, Mousa Alramadan, Mohammed Al Sweed, Adel Al Mahasnah, Ali Al Zayer, Ali Karam, Mohammed Alramadan, thank you all from the bottom of my heart. I also want to express my sincere thanks to my three special friends, Mazen Shawosh, Mahdi Mahmoudzadeh, and Sehee Han, who were there to spend hours to listen to and enrich my scientific thoughts while encouraging me to pursue my dreams.

Last but not least, it is my pleasure to present this dissertation in honor of Dr. H. Jeff Smith. Jeff made a lasting impact on the privacy literature and has significantly influenced my personal and professional view of this domain. I first recognized Jeff as a privacy scholar when I was working on my Master's thesis. I was elated to know that I would be working with him during the Ph.D. program (thanks

to Mark for introducing me to Jeff). It was truly an honor and a privilege for me to have had the opportunity to work with Jeff, to learn from him, and I wish he were here to know how much I value his research spirit, personality, and kindness.

Table of Contents

| | |
|---|----|
| CHAPTER 1 [Introduction] | 12 |
| BRIEF BACKGROUND AND OVERARCHING RESEARCH QUESTION | 13 |
| OVERARCHING OBJECTIVE, MOTIVATION, AND CONTRIBUTION | 15 |
| OUTLINE OF THREE EMPIRICAL RESEARCH ESSAYS | 16 |
| REFERENCES | 18 |
| CHAPTER 2 [Research Essay 1] | 20 |
| Toward a Better Understanding of the Privacy Paradox: Identifying Cognitive Absorption as a Boundary Condition | 21 |
| INTRODUCTION | 22 |
| SOCIAL NETWORK SITES | 25 |
| PRIVACY CONCERNS AND SELF-DISCLOSURES IN SOCIAL NETWORK SITES | 25 |
| THE PRIVACY CALCULUS | 28 |
| THE PRIVACY PARADOX..... | 29 |
| Conceptualization of the Privacy Paradox | 30 |
| Existing Evidence of the Privacy Paradox | 31 |
| Explaining the Privacy Paradox..... | 33 |
| Operationalization of the Privacy Paradox | 33 |
| THE CONDITIONAL NATURE OF PRIVACY DECISIONS | 34 |
| COGNITIVE ABSORPTION..... | 37 |
| METHOD | 40 |
| DATA ANALYSIS AND PROPOSITION DEVELOPMENT | 41 |
| Phenomenon 1: Cognitive Absorption, Privacy Concerns, and Self-disclosure..... | 42 |
| Phenomenon 2: Cognitive Absorption, Perceived Benefits, and Perceived Privacy Risks | 44 |
| Phenomenon 3: Cognitive Absorption, Information Sensitivity, and Time | 45 |
| Case Description and Cross-Case Synthesis..... | 47 |
| DISCUSSION | 49 |
| Explaining the Privacy Paradox through Cognitive Absorption..... | 49 |
| Future Research | 51 |
| Theoretical Advances..... | 53 |
| CONCLUSION..... | 54 |
| REFERENCES | 55 |
| APPENDIX A (INTERVIEW PROTOCOL)..... | 62 |
| APPENDIX B (EXAMPLES OF EVIDENCE) | 63 |

| | |
|--|-----|
| CHAPTER 3 [Research Essay 2] | 66 |
| Too Tired and in Too Good of a Mood to Worry about Privacy: Explaining the Privacy Paradox through the Lens of Effort Level in Cognitive Processing | 67 |
| INTRODUCTION | 68 |
| BACKGROUND AND HYPOTHESES | 73 |
| Privacy Concerns and Information Disclosure | 73 |
| <i>The Privacy Paradox</i> | 74 |
| Elaboration Likelihood Model (ELM)..... | 77 |
| Cognitive Resource and Mood State..... | 78 |
| EXPERIMENT 1 | 81 |
| Method | 81 |
| Procedure | 81 |
| Manipulation Check..... | 83 |
| Measurement Validation..... | 83 |
| Dependent Variable | 84 |
| Results..... | 85 |
| Discussion | 89 |
| EXPERIMENT 2 | 89 |
| Method | 90 |
| Procedure | 90 |
| Manipulation Check..... | 91 |
| Independent Variables | 92 |
| Dependent Variable | 92 |
| Results..... | 93 |
| Discussion | 94 |
| GENERAL DISCUSSION | 95 |
| Theoretical Implications | 95 |
| Limitations and Future Research | 98 |
| Practical Implications..... | 99 |
| CONCLUSION..... | 101 |
| REFERENCES | 102 |
| APPENDIX A: METHOD AND ANALYSIS | 108 |
| Appendix A.1: Experiment 1’s Exploratory Factor Analysis..... | 108 |
| Appendix A.2: Experiment 1’s Preliminary Analysis, Control Variables, and Robustness Checks..... | 109 |

| | |
|--|-----|
| <i>Control Variables</i> | 111 |
| <i>Robustness Checks: WLS versus OLS</i> | 111 |
| Appendix A.3: Experiment 2’s OLS Regression Results | 115 |
| Appendix A: References | 116 |
| APPENDIX B: STUDY INSTRUMENTS..... | 117 |
| Appendix B.1: Experiment 1’s Instrument | 117 |
| Appendix B.2: Experiment 2’s Pilot Test and Instrument..... | 121 |
| <i>Pilot Test</i> | 121 |
| <i>Experiment 2’s Instrument</i> | 122 |
| CHAPTER 4 [Research Essay 3] | 125 |
| Exploring Data Donations for Medical Research in the Face of Privacy Concerns | 126 |
| INTRODUCTION | 127 |
| THEORETICAL BACKGROUND AND HYPOTHESES | 132 |
| Privacy Concerns and Disclosure of Personal Information | 132 |
| Health Information Privacy Concerns | 133 |
| The Enhanced Antecedents – Privacy Concerns – Outcomes (APCO) Model | 136 |
| <i>Normative Factor 1: Empowering Donors through Privacy Controls</i> | 138 |
| <i>Non-Normative Factor 1: Motivating Donors’ Altruism through Empathic Concern</i> | 139 |
| <i>Privacy Concerns, Privacy Controls, and Empathic Concern: A Three-Way Interaction</i> . | 140 |
| <i>Normative Factor 2: Facilitating Donors through Ease of Donation</i> | 141 |
| <i>Non-Normative Factor 2: Herding Donors through Social Nudging</i> | 143 |
| <i>Privacy Concerns, Ease of Donation, and Social Nudging: A Three-Way Interaction</i> | 145 |
| METHOD | 146 |
| EXPERIMENT 1 | 147 |
| Sample and Procedure..... | 147 |
| Manipulations and Measurements | 148 |
| Statistical Analyses | 150 |
| Results..... | 151 |
| EXPERIMENT 2 | 153 |
| Sample and Procedure..... | 153 |
| Manipulations and Measurements | 154 |
| Statistical Analyses | 156 |
| Results..... | 156 |
| GENERAL DISCUSSION | 159 |

| | |
|---|-----|
| Ethical Implications | 163 |
| Limitations and Future Research | 164 |
| CONCLUSION..... | 165 |
| REFERENCES | 166 |
| APPENDIX A: EXPERIMENT 1 | 172 |
| Appendix A.1 Experiment 1’s Instrument | 172 |
| Appendix A.2 Experiment 1’s Measurement Validation..... | 179 |
| Appendix A.3 Experiment 1’s Additional Statistical Analyses..... | 180 |
| APPENDIX B: EXPERIMENT 2..... | 181 |
| Appendix B.1 Experiment 2’s Instrument | 181 |
| Appendix B.2 Experiment 2’s Measurement Validation..... | 183 |
| Appendix B.3 Experiment 2’s Additional Statistical Analyses | 184 |
| APPENDIX: REFERENCES..... | 185 |
| CHAPTER 5 [Conclusion] | 186 |
| SUMMARY OF BOUNDARY CONDITIONS AND GUIDELINES FOR FUTURE RESEARCH..... | 188 |
| CONCLUDING REMARKS ABOUT POLICY IMPLICATIONS: TOWARD A PRIVACY INTELLIGENCE PERSPECTIVE..... | 189 |

CHAPTER 1

Introduction

BRIEF BACKGROUND AND OVERARCHING RESEARCH QUESTION

Utilization of Information and Communication Technologies (ICTs) commonly entails disclosure of personal information. The use of social media, online games, online shopping, online banking, and even the mere use of web browsers involve disclosure of large amounts of personal information. Some disclosure behaviors are intentional, such as sharing an opinion, expressing a feeling, or posting a personal photo on a social network site. In this case, users' disclosure of personal information is assumed to be based on weighing the costs and benefits involved along with consideration of dispositional privacy beliefs, such as privacy concerns. In other words, individuals are assumed to adopt a privacy calculus (Dinev and Hart 2006). Other types of disclosures, however, may occur spontaneously, grudgingly, or without consent. For example, while users of a news website read an article, they are, in many cases, unknowingly disclosing their browsing preferences and other personal data that are exploited by online companies. In this case, users have neither disclosure intentions nor control over the disclosing activity; therefore, the probability of a privacy calculus taking place is tenuous. Put simply, disclosure of personal information has become inevitable in today's digital age.

Public polls continue to reveal heightened levels of privacy concerns among online users (FTC 2000; Rainie 2013, 2016; TRUSTe 2016). The collective evidence from the privacy literature suggests that individuals who have high concerns for information privacy are more likely to refrain from sharing personal information online and more willing to discontinue using online services (Li 2011; Smith et al. 2011; Yun et al. 2014). Although the extant literature provides general support for the negative association between privacy concerns and disclosure-related behavioral outcomes, more recent research suggests that discrepancies between privacy concerns and disclosure behaviors are commonly observed. In other words, users tend to make disclosure decisions that contradict their dispositional privacy concerns, a phenomenon referred to as the privacy paradox (Acquisti et al. 2016; Barth and de Jong 2017; Dienlin and Trepte 2015; Kokolakis 2017). The underlying theme of this dissertation revolves around testing and explaining this phenomenon.

Essentially, the privacy paradox reflects a weak relationship between dispositional privacy concerns and disclosure behaviors. Evidence supporting the privacy paradox as an empirical phenomenon has been discussed in the literature (Acquisti et al. 2016). For instance, research has shown that privacy concerns do not predict disclosure outcomes (Acquisti and Gross 2006; Acquisti and Grossklags 2005; Tufekci 2008). Thus, we know that privacy concerns may not necessarily predict disclosure behaviors. In other words, individuals may not act on their privacy concerns when making a disclosure decision.

The existing literature attempting to explain the privacy paradox focuses on exploring factors that motivate or determine disclosure outcomes. Findings from this literature suggest that individuals may disclose personal information because they perceive high benefits associated with the disclosure decision. For example, individuals share personal experiences to seek social support (Debatin et al. 2009; Saffarizadeh et al. 2017). In addition, many other factors (e.g., mood, enjoyment, convenience, and privacy assurances) have been shown to determine disclosure outcomes (Krasnova et al. 2010; Li et al. 2011; Lowry et al. 2012; Wakefield 2013). These findings have led researchers to conclude that the privacy paradox can be explained as individuals weigh other factors (e.g., mood, convenience, etc.) over their privacy concerns. However, I claim that the evidence used to make such conclusions cannot explain the privacy paradox.

Evidence from this literature is simply about the direct effect of a number of factors on disclosure outcomes along with the direct effect of privacy concerns. If individuals weigh the benefits (or other factors) more than their privacy concerns, this does not imply that privacy concerns do not play a significant role in predicting disclosure behaviors. More important, the approach of examining the direct effect of relevant factors cannot predict when or explain why individuals who profess to have privacy concerns behave contradictorily by disclosing too much personal information. It simply tests and predicts the direct effect of a number of factors (e.g., benefits, privacy concerns, etc.) on disclosure outcomes. Thus, such an approach (i.e., focusing on the determinants of disclosure) neither predicts nor explains the causes of the privacy paradox. In other words, evidence based on this approach cannot predict the conditions (e.g., positive mood, convenience, or in the presence of privacy assurances) under which the

privacy paradox may occur, which is what one would seek to predict the privacy paradox. Accordingly, evidence from this approach cannot explain why privacy concerns in some cases do not match disclosure behaviors, and hence it cannot explain why the privacy paradox exists in the first place.

Explaining the privacy paradox requires exploring the conditions under which privacy concerns exhibit a weak or insignificant association with disclosure behaviors. To explain why this phenomenon exists, I propose and test a number of boundary conditions that may attenuate the relationship between privacy concerns and disclosure behaviors. Therefore, this dissertation presents a number of conditions that can predict and explain occurrences of the privacy paradox. The overarching research question is:

Research Question: Under what conditions do dispositional privacy concerns exhibit weak influence on disclosure behaviors?

As will be seen in the empirical studies (i.e., Research Essay 1, 2, and 3), there are a number of conditions under which individuals' disclosure decisions are not determined by their dispositional privacy concerns. Such conditions explain why the privacy paradox exists.

OVERARCHING OBJECTIVE, MOTIVATION, AND CONTRIBUTION

The main objective of this dissertation is to identify boundary conditions of the relationship between dispositional privacy concerns and disclosure behaviors. The privacy paradox, defined as a mismatch between privacy concerns and disclosure behaviors, is likely due to the lack of knowledge about the boundary conditions of the causal link between privacy concerns and disclosure behaviors. From a theoretical perspective, reductions in cognitive ability and/or disruptive emotional states represent boundary conditions that could compromise the significant negative effect of privacy concerns on disclosure behaviors (Dinev et al. 2015). These boundary conditions, including many others, could explain why privacy concerns may not always be causally predictive of disclosure behaviors (Acquisti et al. 2016; Dinev et al. 2015). Motivated by the lack of empirical evidence in this regard, this dissertation aims to help establish a sounder causal link between privacy concerns and disclosure behaviors by identifying a number of boundary conditions across different contexts. Thus, the key contribution of this

dissertation is to present a deeper understanding of the privacy paradox which will help in advancing privacy theories that explain and predict disclosure behaviors in light of dispositional privacy concerns.

This dissertation is also motivated by a critical limitation in the extant privacy literature (i.e., reliance on disclosure intentions rather than disclosure behaviors). More specifically, the majority of privacy studies tested the effect of privacy concerns on disclosure intentions rather than actual disclosure behaviors. However, disclosure intentions may not be consistent with disclosure behaviors (Norberg et al. 2007). As a result, the current collective evidence provides limited understanding of disclosure behaviors and the degree to which disclosure behaviors are influenced by dispositional privacy concerns. Smith et al. (2011) attribute this limitation to the lack of knowledge about the privacy paradox. Hence, it is imperative to replicate previous findings (i.e., the relationship between privacy concerns and disclosure outcomes) by using appropriate measures of disclosure (i.e., disclosure behaviors instead of disclosure intentions). Accordingly, the current dissertation tries to get at actual disclosure behaviors. In cases where measuring actual disclosure behaviors was infeasible, suitable proxies for actual disclosure behaviors rather than intentions were used. Thus, another contribution of this dissertation is to address a known limitation that is present in much of the privacy literature, namely by testing the effect of dispositional privacy concerns on disclosure behaviors rather than disclosure intentions.

This dissertation encompasses three empirical research essays. While each one is designed to achieve the same overarching objective – i.e., identifying boundary conditions to explain the privacy paradox – each essay has its own objectives, motivations, and theoretical and practical contributions. The context of each essay is also different. For brevity and due to the diversity of these attributes across the three essays, the objective, motivation, and contribution of each essay are not repeated here.

OUTLINE OF THREE EMPIRICAL RESEARCH ESSAYS

Table 1 presents an outline for the three essays that comprise this dissertation. The first essay (Chapter 2) is a qualitative research study that examines inconsistencies between dispositional privacy concerns and disclosure behaviors in the context of social network sites. This essay presents a detailed discussion on the state of the art in privacy research and points to issues in the related literature attempting to address

the privacy paradox. Then it proposes a roadmap that emphasizes the need for identifying boundary conditions that will make the surprising anomaly (i.e., privacy paradox) part of our normal understanding of privacy-related decisions. It then presents cognitive absorption (Agarwal and Karahanna 2000) as a wide-ranging boundary condition along with empirical evidence based on a multiple-case study. It concludes with a mid-range theory that explains the interwoven effects of privacy concerns, information sensitivity, and cognitive absorption on disclosure behaviors.

| Table 1. Outline of Research Essays | | | | |
|---|----------------------|--------------------|--|--------------------------------------|
| Research Essay Title | Research Type | Methodology | Theoretical Background | Context |
| Chapter 2 Toward a Better Understanding of the Privacy Paradox: Identifying Cognitive Absorption as a Boundary Condition | Qualitative | Case Study | Cognitive Absorption Enhanced APCO Model | Social Media |
| Chapter 3 Too Tired and in Too Good of a Mood to Worry about Privacy: Explaining the Privacy Paradox through the Lens of Effort Level in Cognitive Processing | Quantitative | Two Experiments | Elaboration Likelihood Model Enhanced APCO Model | Mobile Apps and Online Surveys |
| Chapter 4 Exploring Data Donations for Medical Research in the Face of Privacy Concerns | Quantitative | Two Experiments | Enhanced APCO Model Elaboration Likelihood Model Behavioral Economics Theory of Altruistic Motivation | Health Data Donation |

The second essay (Chapter 3) is a quantitative research study that examines low-effort cognitive processing on disclosure behaviors. It draws mainly upon the Elaboration Likelihood Model (ELM) (Petty and Cacioppo 1986; Petty and Briñol 2010) while referring to the enhanced Antecedents – Privacy Concerns – Outcomes (APCO) model (Dinev et al. 2015). This essay proposes cognitive resource depletion and positive mood as two boundary conditions under which the privacy paradox may be observed and provides empirical evidence based on two experiments.

The third essay (Chapter 4) is a quantitative research study that proposes four boundary conditions (i.e., privacy controls, ease of donation, empathic concern, and social nudging) in the context of data donation, an emerging healthcare practice whereby individuals are encouraged to donate their personal information for medical research (Shaw et al. 2015, 2016; Taylor and Mandl 2015; Topol 2015). The essay draws mainly upon the enhanced APCO model while referring to the ELM, behavioral economics principles, and other theories from cognitive psychology. This essay proposes that the privacy paradox may be observed when potential data donors are provided with granular privacy controls or when

their empathy is induced. It also proposes that the privacy paradox may be observed when potential data donors are provided with an automatic donation method or when they are distracted by a simple social nudge. Empirical evidence is based on two experiments involving screen mockups of an app designed for data donation.

REFERENCES

- Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technology*, G. Danezis and P. Golle (eds.), Cambridge, UK: 6th International Workshop, pp. 36-58.
- Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26-33.
- Acquisti, A., Taylor, C. R., and Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (52:2), pp. 1-64.
- Agarwal, R., and Karahanna, E. 2000. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage," *MIS Quarterly* (24:4), pp. 665-694.
- Barth, S., and de Jong, M. 2017. "The Privacy paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review," *Telematics and Informatics* (34), pp. 1038-1058.
- Debatin, B., Lovejoy, J. P., Horn, A. K., and Hughes, B. N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* (15:1), pp. 83-108.
- Dienlin, T., and Trepte, S. 2015. "Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors," *European Journal of Social Psychology* (45:3), pp. 285-297.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80,100.
- 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.
- FTC 2000. "Privacy Online: Fair Information Practices in the Electronic Marketplace". Retrieved (March 25, 2018) from <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>
- Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), pp. 122-134.
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.
- Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), pp. 434-445.
- Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28:28), pp. 453-496.
- Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers," *Journal of the Association for Information Science and Technology* (63:4), pp. 755-776.

- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.
- Petty, R. E., and Briñol P. 2010. "Attitude Change," in *Advanced Social Psychology: The State of the Science*, R. F. Baumeister and E. J. Finkel (eds.), Oxford, UK: Oxford University Press, pp. 217-259.
- Petty, R. E., and Cacioppo, J. T. 1986. *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*, New York: Springer-Verlag.
- Rainie, L. 2016. "The State of Privacy in Post-Snowden America," *The Pew Research Center*. Retrieved (January, 16, 2017) from <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>
- Rainie, L., Kiesler, S., Kang, R., and Madden, M. 2013. "Anonymity, Privacy, and Security Online," *The Pew Research Center*. Retrieved (February, 14, 2018) from <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
- Saffarizadeh, K., Boodraj, M., and Alashoor, T. (2017). "Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-disclosure," in *Proceedings of Pre-ICIS Workshop on Information Security and Privacy*, Seoul, South Korea.
- Shaw, D. M., Gross, J. V., and Erren, T. C. 2015. "Data Donation after Death," *The Lancet* (386: 9991), pp. 340.
- Shaw, D. M., Gross, J. V., and Erren, T. C. 2016. "Data Donation after Death," *EMBO Reports: Science & Society* (17:1), pp. 14-17.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.
- Taylor, P. L., and Mandl, K. D. 2015. "Leaping the Data Chasm: Structuring Donation of Clinical Data for Healthcare Innovation and Modeling," *Harvard Health Policy Review* (14:2), pp. 18-21.
- Topol, E. 2015. *The Patient Will See You Now: The Future of Medicine is in Your Hands*, New York, NY: Basic Books.
- TRUSTe 2016. "NCSA Consumer Privacy Infographic – US Edition," *TrustArc*. Retrieved (August 30, 2016) from: <https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/>
- Tufekci, Z. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society* (28:1), pp. 20-36.
- Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157-174.
- Yun, H., Lee, G., and Kim, D. 2014. "A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.

CHAPTER 2

Research Essay 1

Toward a Better Understanding of the Privacy Paradox: Identifying Cognitive Absorption as a Boundary Condition

Abstract

Research shows that social network site (SNS) users who have privacy concerns intend to self-disclose less information. However, in real-world behavior, users often ignore these concerns. This is the “privacy paradox” where users’ dispositional privacy concerns are inconsistent with their self-disclosure behaviors. In this paper, we elaborate the state of the art in privacy research and point to issues in the related literature attempting to address this paradox. We propose a roadmap that emphasizes the need for identifying boundary conditions that will make the surprising anomaly (i.e., privacy paradox) part of our normal understanding of privacy-related decisions. Following, we present cognitive absorption as a boundary condition through which we explain why SNS users’ privacy concerns might not be consistent with their self-disclosure behaviors. Grounded on the most recent privacy models and a multiple-case study, we present a mid-range theory that explains the interwoven effects of privacy concerns, information sensitivity, and cognitive absorption on self-disclosure behaviors. The theory also accounts for time which explains the evolutionary nature of privacy-related decisions. The proposed theory contributes to the privacy domain in particular but it could potentially address paradoxical behaviors in other IS domains.

Keywords: information privacy, privacy concerns, self-disclosure, privacy paradox, privacy calculus, cognitive absorption, social network sites, theory development, case study.

INTRODUCTION

Communicating via Social Network Sites (SNSs) has become ubiquitous with 81% of Americans using at least one SNS and 52% using two or more SNSs (e.g., Facebook, Twitter, Instagram, Snapchat, and LinkedIn) (Bergstrom 2018; Duggan et al. 2015). Facebook continues to dominate the industry with 53% of Americans accessing the site several times a day (Richter 2017; Statista 2017). While its adoption has not increased much, the use of other SNSs has marginally increased (Duggan et al. 2015), suggesting that SNSs consumption continues to proliferate. SNSs provide a number of benefits to users including communicating and socializing, reading and sharing news, and building communities. Realizing these benefits, however, does not come without cost. Information shared on SNSs is permanently stored, easily searched, instantly shared, and heavily traded and harnessed by organizations for different purposes, such as targeted ads, surveillance, and monetization with or without users' awareness (Craig and Ludloff 2011; Hurwitz et al. 2013). People's consumption of SNSs has significantly influenced today's communication patterns (Acquisti and Gross 2006; Cao et al. 2015; Debatin et al. 2009; Ellison et al. 2007; James et al. 2015). Yet, a conceptual tension arises. On the one hand, users have high interest in consuming SNSs, which by design encourage users to self-disclose personal information. After all, much of the interesting content of SNSs can arise from self-disclosures in one form or another. On the other hand, users have high privacy concerns discouraging their willingness to consume SNSs, particularly self-disclosing personal information, especially with the recent rise in the topic of privacy, Cambridge Analytica and General Data Protection Regulation (<https://www.eugdpr.org/>) (Meredith 2018; Rainie 2016, 2018; Sly 2018).

Research on privacy has intrigued scholars from different fields, including Information Systems (IS). Reviews of this literature provide overarching models describing the antecedents and outcomes of privacy concerns (a trait-like or dispositional construct that represents the focus of prior research) (Bélanger and Crossler 2011; Li 2011; Smith et al. 2011). In the current study, we focus exclusively on

dispositional privacy concerns and self-disclosure behaviors.¹ Self-disclosure is an important behavioral outcome that has essential practical implications. In particular, for SNS providers to gain competitive advantage, they rely heavily on users' continuous usage of the services provided and, more importantly, the amount (breadth) and intimacy (depth) of the personal information disclosed. Without rich data shared by users, SNS providers are not capable of supplying marketers and data brokers, especially those whose business models are driven by SNS big data (Craig and Ludloff 2011; Manyika et al. 2011).

The privacy literature has established strong support for a negative relationship between privacy concerns and self-disclosure intentions (Smith et al. 2011). This relationship raises an expectation that users will tend to disclose less information or even discontinue usage of SNSs because of their privacy concerns (Krasnova et al. 2010, 2012). But in natural settings, some research finds that users' behaviors are different. Specifically, this work established a *privacy paradox* such that users express privacy concerns but behave in contradiction to their stated preferences by disclosing an extensive amount of intimate personal information (Bélanger and Crossler 2011; Dinev 2014; Smith et al. 2011). In other words, users appear to act imprudently in relation to their stated privacy concerns. Empirical research into the privacy paradox is building (Adjerid et al. 2016, 2018b; Baek 2014; Karwatzki et al. 2017; Kehr et al. 2015; Li et al. 2017), finding it to be a phenomenon that is highly prevalent in the SNSs context (Acquisti and Gross 2006; Barnes 2006; Chen and Chen 2015; Hargittai and Marwick 2016; Taddicken 2014; Utz and Kramer 2009). Against this backdrop, a number of researchers investigated situational factors and others adopted alternative theoretical approaches, such as bounded rationality and the Elaboration Likelihood Model (ELM), in an attempt to understand this seemingly paradoxical behavior (Acquisti et al. 2016, 2017; Dinev et al. 2015).

Most recently, two review papers have made attempts to compile existing findings within this literature (Barth and de Jong 2017; Kokolakis 2017). Such contributions are important given the fast-growing interest in studying the paradox. However, this literature lacks an explicit explanation(s) that

¹ Across the manuscript, unless specified, we use the term *privacy concerns* to refer to dispositional privacy concerns which reflect a trait-like construct that can be measured by one or more of the dimensions listed in Table 1. Also, unless specified, we use the terms *self-disclosure behaviors*, *self-disclosures*, or *disclosures* interchangeably to refer to the behavior of disclosing personal information.

demonstrates why the privacy paradox exists. This lack of progress is likely due to the unsystematic approach adopted by researchers to study the privacy paradox.² Evidence from our current research leads us to conclude that 1) cognitive absorption explains the appearance of a privacy paradox in the context of SNSs and 2) the seeming paradox dissolves when considering the temporal change in cognitive absorption and other constructs affecting self-disclosure behaviors.

Cognitive absorption is “a state of deep involvement with software,” analogous to a flow state that results from temporal dissociation, focused immersion, heightened enjoyment, control, and curiosity (Agarwal and Karahanna 2000, p. 673; Csikszentmihalyi 1975). It has been shown to predict intention to use SNSs and other technologies (Saadé and Bahli 2005). Cognitive absorption is “important to the study of technology use behavior because it serves as a key antecedent to salient beliefs about an information technology” (Agarwal and Karahanna 2000, p. 666). Csikszentmihalyi (1975) states that “because the flow activity has clear and noncontradictory rules, people who perform in it can temporarily forget their identity and its problems” (p. 48). Drawing on this literature, we argue that users who are immersed in SNSs enter into a flow state or, more broadly, become cognitively absorbed. This state leads them to temporarily overlook their dispositional privacy concerns during the social networking activity and hence make imprudent self-disclosures. This cognitive state sets the foundation for the current study to explain the privacy paradox. The research questions we investigate are:

RQ1: Why are SNS users’ dispositional privacy concerns inconsistent with their self-disclosure behaviors?

RQ2: How does the state of cognitive absorption explain inconsistencies between dispositional privacy concerns and self-disclosure behaviors in the context of SNSs?

Generally, we draw upon Dinev et al.’s (2015) enhanced Antecedents-Privacy Concerns-Outcomes (APCO) model which leverages dual process models, such as the ELM (Petty and Briñol 2010; Petty and Cacioppo 1986), System 1 vs. System 2 thinking (Kahneman 2011), and related theories from behavioral economics (Acquisti et al. 2016). Because the enhanced APCO model explains the cognitive processes involved in privacy behaviors, it provides a suitable overarching theory for our examination of

² In the “The Privacy Paradox” section, we articulate the state of the art and point to a number of issues in the current literature.

the role of cognitive absorption in explaining inconsistencies between privacy concerns and self-disclosure behaviors.

We contribute to the literature by proposing a mid-range theory that explains and predicts self-disclosures in light of privacy concerns and thereby addresses the limited understanding of inconsistent privacy behaviors. First, we review the literature, articulate the state of the art in the privacy paradox, and suggest a roadmap for studying inconsistent privacy behaviors. Next, we discuss cognitive absorption and present empirical evidence based on a qualitative multiple-case study. Last, we present a theoretical framework with four theoretical propositions and discuss avenues for future research.

SOCIAL NETWORK SITES

SNSs can be traced to the mid-to-late 1990s when theglobe.com and SixDegrees.com were first recognized (boyd and Ellison 2007). Many SNSs appeared in the dot-com bubble, but only a few survived after the Internet boom. Some earlier SNSs provided similar features like those provided by today's SNSs (e.g., profile photo, post, comment, private message, and friend request). LinkedIn was launched in 2003 followed by Facebook in 2004. Since then, these sites have shaped our view of the social media world. In general, SNSs provide online services, mostly for free, through which users interact, socialize, and share different kinds of personal information publicly or privately via personalized profiles. We adopt Kane et al.'s (2014) definition, as it aptly describes today's most popular SNSs in which "users (1) have a unique user profile that is constructed by the user, by members of their network, and by the platform; (2) access digital content through, and protect it from, various search mechanisms provided by the platform; (3) can articulate a list of other users with whom they share a relational connection; and (4) view and traverse their connections and those made by others on the platform." (p. 279).

PRIVACY CONCERNS AND SELF-DISCLOSURES IN SOCIAL NETWORK SITES

SNSs generate a gigantic amount of data which presents a wealth of opportunities to academic researchers and organizations. Researchers harness SNS data to study human behavior. For instance, Stutzman et al. (2012) analyzed a longitudinal panel of 5,076 college Facebook users to study privacy and self-disclosure between 2005 and 2011. Cavusoglu et al. (2016) studied the effect of privacy policy change on self-

disclosure among 13,145 college Facebook users. Organizations analyze users' data to make sound decisions for targeted ads and business improvements (Varadarajan and Soundarapandian 2013). In addition, the plethora of unstructured data is transformed to structured data which is ultimately used as an additional source of revenue, by monetizing big data containing users' personal information and product preferences (Hurwitz et al. 2013; Schmarzo 2013). Companies use SNSs to qualify or disqualify job candidates (Acquisti and Fong 2015; Breznitz et al. 2011). Governments monitor SNSs to trace malicious content and to identify terrorists (Hurwitz et al. 2013).

Whereas the above examples clearly illustrate the benefits of data generated by SNS users, the privacy issue can impede such practices (Manyika et al. 2011). First, organizations are apprehensive about invading users' privacy when adopting social media mining tools (Gundecha and Liu 2012). Second, lawsuits against well-recognized websites, such as Facebook and Google, for violating online privacy indicate the criticality of privacy. Third, users' privacy concerns are increasing as 50% of Internet users reported that they are concerned about their personal information that is available online, an increase of 33% since 2009 (Rainie et al. 2013). These heightened levels of privacy concern continue to hinder adoption of new IS. For instance, a recent study investigating attitudes toward the use of biometric identity authentication in Automated Teller Machines (ATM) indicated that privacy was the most cited concern (Breward et al. 2017). Hence, privacy research is imperative to find ways to alleviate these concerns while helping service providers to avoid adverse behaviors emanating from negative privacy attitudes.

Information privacy is "the claim of an individual to determine what information about himself or herself should be known to others" (Westin 2003, p. 431). It reflects users' control over their personal information (Solove 2006). In empirical research, privacy concern has been shown to explain and predict willingness to self-disclose (Smith et al. 2011). This construct has been defined in different ways due to its multidimensional nature. Smith et al. (2011) classify general privacy based on two main categories: value-based and cognate-based. The value-based category revolves around defining general privacy as a right or as a commodity, whereas the cognate-based category deals with general privacy as a state or as

control. Nevertheless, general privacy, in most empirical studies, reflects users’ concerns about the loss of information privacy, a definition based on the control aspect within the cognate-based category. For example, Culnan and Bies (2003) maintain that privacy is “the ability of individuals to control the terms under which their personal information is acquired and used” (p. 326). Smith et al. (1996) maintain that privacy concerns relate to collection, improper use, unauthorized secondary use, and the sharing of users’ personal information with other parties. Bélanger and Crossler (2011) define privacy concerns based on the interest in having control over personal information. These different conceptualizations resulted in diverse measurement proxies for privacy concerns (Buchanan et al. 2007; Chen and Rea, 2004; Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). More recently, Hong and Thong (2013) presented a comprehensive conceptualization of privacy concerns with three items measuring each of the six dimensions presented in Table 1.

| Table 1. Internet Privacy Concerns Dimensions (Hong and Thong, 2013, p. 278-279) | |
|---|---|
| Interaction Management – Second-Order Factor | |
| Collection | “The degree to which a person is concerned about the amount of individual-specific data possessed by websites” |
| Secondary Usage | “The degree to which a person is concerned that personal information is collected by websites for one purpose but is used for another, secondary purpose without authorization from the individual” |
| Control | “The degree to which a person is concerned that he/she does not have adequate control over his/her personal information held by websites” |
| Information Management – Second-Order Factor | |
| Errors | “The degree to which a person is concerned that protections against deliberate and accidental errors in personal data collected by websites are inadequate” |
| Improper Access | “The degree to which a person is concerned that personal information held by websites is readily available to people not properly authorized to view or work with the data” |
| Awareness – First-Order Factor | |
| Awareness | “The degree to which a person is concerned about his/her awareness of information privacy practices by websites” |

Note: Hong and Thong (2013) adapted these definitions from Malhotra et al. (2004) and Smith et al. (1996).

Privacy concerns may originate from organizational practices (e.g., SNSs sharing personal information with third parties). Yet they may also result from peer behaviors. For example, a SNS user may publicly share the private information of another user without the permission of the latter (who is the original owner of the information). In other words, the private boundary is subject to unknown limits of co-ownership within the SNSs context. Such co-ownership leads to increased uncertainty about privacy practices and loss of control (Petronio 2002). A recent study shows that ‘peer’ privacy concerns correlate negatively with self-disclosure behaviors in the SNSs context (Ozdemir et al. 2017). Therefore, we define

privacy concerns as the degree to which a SNS user is concerned about others' (e.g., SNS providers and users) practices pertaining to the treatment of their personal information in terms of collection, improper and secondary use, control, and errors, in addition to concerns about being aware of such practices. Because the focus of our study is on the paradoxical relationship between privacy concerns and self-disclosures, we limit our review to this relationship.³

Self-disclosure refers to “the breadth and depth of the revelations a user makes” (Krasnova et al. 2010, p. 111).⁴ It reflects voluntarily disclosure of personal information to others (Posey et al. 2010). In SNSs, self-disclosures of demographics, images, locations, preferences, and beliefs can be carried out in the form of profile information, post, comment, and ‘like’. The amount of disclosed information reflects the breadth while the intimacy of information reflects the depth of self-disclosure (Cozby 1973; Petronio 2002). As discussed earlier, SNS users’ data are a valuable organizational asset as they enable creating a strategic advantage. However, in various online contexts including SNSs, studies have shown that users tend to disclose less, falsify information, or discontinue usage due to privacy concerns (Alashoor et al. 2017b; Choi et al. 2015; Dinev and Hart 2006; Jiang et al. 2013; Keith et al. 2013, 2015; Krasnova et al. 2012; Li et al. 2011; Lowry et al. 2011; Marwick and boyd 2014; Peters et al. 2015).

THE PRIVACY CALCULUS

The privacy calculus proposes that self-disclosure is a product of two constructs: perceived privacy risk which is sometimes measured by privacy concerns⁵ and perceived benefit which is measured by cognitive attractions to Internet content. The literature indicates that perceived benefits (privacy risks) positively (negatively) affect self-disclosure outcomes (Malhotra et al. 2004; Ozdemir et al. 2017; Xu et al. 2010, 2013). Some research also suggests that trust in the service provider is highly relevant to privacy behaviors (Dinev and Hart 2006). Thus, by considering the risks and benefits, and in some cases trust, users can consciously manage their self-disclosure decisions. This economic principle of risk and benefit

³ For broader reviews of the determinants and outcomes of privacy concerns see Acquisti et al. (2016, 2017), Bélanger and Crossler (2011), Li (2011), Li (2012), and Smith et al. (2011).

⁴ For comprehensive reviews of self-disclosure, see Burgoon et al. (1989), Cozby (1973), Joinson and Paine (2012), and Omarzu (2000).

⁵ In “The Privacy Paradox” section, we describe why it is problematic to measure privacy concerns in lieu of perceived privacy risk when applying the privacy calculus.

analysis is a major tenet in privacy research (Culnan and Armstrong 1999; Culnan and Bies 2003; Dinev and Hart 2006). In this regard, privacy is treated as a commodity with a subjective value (Smith et al. 2011).

While the privacy calculus is a plausible theory to explain and predict disclosure intentions and behaviors, it is recognized as an inadequate theory to explain the complexities involved in disclosure behaviors. For example, the privacy calculus, unaccompanied by other theories, cannot explain why users' stated privacy concerns do not match their high disclosure behaviors. Primarily, the original premises of the privacy calculus do not consider trait-like constructs, such as privacy concerns, which can significantly determine self-disclosures (Dinev and Hart 2006). Accordingly, this theory, if not unsuitable, is inherently inadequate to answer such questions. More importantly, however, users' ability to follow a rational calculus is not the usual case because users have 1) incomplete information about the potential risks of most online privacy decisions, 2) limited mental resources to assess the risks versus the benefits (bounded rationality), and 3) as a result, cognitive and behavioral biases and simple heuristics are likely to affect users' privacy decisions (Acquisti and Grossklags 2004; Acquisti et al. 2016, 2017; Dinev et al. 2015; Simon 1982). These principles along with the privacy calculus (which we adopt as our overarching theoretical background) provide plausible explanations as to why (in some cases) SNS users' high privacy concerns do not predict low self-disclosure behaviors (i.e., the privacy paradox phenomenon). Next, we visit and discuss the privacy paradox literature in detail.

THE PRIVACY PARADOX

In a nutshell, the privacy paradox phenomenon suggests that individuals tend to make privacy decisions (i.e., disclosure of personal information) that contradict their privacy attitudes (i.e., dispositional privacy concerns). For example, SNS users disclose personal information publicly to the point that their disclosure behavior does not match their expressed concerns for privacy (Acquisti and Gross 2006;

Barnes 2006; Tufekci 2008).⁶ Accordingly, high privacy concerns should not be taken for granted as a strong predictor of low disclosure behaviors.

From a scientific perspective, if the privacy paradox is indeed a real phenomenon, an argument supported by a number of empirical studies, the reality of its existence, *per se*, indicates some lack of knowledge about the boundary conditions of the causal link between privacy concerns and disclosure behaviors. Thus far, the relationship between privacy concerns and disclosure behaviors has largely remained at the hypothesis level and that evidence for a privacy paradox is equivocal (at best) at the theoretical level. There is a need to identify boundary conditions (i.e., moderators that predict when or under what conditions privacy concerns do or do not predict disclosure behaviors) (Busse et al. 2017; Whetten 1989) in order to establish a theoretically sounder causal link between privacy concerns and disclosure behaviors.

In this section, we discuss four critical issues that could have inhibited recent reviews (Barth and de Jong 2017; Kokolakis 2017) from reaching a solid conclusion about the causes of the privacy paradox. These issues are related to the conceptualization, existing evidence, explanation, and operationalization of the privacy paradox, respectively. By addressing the existing issues and identifying important boundary conditions, privacy scholars will not only have a profound understanding of privacy paradoxical behaviors, but also contribute to developing a primary theory that explains and predicts disclosure behaviors and other privacy-related decisions in light of privacy concerns.

Conceptualization of the Privacy Paradox

First, there is ambiguity with the conceptual definition of the paradox that needs to be clarified. Is it a mismatch between stated privacy concerns and disclosure behaviors; or is it instead a mismatch between stated disclosure intentions and disclosure behaviors?

⁶ From a logical perspective, the privacy paradox may also suggest that users do not disclose personal information although they are not at all concerned about privacy. Privacy researchers have overlooked this logical statement although it is a valid one according to the meaning of the privacy paradox. In fact, examining the paradox from this perspective can enrich our understanding of the causal link between privacy concerns and disclosure behaviors. We do not expatiate this issue because the scope of this article pertains to the generally accepted definition of the privacy paradox (i.e., higher privacy concerns are not associated with lower disclosure behaviors)

Spiekermann et al.'s (2001) study is one of the earliest that documented some inconsistencies between privacy concerns and disclosure behaviors in an experimental e-commerce website. Acquisti and Grossklags (2004) found a similar observation based on a survey instrument in which privacy concerns and self-reported disclosure behaviors were measured. Both studies concluded that privacy concerns are not necessarily predictive of disclosure behaviors and the latter provided sound theoretical arguments for such findings. Acquisti and Gross (2006) also presented evidence supporting the paradox based on observational data in the SNS context. To summarize, these studies were not able to detect a significant association between privacy concerns and disclosure behaviors, and hence declared the paradox. Norberg et al. (2007), however, described and provided evidence of the paradox as a mismatch between stated disclosure intentions and disclosure behaviors. Although many privacy researchers cite Norberg et al.'s (2007) study as evidence of the paradox, Norberg et al.'s definition does not conform to what most researchers mean by the paradox (cf. Baek 2014; Choi et al. 2018; D'Souza and Phelps 2009; Keith et al. 2013; Ozdemir et al. 2017; Wakefield 2013; Wottrich et al. 2018).

Clarifying what the privacy paradox means is essential for avoiding unsystematic scholarly work. Therefore, we hold that, consistent with most studies, the *privacy paradox* refers to a mismatch, inconsistency, discrepancy, or dichotomy between *stated or dispositional* privacy concerns and disclosure behaviors.⁷

Existing Evidence of the Privacy Paradox

The second issue pertains to the robustness of existing evidence supporting the privacy paradox. On the one hand, some researchers conclude that the paradox exists when a non-significant relationship between privacy concerns and disclosure intentions⁸ or behaviors is observed (for review, see Kokolakis 2017). However, non-significant findings may also stem from sampling method, statistical power, measurement issue, and context nature. More importantly, non-significant findings could simply be due to absence of

⁷ The paradox between intention and behavior is a much broader phenomenon that is not specific to the privacy context (Ajzen 1991). Accordingly and given that the vast majority of privacy researchers have defined the paradox as a mismatch between privacy concerns and disclosure behaviors, we adopt this definition.

⁸ Studies that measured disclosure intentions instead of disclosure behaviors do not conform to the generally accepted definition of the privacy paradox and therefore they are subject to the operationalization issue (we discuss this issue in detail below).

essential factors that may interact with privacy concerns (Dinev et al. 2015). For instance, privacy concerns may well be related to disclosure of sensitive but not insensitive personal information (Malhotra et al. 2004; Mothersbaugh et al. 2012; Xie and Kang 2015). Accordingly, it is difficult to declare the paradox before addressing such methodological and theoretical issues.

On the other hand, a number of researchers back their theoretical claims for the paradox by citing research that supports the negative relationship between privacy concerns and disclosure behaviors with references to public polls that contradictorily report high levels of disclosure behaviors.⁹ This theoretical argument is not grounded on empirical evidence of the paradox, because it relies on comparing completely different populations likely sampled at different points in time. In addition, the vast majority of empirical studies report a significant relationship between privacy concerns and disclosure outcomes (Li 2011; Smith et al. 2011) and a meta-analysis supports this conclusion (Yun et al. 2014). This collective finding presents a challenge to the few studies that back claims for the privacy paradox based on non-significant statistical tests or public polls.

Nevertheless, there seems to be a general consensus that an observation of a non-significant relationship between privacy concerns and disclosure behaviors represents evidence of the privacy paradox. Assuming the validity of this evidence, accordingly, observing a non-significant relationship between privacy concerns and disclosure behaviors represents a necessary condition for explaining the privacy paradox. In other words, a study aimed at explaining the privacy paradox must first present evidence showing a null association between privacy concerns and disclosure behaviors (which implies having measures for both privacy concerns and disclosure behaviors, not intentions) before making attempts to explain why this null association was observed. Unfortunately, many studies claiming to explain the privacy paradox have not met this necessary condition which renders their explanations ambiguous.

⁹ Because this practice is so prevalent in the majority of this literature, we do not cite specific studies. In fact, even review papers of the privacy paradox tend to leverage this limited argument (see the first paragraph in Barth and de Jong 2017; Kokolakis 2017).

Explaining the Privacy Paradox

The third issue pertains to the clarity of the collective explanations for the privacy paradox. Several studies simply show evidence of a direct or indirect effect of various factors (e.g., affect, enjoyment, engagement, and social capital) on disclosure outcomes and conclude that the paradox is explained as individuals weigh the benefits of such factors more than their privacy concerns (Debatin et al. 2009; Kehr et al. 2015; Wakefield 2013; Yu et al. 2015). While such studies leverage the paradox by discounting the utility of the privacy calculus, they ultimately extend or complicate the privacy calculus and thereby heap more ambiguity on explanations for the paradox. In fact, the calculus is likely to interact with other factors (e.g., privacy concerns, emotions, heuristics) when users make disclosure decisions (Acquisti et al. 2017; Alashoor et al. 2018; Dinev et al. 2015). Thus, backing the privacy paradox claim by debunking the calculus, *per se*, lacks coherence as a theoretical argument. Popper (1959) suggests that identifying alternative explanations is an essential step prior to any attempt to falsify a theory. To explain the privacy paradox in a systematic way, researchers need to 1) present evidence for its existence and then using the same data 2) identify the conditions under which privacy concerns may not be related to disclosure behaviors.

Operationalization of the Privacy Paradox

Fourth, most studies claiming to explain the paradox exhibit a mismatch between conceptualization and operationalization of the paradox: a Paradox within the Privacy Paradox (PPP). Specifically, like us, most existing studies define the paradox as a mismatch between *stated* privacy concerns and disclosure behaviors. Yet, the same studies contradictorily operationalize disclosure using intention or willingness to disclose or at best self-reported disclosure instead of observing *actual* disclosure behaviors (e.g., Adjerid et al. 2016; Choi et al. 2018; Karwatzki et al. 2017; Kehr et al. 2015; Ku et al. 2013; Mothersbaugh et al. 2012; Sun et al. 2017; Wakefield 2013; Wottrich et al. 2018; Yu et al. 2015). Self-reports of intentions are not necessarily reliable predictors of actual behaviors, especially those that require volitional control (Ajzen 1991; Norberg et al. 2007). Volitional control is a notable feature of privacy and disclosure behaviors. Self-reports of disclosure behaviors are subject to biases (i.e., common method bias) emerging

from the survey instrument used. For instance, individuals report lower disclosure behaviors when they are initially asked to report their privacy concerns (Alashoor et al. 2017a). An appropriate measurement scale for disclosure behaviors should solicit personal information from subjects within the research instrument (for examples, see Acquisti et al. 2012, 2013; Adjerid et al. 2018a, 2018b; John et al. 2010; Norberg et al. 2007).

Another critical issue is that some studies purporting to address the paradox do not even measure privacy concern, although it is a focal part of their definition of the paradox. Rather, they rely on measuring perceived privacy risk or a variant thereof (Sun et al. 2017; Yu et al. 2015). Privacy concern, as a trait-like construct, is rather different from, although it correlates with, perceived privacy risk. For example, a social media user might be highly concerned about her privacy but would be willing to share her personal photos or feelings publicly only when she perceives low risk of sharing that information.

We believe that the PPP is a key issue impeding advancements in this literature. As suggested by Acquisti and Grossklags (2004), understanding discrepancies in privacy and disclosure behaviors would require data about privacy attitudes, actual disclosure behaviors, and the nature of the context in which disclosures are carried out. Smith et al. (2011) also noted that peculiar findings will be explained when researchers start measuring actual disclosure behaviors.

THE CONDITIONAL NATURE OF PRIVACY DECISIONS

A thorough perusal of early studies from which the term *privacy paradox* emerged indicates that individuals' privacy concerns do affect disclosure behaviors, but this effect is highly conditional. For instance, in Spiekermann et al.'s (2001) study, a majority of privacy fundamentalists (74%) and those who were identity concerned (76%) refused to reveal their physical addresses, consistent with their privacy concerns. However, under the condition in which these participants were interacting with an experimental agent, they contradictorily had a high tendency toward disclosing their purchasing preferences. Requesting physical address is much more sensitive than requesting purchasing preference. It is also important to note that the participants indicated a highly positive feedback about their experience with and seemed to develop a positive feeling toward the experimental agent. Accordingly, these

conditions (i.e., low sensitivity and interactivity) were probably influential in driving participants to self-disclose their purchasing preferences, thus resulting in a null association between privacy concerns and disclosure behaviors.¹⁰ Even so, Spiekermann et al. (2001) concluded that privacy fundamentalists exhibited a comparatively low engagement with the agent which indicated a cautious communication strategy (p. 7). In a similar vein, Acquisti and Grossklags (2004) showed that 87.5% of the highly concerned participants signed up for a loyalty card in which they revealed sensitive identifying information. Under such condition, the participants are perhaps relying heavily on the perceived benefits relative to their stated privacy concerns and the uncertain future risk (e.g., data being sold to third parties). Unfortunately, Acquisti and Grossklags (2004) only reported descriptive statistics and did not report a statistical test of the relationship between privacy concerns and disclosure behaviors. Still, they showed that the majority of participants (75%) adopted at least one privacy-protective strategy (e.g., providing false information) depending on the context of information request.

Acquisti et al. (2016) present a comprehensive review of the literature and suggest that “it is more likely that the purported dichotomy between privacy attitudes [e.g., privacy concerns] and privacy behaviors [e.g., disclosure behaviors] is actually the result of many, coexisting, and not mutually exclusive different factors... such as asymmetric information, bounded rationality, and various heuristics” (p. 40, brackets added). We concur with the notion that privacy decisions are highly conditional. Based on this logic, we argue that the dichotomy between privacy concerns and disclosure behaviors can be explained explicitly by exploring the boundary conditions of this relationship. Recent research provides tentative support to this notion.

For example, individuals become actively engaged in their privacy preferences when they are nudged through a privacy message (Baek, 2014). This suggests that the cognitive activation of privacy attitudes might be a necessary condition for individuals to make prudent disclosures consistent with their privacy concerns. Research also shows that SNS users are likely to relax their privacy concerns when they

¹⁰ Another reason for observing a non-significant association between privacy concerns and self-disclosures (i.e., purchasing preferences) in Spiekermann et al. (2001) could be a power issue (i.e., small sample sizes in each of the privacy clusters).

are able to employ privacy settings or when perceiving high control (Alashoor et al. 2017b; Cavusoglu et al. 2016; Hargittai and Marwick 2016; Marwick and boyd 2014). This indication suggests another condition under which privacy concerns might be a weak (strong) predictor of self-disclosures when perceived privacy control is high (low). In addition to the nature of the context, several other boundary conditions need to be tested to identify the specific conditions under which privacy concerns do or do not predict disclosure behaviors.

Our survey of the literature revealed only eight studies that have adopted this perspective (Anderson and Agarwal 2011; Angst and Agarwal 2009; Karwatzki et al. 2017; Li and Slee 2014; Li et al. 2017; Mothersbaugh et al. 2012), out of which three were conducted in the SNS context (Choi et al. 2018; Chen and Chen 2015; Ku et al. 2013).¹¹ For instance, Choi et al. (2018) identified the condition of privacy fatigue which attenuated the impact of privacy concerns on disclosure intentions among SNS users. Chen and Chen (2015) considered SNS users' self-efficacy as a boundary condition. While self-efficacy did not moderate the relationship between privacy concerns and self-reported disclosure behaviors, highly concerned users were less (more) likely to accept many friends (conceived as a privacy management strategy) when self-efficacy was high (low). In a different context, Wottrich et al. (2018) identified the condition of mobile app value and found the relationship between privacy concerns and permission acceptance intention to be significant only when the perceived app value was low (study 1) and this interaction effect might also depend on the app intrusiveness level (study 2).

These few studies present promising boundary conditions. Yet, due to their susceptibility to the PPP, their actual contribution evades the real question (i.e., what causes the mismatch between privacy concerns and *actual* disclosure behaviors?). While one study measured self-reported disclosures which represent a reasonable proxy for disclosure behaviors (Chen and Chen 2015), the other seven relied on disclosure intention. Although such studies present some preliminary findings for explaining the privacy paradox, we argue that it is the wide-ranging conditions that need to be identified first given their

¹¹ The dependent variable in two of these studies is intention to adopt electronic health records (Angst and Agarwal 2009; Li and Slee 2014) which is conceivably a disclosure-related outcome. The dependent variable in Ku et al.'s (2013) study is continuance use intention which is not a disclosure outcome, and hence this study does not count in the total of eight studies.

generalizability across various contexts. Against this backdrop, our study aims to identify the critical condition of cognitive absorption, which reflects the holistic experience with information technologies and contributes to shaping many of the temporary attitudes and behaviors at the moment of interaction with SNSs.

COGNITIVE ABSORPTION

The *cognitive absorption* concept was developed based on three inter-related research streams: the trait of absorption, flow theory, and cognitive engagement. First, Tellegen and Atkinson (1974) conceptualized the trait of absorption as a distinct trait that results in sequences of total attention where the object of attention fully consumes individual's attentional resources. Second, Csikszentmihalyi (1975) developed the state of flow which suggests that people enjoying themselves during an activity can become so totally involved that nothing else seems to matter. According to Csikszentmihalyi (1975, 1990), what makes people enjoy the moment of different life activities, "a state of optimal experience," is this flow state that derives from intrinsic motivation regardless of external rewards. The flow state is conceptualized as a multi-dimensional construct which includes a feeling of control, intense concentration, a loss of self-consciousness, and a transformation of time. Third, cognitive engagement refers to the state of playfulness in the context of human-computer interaction (Webster and Ho 1997). Cognitive engagement is identical to the flow state but without the notion of control. The three distinct dimensions of cognitive engagement include intrinsic interest, curiosity, and attention focus (Webster and Hackley 1997). Grounded on these three concepts, Agarwal and Karahanna (2000) conceptualized cognitive absorption and empirically supported its direct and indirect effect on behavioral intentions to use the Web. Since then, several scholars have continued examining cognitive absorption in different contexts (Leong 2011; Lin 2009; Rouis 2011; Saadé and Bahli 2005). As such, most of these studies have focused on finding ways that increase the absorption level as a means to drive positive technology use (e.g., increased SNS use).

These three collective dimensions of cognitive absorption (absorption, flow, and engagement) can release SNS self-disclosure behaviors in the following way. First, affective reactions such as emotion,

enjoyment, engagement, habit, and need for gratification have been shown as significant determinants of users' beliefs, behaviors, and continuous use of SNSs and other technologies. Turel and Serenko (2012) show that users who enjoy using SNSs become highly engaged in, and enthusiastic about, SNSs. These affective reactions contribute to *absorption*: the SNSs can fully consume users' attentional resources. Second, perceived enjoyment is an intrinsic motivator defined as "the extent to which the activity of using the computer is perceived to be enjoyable in its own right" (Davis et al. 1992, p. 1113). Self-disclosure can become highly enjoyable when it arises based on intrinsic motivations where external rewards become less important, such as audience feedback or social benefits (Ko 2013). Such intrinsic motivations drive continuous, habitual use of SNSs. The sheer, intrinsic fun of SNSs use contribute to *flow*: users gradually grow so totally involved that nothing else seems to matter. Third, SNSs use can develop a temporally disassociated immersion into the joy, power, and curiosity of the experience. Such an immersion in SNSs contributes to *cognitive engagement*: SNSs use can release an uncontrolled playfulness in users.

Evidence has already shown that cognitive absorption leads to increased intentional and actual use of technology (Agarwal and Karahanna 2000; Venkatesh 1999). The line of reasoning above further suggests that cognitive absorption leads to higher self-disclosure behaviors in SNS settings. Unlike individual affective reactions, cognitive absorption not only accounts for the holistic experience with technology, but also represents a combination of temporal, affective, and cognitive factors, an all-inclusive construct suitable to capture users' cognitive state at the moment of social networking. Because cognitive absorption constrains users' consciousness, it can have negative outcomes, such as less attention to dispositional privacy concerns, uninformed or underestimated privacy risks, and uncontrolled, imprudent self-disclosures.

While the privacy literature has not explored the effect of cognitive absorption on self-disclosure, prior research on habit and enjoyment does provide some supporting evidence. For example, LaRose et al. (2010) discuss and show that users who develop a habitual and impulsive use of SNSs become less attentive to and aware of potential negative consequences. Turel and Serenko (2012) found that while

users' enjoyment with SNSs positively affects the level of engagement, this enjoyment can lead to a habitual use of SNS. Turel and Serenko (2012) also show that bad habits, such as fulfilling short-term gains regardless of long-term outcomes, emerge because of perceived enjoyment and excessive SNSs use. Kehr et al. (2015) found that an interface that elicits positive affect leads users to underestimate potential privacy risks. Moreover, Li et al. (2011) found that the more entertainment consumers experience in a website, the lower are their privacy risk beliefs. Further, the higher their privacy protection beliefs, the stronger their intentions to self-disclose. These findings might also suggest that enjoyment can co-vary or even overpower the effects of trust on system use and self-disclosure.

Nakamura and Csikszentmihalyi (2002) state that "what to pay attention to, how intensely and for how long, are choices that will determine the content of consciousness" (p. 92). Because SNSs fill social voids in people's lives and bring about ongoing thrills, being cognitively absorbed and losing consciousness at the moment of social networking is a plausible phenomenon (Csikszentmihalyi 1975; Lin 2009; Rouis 2011; Tamir and Mitchell 2012; Turel and Serenko 2012). Accordingly, we argue that users who are highly absorbed in SNS environments would be more willing to self-disclose (in the form of posts, comments, or 'likes') and more likely to respond to information requests by SNSs. Further, we contend that when self-consciousness is lost (due to a high absorption state dominating users' cognition at the moment of use), self-disclosure does not entirely adhere to the rational calculus (i.e., perceived privacy risks and perceived benefits) and is less likely to be based on dispositional privacy concerns. On the other hand, self-disclosure is more likely to be based on a rational calculus and privacy concerns when users have sufficient cognitive resources (Dinev et al. 2015), e.g., during a low absorption state where self-consciousness is more salient.

For example, when a user decides to share personal feelings in a post or decides to 'like' a certain Facebook page, he is likely affected by what other users are posting and 'liking'. If he let himself into that environment, however, his overall self-disclosure behavior is likely to be innocently shaped by the state of cognitive absorption, even in the presence of privacy concerns. Unknowingly, this state may entail acts that result in short-term goals, such as heightened perceived benefits, but contradict long-term goals, such

as underestimating privacy risks. This phenomenon can explain the dichotomy between privacy concerns and self-disclosures as being absorbed in a SNS not only increases the level of self-disclosure, but also results in less attentiveness, consciousness, and awareness of privacy concerns which in turn lead to imprudent self-disclosure. In other words, cognitive absorption restrains users from thinking prudently about self-disclosure behaviors.

One may argue that the nature of SNS, *per se*, encourages self-disclosure and is absorbing by design and hence self-disclosure is simply determined by this nature. We address this argument by holding constant the nature of SNS (i.e., one SNS) and show that variations in self-disclosure can still be attributed to cognitive absorption within the same SNS. Another issue is the direction of the relationship between cognitive absorption and self-disclosure. One may argue that higher self-disclosure could increase the amount of absorption, reflecting a reverse direction. Yet, we argue that this direction is less likely the case because a large number of SNS users experience cognitive absorption without self-disclosing personal content (i.e., passive users or lurkers) (Chen et al. 2014). Next, we present our empirical evidence which explains how cognitive absorption explains the privacy paradox.

METHOD

We conducted a qualitative multiple-case study to explore the role of cognitive absorption. A case study is suitable considering that the social networking activity involves various attitudinal, cognitive, and behavioral factors over which we have low control (Myers 2013; Yin 2014). After analyzing the qualitative data, we developed four theoretical propositions.

Case Study Design and Data Collection: Users represent the unit of analysis in a holistic multiple-case design (Yin 2014). We adopted Yin's (2014) general strategies and specific techniques to guide the data collection and analysis. For the general strategies, we relied on the theoretical arguments discussed above which determined the protocol for the semi-structured interviews (Appendix A). We developed a case description that depicts the overall pattern of each case. We also examined rival explanations. The data analysis involved four specific techniques: (1) pattern matching to test whether the cases support our theoretical arguments, (2) explanation building to describe the mechanisms determining self-disclosure

behaviors, (3) time-series analysis to test whether the observed constructs vary across time, and (4) cross-case synthesis to examine similarities and differences of the profiled cases.

We selected the cases carefully to predict similar (i.e., literal replications) and contrasting results (i.e., theoretical replications). To do so, we conducted a survey (n = 140) prior to, and as a means for, selecting the cases. The selection criteria included demographics, SNSs activity, privacy concern, cognitive absorption, and self-disclosure. This selection method helps in establishing internal validity and theoretical generalization (Yin 2014). The fifteen selected cases were recruited from a large public southern university (Table 2). The empirical evidence was mainly collected from interviews (approx. 30 minutes) triangulated with the survey and archival SNS data (i.e., interviewees recalled their actual self-disclosures via their mobile devices). This triangulation method helps in establishing construct validity (Yin 2014). We chose Facebook as our context due to its popularity (Richter 2017; Statista, 2017). Nevertheless, our cases were allowed to elaborate on their attitudes and behaviors based on other SNSs.

Table 2. Descriptive Statistics

| Case Pseudonym | Age | Gender | Ethnicity | Education | Facebook Years | Facebook Friends |
|----------------|-----|--------|--------------------|-------------------|----------------|------------------|
| Anna | 19 | Female | Black | College Sophomore | 6 | 854 |
| Bob | 27 | Male | White non-Hispanic | Graduate | 10 | 1155 |
| David | 20 | Male | White non-Hispanic | College Sophomore | 7 | 989 |
| Dina | 49 | Female | Black | Graduate | 8 | 491 |
| Ella | 31 | Female | White non-Hispanic | College Senior | 8 | 118 |
| Eric | 21 | Male | Black | College Senior | 8 | 2498 |
| Ethan | 27 | Male | White Hispanic | Associate | 9 | 1579 |
| Gary | 30 | Male | White non-Hispanic | Graduate | 9 | 817 |
| Gordon | 49 | Male | White non-Hispanic | Graduate | 9 | 196 |
| Jake | 53 | Male | White non-Hispanic | Bachelor | 11 | 1320 |
| Macey | 20 | Female | White non-Hispanic | College Junior | 8 | 527 |
| Mark | 22 | Male | Other | College Senior | 9 | 362 |
| Phillip | 35 | Male | Asian | Associate | 9 | 235 |
| Rachael | 26 | Female | Asian | Graduate | 9 | 629 |
| Yara | 21 | Female | Asian | College Senior | 8 | 454 |

Note: mean age = 30 years; 40% female; 46% White non-Hispanic; 33% graduate; mean Facebook years = 8.53 years; mean Facebook friends = 815.

DATA ANALYSIS AND PROPOSITION DEVELOPMENT

The analysis revolves around three phenomena: 1) how cognitive absorption restrains users from thinking prudently when confronted with self-disclosure decisions, 2) how cognitive absorption magnifies perceived benefits and diminishes perceived privacy risks, and 3) how the effect of cognitive absorption attenuates when confronted with self-disclosures of sensitive information. Moreover, we consider a temporal aspect which shapes the patterns in these phenomena.

Phenomenon 1: Cognitive Absorption, Privacy Concerns, and Self-disclosure

First, we tested the established associations between privacy concerns, information sensitivity, and self-disclosures. We found strong evidence that SNS users do consider privacy concerns (both organizational and social) when self-disclosing personal information. This direct effect pattern emerged clearly in ten cases. In addition, all cases indicated that this direct effect is stronger when the sensitivity of information is high (e.g., address, political views, personal experiences, and family information). Sensitivity is a key factor even for those who are unconcerned, confirming this conditional pattern. Table 3 presents some evidence. Therefore, we concluded that self-disclosure behaviors depend on privacy concerns in general and may sometimes be conditional on perceived sensitivity. Next, we discuss how the effect of privacy concerns on self-disclosures is likely to be conditional on the state of cognitive absorption.

| Table 3. Examples of Evidence for the Effect of Privacy Concerns and Information Sensitivity on Self-disclosure |
|--|
| Privacy Concerns and Self-disclosure |
| <p><i>"It annoys me that Facebook or other people... be able to tell who I am. I also find it annoying how Facebook can use your data... concerned definitely about employers... and definitely random people, you never know who is out there... So, I don't post pictures ... I do not like posting my location on Facebook; that scares me... privacy wise like I really watch what I post... I don't post statuses anymore but I do share things or 'like' things."</i> [Macey, highly concerned]</p> <p><i>"Because of my concerns, I am not really posting things that I wouldn't like to be discovered there... there are some strangers out there who can easily access this information... So basically, I have a general profile. Like, if I go somewhere and I take pictures, I post them, but other than that I don't really share a lot of information."</i> [Ella, somewhat concerned]</p> <p><i>"I am not too concerned. I do not think it is an issue. I mean we are not posting things like I would not want anybody to see. It is not like anybody can use it against me. I am openly putting it out there."</i> [Eric, unconcerned]</p> |
| Privacy Concerns, Information Sensitivity, and Self-disclosure |
| <p><i>"I am pretty concerned but as far as what I share I do not share like certain things like my home, my family, my address you know things out of the norm... If me and my wife are having a fight I am not going to put that out there. It is our privacy."</i> [Ethan, highly concerned]</p> <p><i>"I definitely do not share my opinion on politics because it is not worth it... the costs outweigh the reward."</i> [David, somewhat concerned]</p> <p><i>"I have a system like whenever an event happens in my life I will post that, even in politics... There are some articles which I feel are a little too extreme to post... there is a 25%-30% chance that I would have to think about something before I post."</i> [Anna, unconcerned]</p> |

We proposed that higher cognitive absorption is associated with higher self-disclosures (i.e., direct pattern) coupled with deactivated privacy concerns leading to imprudent self-disclosures (i.e., conditional pattern). All cases supported the direct pattern. Those who lose track of time, engage heavily in the newsfeed, relish the moment, and browse curiously are more likely to self-disclose personal

information in the form of profile and status updates, comments, and ‘likes’. Bob stated that “*there is definitely a positive correlation there*” between cognitive absorption and self-disclosures.¹² Gary, whose absorption is generally low, very rarely updates his profile/status or comments on other users’ posts. The most he would do is a ‘like’ for certain friends only. Thus, we concluded that the cases support the direct pattern (for example of evidence, see Phenomenon 1 in Table 4). Twelve cases supported the conditional pattern which suggests that privacy concerns are likely to be inactive under a high cognitive absorption state. For example, Ethan and Macey are highly concerned about privacy. However, they are also highly absorbed:

“Whenever I put a status, I get a few ‘likes’ or comments and discuss things... one time I made a funny comment and I got a hundred ‘likes’ and I am like wow” [Ethan].

“I am more like let’s see what people posted, ‘like’, ‘like’, ‘like’ [‘liking’ self-disclosure]. It is enjoyable... you can read anything and share all that stuff. I like that” [Macey].

Such high absorption explained the imprudent self-disclosures involved in Ethan, Macey, and ten other cases. As Ethan reflected on his actual self-disclosures after browsing his Facebook activities, he found a number of posts that contradicted his privacy concerns. It appeared that nothing else seems to matter when he was engrossed in the social networking activity:

“I am a big anti-trump person, so whenever something pops up, I try like a meme or my opinion about it... Hopefully no employer looks at our stuff and sees that... Sometimes when I see something I am like that’s gay [commenting in a post]. It’s nothing against those gay people, but I feel if like my employer looked at my stuff that might affect me negatively... a lot of times whenever I say things, I don’t really think about it.”

The underlying mechanisms explaining such contradictory behaviors are 1) the positive association between cognitive absorption and informed self-disclosures and 2) the ability of cognitive absorption to deactivate privacy concerns and thus lead to uninformed or imprudent self-disclosures. These patterns emerged in the majority of the cases that described how attention to privacy is trivial or unattainable under high absorption. These mechanisms will be more evident in the next phenomenon.

Proposition 1: *High level of cognitive absorption with SNSs can lead to numerous negative outcomes including imprudent self-disclosure behaviors due to deactivated privacy concerns.*

¹² In all interviews, the term *cognitive absorption* was not used when measuring cognitive absorption (see Appendix A).

Table 4. Examples of Evidence from the Multiple-Case Study

| Phenomenon 1: Cognitive Absorption, Privacy Concerns, and Self-disclosure | |
|--|---|
| Cognitive Absorption | <i>"Yup, yup, I sometimes set it to look through most recent stuff and then I am trying catch myself up, the next thing I know it's been 30 or 45 minutes and I am still scrolling through stuff."</i> [Gordon, somewhat concerned] |
| Temporal Dissociation | <i>"I do get engaged sometimes in different things, sometimes you find different things like... when I find certain things, I am like "wow" this is surprising... So I do get engaged, I do comments... I do get engaged a lot ... it brings issue in my relationship with my wife, like my wife gets mad at me whenever like I am not paying attention to her. I feel like whenever I am on Facebook and she is talking to me, I don't listen to her sometimes and she gets mad and I am like 'I am sorry'."</i> [Ethan, highly concerned] |
| Immersion Engagement | <i>"I find enjoyment in this specific idea of having a good understanding of what everybody is up to... So, there is enjoyment in that and there is enjoyment in the entertainment factor like videos and stuff and sharing those enjoyments."</i> [David, somewhat concerned] |
| Enjoyment | <i>"I think that for the most part I control what I share."</i> [Bob, somewhat concerned] |
| Control | <i>"I think that's why I got on Facebook, to see what is going on in my friend's and family's lives. I'm very interested in seeing what is going on in their lives for sure... so yeah, I search through and see what's going. As long as I have some time, I'll continue to scroll."</i> [Gary, unconcerned at all] |
| Curiosity | |
| Phenomenon 2: Cognitive Absorption, Perceived Benefits, and Perceived Privacy Risks | |
| | <i>"I wasn't really thinking what I was posting [deactivated privacy concerns]. I just thought the moment was cool and did it [magnified perceived benefits]"</i> [Ethan, highly concerned] |
| | <i>"That is very at the moment sort of thing which I wouldn't really think through [deactivated privacy concerns], OK, what kind of consequences it can have later in terms of potential employers or strangers [diminished perceived risks]"</i> [Rachael, somewhat concerned] |
| Phenomenon 3.1: Cognitive Absorption and Information Sensitivity | |
| | <i>"Photos and locations... If you're enjoying, you would sometimes want to check-in, again everyone does, so you would want to do that. But I backed down...because again it is public information... it is captured, so anyone can view it. Even if I don't make it public, I know that there are ways of getting data from Facebook. So, I wouldn't probably want to take that risk."</i> [Rachael, somewhat concerned] |
| Phenomenon 3.2: Temporal Effect | |
| | <i>"Impulsiveness, you kinda do it before you think. It's not just that your friends could see it. Everybody could see it. It's not recent, over a year ago. I guess if you got to think about it you probably should not post it. It took me long time to see that, for me to realize that I cannot play with that... I don't have any 'likes' that I am ashamed of, not in recent years. The adult me, I am aware of what is going on."</i> [Eric, unconcerned] |

Note: Cognitive absorption was measured in a holistic manner such that each case was assigned one score reflecting his/her absorption level (see Table 5).

Additional evidence is presented in Table B.1, Appendix B.

Phenomenon 2: Cognitive Absorption, Perceived Benefits, and Perceived Privacy Risks

Cognitive absorption may heighten perceived benefits and diminishes perceived privacy risks leading to imprudent self-disclosures. To examine this effect in our case study, we asked the interviewees whether they have shared personal information in the past but later decided to delete, and more importantly why they shared that information in the first place. Eight cases indicated the deletion of information and two cases only thought about deletion. The remaining five cases did not delete any information, most likely because they had exhibited high levels of privacy control and prudent self-disclosures. Reflecting on such

retraction decisions, the cases not only provided support for the effect of cognitive absorption on perceived benefits and risks, but also added further support for Proposition 1 (for examples of evidence, see Phenomenon 2 in Table 4). The interviewees attributed their original self-disclosures to heightened perceived benefits and undermined perceived privacy risks along with absorption-related concepts.

Proposition 2: *High level of cognitive absorption with SNSs can magnify perceived benefits and diminish perceived privacy risks leading to imprudent self-disclosure behaviors.*

Phenomenon 3: Cognitive Absorption, Information Sensitivity, and Time

Intention to disclose sensitive information may undermine the absorption level by triggering privacy attitudes leading to prudent self-disclosures. To probe this argument, we asked the interviewees if they ever had an incident where they were about to share personal information but instantly decided to back down because they thought that the information is too private to be shared. Fourteen cases had experienced such incidents and the reason they decided not to share that information was the high sensitivity involved. The only case in which this incident did not happen is Gary, unsurprisingly because his self-disclosures are extremely prudent. In such a case, Gary managed the privacy boundary by limiting disclosure of sensitive information to a certain audience, for example his mother-in-law was not among those who could see his post that involved sexual situations. All other cases confirmed that the sensitivity level could bring about a nudge that relaxes the prevailing cognitive absorption state leading to prudent self-disclosure decisions (for examples of evidence, see Phenomenon 3.1 in Table 4).

Proposition 3.1: *Intentions to disclose sensitive information can attenuate the high level of cognitive absorption by activating privacy concerns leading to prudent self-disclosure behaviors.*

As can be seen, we used direct and indirect questions to examine how cognitive absorption explains the dichotomy between privacy concerns and self-disclosures. The most direct one was when we asked the interviewees to browse their actual disclosure activities and to identify any activity that does not adhere to their privacy concerns and to reflect on that activity. Eight cases were amazed at the high amount of information they have actually shared via status updates, comments, or ‘likes’, especially the highly concerned cases. Four others realized their impulsive ‘like’ revelations. Some concerned cases regretted the majority of their past disclosures and expressed a strong urge to retract those decisions by

removing statuses, photos, comments, and ‘likes’. While this information was once disclosed for a reason, the users now perceive such past disclosures to be imprudent. As a result, interviewees’ reflections on privacy concerns, self-disclosures, or cognitive absorption were time variant (for example of evidence, see Phenomenon 3.2 in Table 4). Thus, we further explore this temporal aspect.

Several cases exhibited high absorption in the first few years (Time 1: expressed as “*not recent*,” “*in the past*,” or “*back then*”), but the absorption level decreased in the current present or recent past (Time 2: expressed as “*now*,” “*these days*,” or “*recent*”). Although this reduction might be due to the presence of new SNS platforms, a significant temporal change in cognitive and privacy control was evident in ten cases. Cognitive control reflects the user’s perception of being in charge of the networking activity (Agarwal and Karahanna 2000). Privacy control is the perceived ability of controlling personal revelations (Dinev and Hart 2004). Users’ cognitive control over the networking activity was high while privacy control was low in Time 1. Besides, when low privacy control was attended by high temporal dissociation, immersion, enjoyment, and curiosity, privacy concerns, if any, were devoid of any effect on self-disclosures. In fact, some cases were less attentive to the privacy issue in Time 1.

The temporal effect provides a subtle and comprehensive explanation to the dichotomy in terms of 1) confirming the moderating effect of cognitive absorption and 2) addressing rival explanations (e.g., age, experience, maturity, and privacy awareness and control). Consider the following scenario derived from the observed data. In Time 1, typical users made various imprudent self-disclosures caused by inattention to privacy, unawareness of privacy risks, or due to low privacy control coupled with intense absorption state. In contrast, in Time 2, these users tended to avoid imprudent self-disclosures given their privacy concerns, awareness of privacy risks, or their high privacy control coupled with moderate absorption state. Note that Time 2 neither implies that users are capable of avoiding imprudent nor able to maintain extremely prudent disclosure behaviors. It simply suggests that users’ privacy attitudes, awareness, and cognition have evolved. This evolution which correlated with age, maturity, experience, and privacy control – i.e., time as a loaded construct – may or may not lead users to be attentive to their dispositional privacy concerns. Based on our cross-case synthesis (to be discussed next), one case [Yara]

evolved from imprudence to high prudence, whereas another case [Ethan] exhibited continuous imprudence in both time periods. The remaining cases are scattered along the imprudence-prudence continuum because cognitive absorption continued to explain the dichotomy in Time 2.

Inconsistent privacy behaviors were not only foreseeable but also inevitable given the rise in both informed (prudent) and uninformed (imprudent) self-disclosures caused by cognitive absorption. Further, users are incapable of purging their entire records of imprudent disclosures from Time 1, which they are being reminded of every now and then via the Facebook memory feature. This incapability leaves users with a psychological cost, uncertainty of privacy risk, and hence continued concerns for privacy.

Proposition 3.2: *Privacy concerns, information sensitivity, and cognitive absorption are time variant constructs, such that their interaction effect on self-disclosure behaviors can vary depending on how these constructs evolve across time.*

Case Description and Cross-Case Synthesis

Table 5 describes each case according to its imprudence-prudence, privacy concerns, and cognitive absorption. We developed a 6-point scale to describe each case. The scale reflects the inconsistency-consistency between privacy concerns and self-disclosures. High imprudence reflects extreme inconsistency. High prudence reflects extreme consistency. The final descriptions were developed based on understanding each case in its own right and the salience of a temporal effect. For example, Gary stated that he used to share his interests and favorites in the form of profile information when he first joined Facebook (Time 1) but has deleted such personal information later (Time 2). However, we describe Gary by ‘High Prudence’ without indication of a temporal change because he is not at all concerned and his disclosure of less sensitive information does not fall under paradoxical privacy behaviors. Similarly, Ethan is described by ‘Imprudence’ because this case, as a whole, appeared to be highly contradictory in both time periods. On the other hand, we consider the temporal effect in the description of ten cases in which a clear cognitive and behavioral change was salient. For instance, Rachael, Bob, Mark, and Ella are described as shifting from ‘Moderate Imprudence’ to ‘Prudence’ because their privacy concerns or sensitivity perception did not agree with their self-disclosures in Time 1 but the consistency level emerged in Time 2. The same logic applies to other descriptions, except Jake

who is described by ‘Self-determination’ as his self-disclosures were self-determined regardless of privacy or cognitive absorption.

Table 5. Case Description & Cross-Case Synthesis

| Case Pseudonym | Case Description | Privacy Concerns | Cognitive Absorption Effect | |
|----------------|---|--------------------|-----------------------------|-----------------|
| | | | Time 1 | Time 2 |
| Ethan | Imprudence | Highly Concerned | Very Likely | Very Likely |
| Macey | Imprudence → Moderate Prudence | | Very Likely | Likely |
| David | Moderate Imprudence → Moderate Prudence | Somewhat Concerned | Very Likely | Likely |
| Gordon | Moderate Prudence → Prudence | | Likely | Fair Likelihood |
| Phillip | Moderate Prudence → Prudence | | Likely | Fair Likelihood |
| Rachael | Moderate Imprudence → Prudence | | Very Likely | Fair Likelihood |
| Bob | Moderate Imprudence → Prudence | | Very Likely | Fair Likelihood |
| Mark | Moderate Imprudence → Prudence | | Very Likely | Fair Likelihood |
| Ella | Moderate Imprudence → Prudence | | Very Likely | Fair Likelihood |
| Dina | Moderate Prudence | | Fair Likelihood | Fair Likelihood |
| Anna | Prudence | Unconcerned | Unlikely | Unlikely |
| Eric | Moderate Imprudence → Prudence | | Very Likely | Unlikely |
| Jake | Self-determination | | Unlikely | Unlikely |
| Yara | Imprudence → High Prudence | Unconcerned at All | Very Likely | Very Unlikely |
| Gary | High Prudence | | Very Unlikely | Very Unlikely |

Case description scale: High Imprudence, Imprudence, Moderate Imprudence, Moderate Prudence, Prudence, High Prudence

Cognitive absorption effect scale: Very Unlikely, Unlikely, Fair Likelihood, Likely, Very Likely

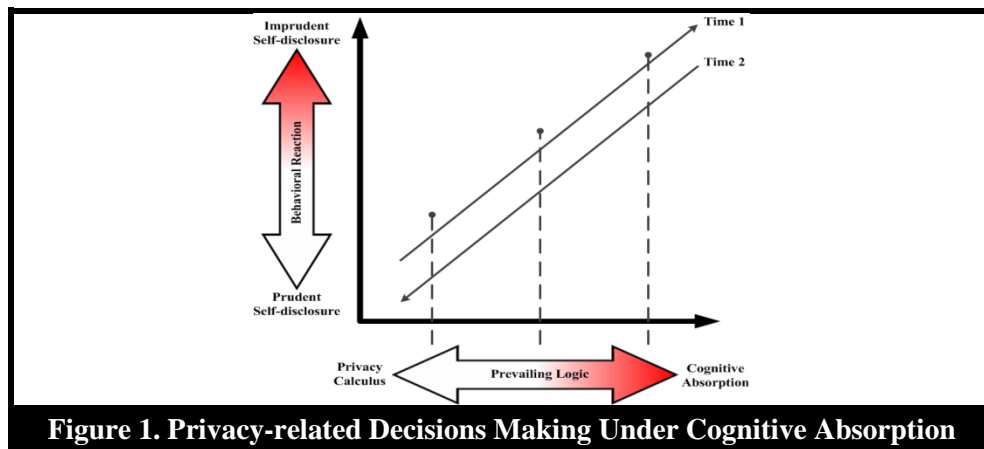
This synthesis also shows the distribution of privacy concerns: highly concerned (13.3%), somewhat concerned (46.6%), unconcerned (26.6%), and unconcerned at all (13.3%). The column on the right side reflects the susceptibility of each case across the two time periods to exert cognitive absorption that affected self-disclosures in general or deactivated privacy concerns at the moment of social networking. Overall, the synthesis conveys two major insights. First, the inconsistency between privacy concerns and self-disclosures is most noticeable in Time 1 and it tends to disappear in Time 2. This inference can be validated by observing the temporal effect associated with the case descriptions. Ten cases reflect a positive change as they improved in terms of aligning their privacy concerns with self-disclosures while none of the cases shifted from a prudent stage to an imprudent one. Second, the effect of cognitive absorption on self-disclosures and/or deactivating privacy concerns is most salient in Time 1. While past self-disclosures of three cases were ‘unlikely’ or ‘very unlikely’ affected by cognitive absorption, ten cases were ‘very likely’ and two others were ‘likely’ affected by cognitive absorption in Time 1. This effect, however, attenuates as we move to Time 2. The effect is ‘very likely’ only in one case, ‘likely’ in two cases, and ‘fairly likely’ in seven others. The effect is ‘unlikely’ or ‘very unlikely’ in

the remaining five cases. The salience in Time 1 and attenuation in Time 2 of the cognitive absorption effect correlates with the case descriptions. In other words, the more likelihood of a cognitive absorption effect, the more imprudent is the case description. Likewise, the less likelihood of a cognitive absorption effect, the more prudent is the case description.

DISCUSSION

Explaining the Privacy Paradox through Cognitive Absorption

Figure 1 depicts the process involved in self-disclosure behaviors as reframed under the assumptions of the privacy calculus and cognitive absorption. The x-axis maps the prevailing logic and the y-axis maps the behavioral reaction. The highly prudent privacy calculus prevails at the left of the x-axis, depicted in a gradient white color. At this point, users adopt the risk-benefit analysis mode along with active privacy concerns (i.e., high effort processing, Dinev et al. 2015) leading to low-to-moderate prudent self-disclosures. The highly expedient cognitive absorption prevails at the right of the x-axis, depicted in a gradient red (dark) color. At this point, users succumb to cognitive absorption (i.e., low effort processing) leading to moderate-to-high imprudent self-disclosures. The behavioral reaction tends toward more prudent disclosures at the bottom of the y-axis, depicted in a gradient white color, and more imprudent disclosures at the top, depicted in a gradient red (dark) color. The temporal progression begins from early forms of prudent, calculated self-disclosures (lower left area) to later forms of imprudent, expedient self-disclosures (upper right area) where the temporal effect matures and reverses the progression.



Consider a user who just joined Facebook. She would not be expected to pursue imprudent self-disclosures in the early days when she started using Facebook. She might actually be apprehensive about providing personal information when she first signed up. Also, it would have taken her a few days or weeks to get acquainted with Facebook. This stage is depicted by the dotted-line in the left side of Figure 1 where cognitive absorption is at its minimum leading to prudent self-disclosures. A few weeks later, however, this user may become very absorbed in Facebook where she begins pursuing imprudent disclosure behaviors. This is depicted by the middle-dotted line where the level of disclosure shifts from prudence toward imprudence. This early, although rapid, progression was also observed in the case study indicating that as cognitive absorption becomes greater, self-disclosures are likely to be imprudent. From our case study, the disclosure behavior of Anna, Ella, and Gordon fit in the continuum between the middle-dotted line and the one situated in the right side of Figure 1. Such users exhibited a compulsive use of the 'like' button. This pursuit, which reflects their perceived benefits of the social networking activity, restrained them from thinking about potential privacy risks, such as unintended exposure of personal preferences. Eventually, there is a possibility that users become thoroughly absorbed and tend to exhibit high imprudent self-disclosures with complete overlook of privacy. Ethan's prudent and imprudent self-disclosures were part of his daily activities in which he was intrinsically rewarded by seeing others reacting to his posts. Although prudent thinking would not prevent sharing less sensitive information, it would absolutely inhibit sharing sensitive information as shown in our case study and prior research (Taddicken 2014; Xie and Kang 2015). Nonetheless, nothing else would seem to matter when the social networking activity is intrinsically rewarding and highly enjoyable especially under idle privacy concern, control, and awareness.

Importantly, self-disclosures might shift on this continuum from the peak imprudent down to the prudent calculus. For instance, the stimuli that nudged many of our cases to remove unprofessional posts (Time 1) made them aware of the importance of personal privacy, and consequently returned to the privacy calculus (Time 2). In online shopping, requests for highly sensitive information, such as social security number, can immediately shift users from cognitive absorption to the privacy calculus. On the

other hand, users might reach the absorption state at the early stages of an online activity. For example, impulsive acceptance of a privacy statement reflects a state of cognitive absorption in a sense that, at a very early stage, acquiring the service is what a user pays the most attention to regardless of future privacy consequences. However, reading the privacy statement brings about an undesirable cognitive dissonance which opposes the pleasant absorption state. Individuals in a cognitive absorption state tend to suppress the activation of any construct that has potential of cognitive dissonance (Nakamura and Csikszentmihalyi 2002), and therefore we argue that this is the fundamental behind the dichotomy between privacy concerns and self-disclosure behaviors in the context of SNSs.

This phenomenon may not be an issue of rationality versus irrationality. Rather it may be an issue of different realms of rationality: prudence versus imprudence, high versus low effort cognitive processing (Dinev et al. 2015). These different realms of rationality inhabit the privacy calculus and cognitive absorption respectively. For example, Ethan's exuberant Facebook use might be regarded as making a rational decision based on magnified benefits and underestimated risks: rationality bounded by limited cognition (Acquisti et al. 2016).

Future Research

Future research is needed to test our propositions in other contexts (e.g., other SNSs, location-based apps, e-commerce, and online games) using different methods (e.g., surveys and experiments). It will be insightful to explore cognitive absorption in less mature SNSs (e.g., Snapchat) and to observe the dynamics of self-disclosures along with privacy concerns in a way to test the main assumption of our theory. Longitudinal studies would be suitable for such examination. Users' privacy behaviors may also depend on the privacy features afforded. For instance, Facebook continues to enhance its privacy settings by allowing users to control their revelations. Its new face recognition feature will alert users whenever their images appear in photos uploaded by others (Candela 2017). It enables users to be aware of their information privacy, and hence alleviating the incomplete information dilemma (Acquisti et al. 2016, 2017). Users' revelations in the form of a story (e.g., Facebook and Snapchat) disappear within 24 hours

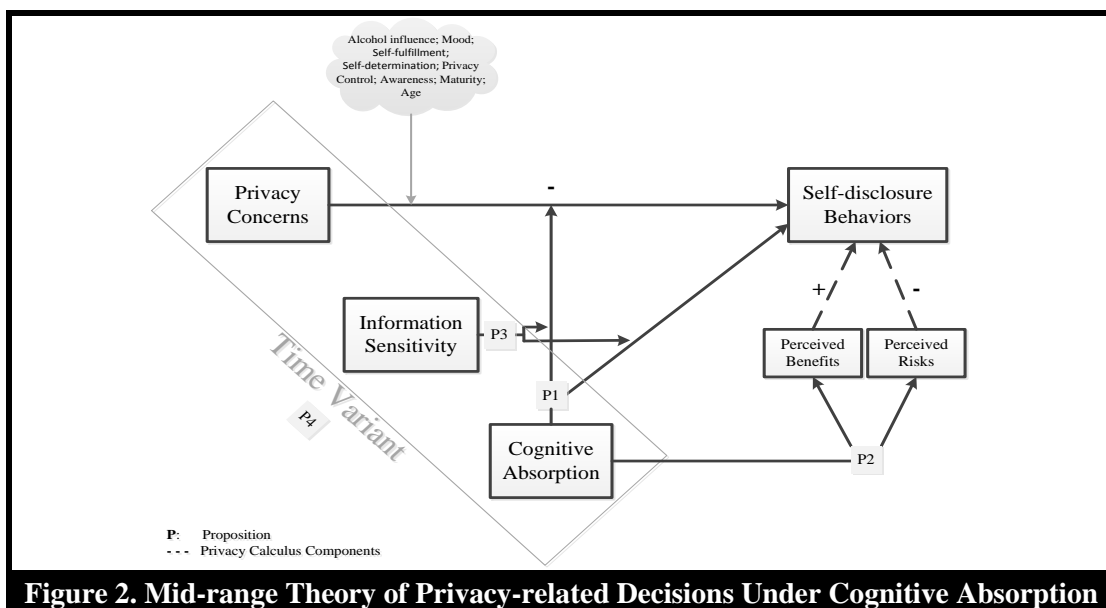
which could eliminate users' psychological costs associated with future privacy risks. Such features can be identified as other boundary conditions to explain anomalies in privacy behaviors.

In other domains, such as online auction, cognitive absorption can explain the prevalence of undesirable outcomes (e.g., winner's regret) that contradict espoused bidding attitudes (Park et al. 2016). It can also explain adverse consequences in online shopping (e.g., debt accumulation), gaming (e.g., fatigue), and streaming services (e.g., sleep deprivation). While research has shown these negative effects (Bridges and Florsheim 2008; Chou and Ting 2003; Turel and Serenko 2012), there is dearth of literature explaining why users' attitudes toward online shopping, gaming, and other technologies are inconsistent with their actual behaviors. The research roadmap we articulated can serve well to study attitude-behavior discrepancies in other domains. Our findings help improve our understanding of privacy, security, and other IS paradoxical phenomena that cannot be explained solely by classic behavioral theories, such as theory of planned behavior and protection motivation theory (Ajzen 1991; Rogers 1975).

Such a roadmap should also aim to present practical solutions to the problems being addressed. For example, our empirical findings suggest a need for applying new features to address imprudent behaviors that often result in unintended exposure, regret, embarrassment, and job denial. One promising solution is the application of nudges (Acquisti et al. 2017). Given advanced machine learning and sentiment analysis tools, SNSs are capable of introducing features that nudge users prior to self-disclosing an apparently improper content. SNSs can also infer users' privacy preferences based on their use of privacy settings. By having a database of users' privacy preferences, SNSs can tailor these preferences to the nudging design. For instance, a user who has strict privacy preferences and is about to post sensitive information or improper content can be warned via a pop-up to remind the user of her privacy preferences and potential exposure of the post. This nudge is aimed to reactivate dispositional privacy concerns in hot states like cognitive absorption. The nudging paradigm, however, presents institutional, design, and ethical challenges that are outside the scope of our study (see Acquisti et al. 2017).

Theoretical Advances

Our research questions arise in a way that conforms to approximation and problematization methodology (Alvesson and Sandberg 2011; Van de Ven 2007; Weick 1995). Alvesson and Sandberg (2011) encourage researchers “to produce more novel research questions and theories by actively questioning and critically scrutinizing established knowledge in academia” (p. 267). First, we elaborated the state of the art in privacy research and articulated a research roadmap for studying privacy behaviors. Then, we leveraged the context of SNSs (Alvesson and Kärreman 2007; John 2006) in order to construct a mid-range theory that explains inconsistencies in privacy behaviors. The reality of discrepancies in privacy behaviors is a social phenomenon too rich to be fully understood by one perspective (Acquisti et al. 2016). For this reason, we adopted an abductive theory-building approach by creating a new conjecture (cognitive absorption) to make the surprising anomaly (privacy paradox) part of our normal understanding of privacy-related decisions (Van de Ven 2007). Deductive and inductive reasoning were also applied as we drew upon existing theories (i.e., privacy calculus and enhanced APCO model) while relying on empirical data to support the theorized conjecture (Miles et al. 2014). Our resulting mid-range theory is depicted in Figure 2.



The framework emphasizes a moderating effect of cognitive absorption on the relationship between privacy concerns and self-disclosure behaviors in addition to a direct effect (*Proposition 1*). It incorporates constructs from the privacy calculus and shows an indirect effect of cognitive absorption on self-disclosure behaviors through magnifying perceived benefits and undermining perceived privacy risks (*Proposition 2*). The more sensitive the information to be disclosed, the more likely privacy concerns will overpower cognitive absorption. Accordingly, intent to disclose sensitive information relaxes the absorption effect as privacy concerns become more salient, resulting in a 3-way interaction (*Proposition 3*). Cognitive absorption, privacy concerns, and information sensitivity are time variant constructs, such that their individual and collective effects on self-disclosure may vary depending on their evolution across time (*Proposition 4*). The gray cloud in Figure 2 lists some rival explanations derived from our case study that could also explain the dichotomy. We did not elaborate these factors minutely as the explanatory power of alcohol influence or mood is specific to certain situations while our consideration of the temporal effect accounts for the effect of other factors (e.g., privacy control, awareness, maturity, and age). This theoretical framework and its rival explanations provide interesting research opportunities.

CONCLUSION

Cognitive absorption is a highly relevant construct in the context of SNSs. Although it has positive outcomes, such as continued use, engagement, and enjoyment, it can have negative outcomes, such as overlooking privacy preferences and underestimating privacy risks. Our study suggests that high levels of cognitive absorption in the social networking activity can explain why SNSs users' dispositional privacy concerns are sometimes inconsistent with their self-disclosure behaviors, the privacy paradox phenomenon.

REFERENCES

- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., and Wilson, S. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys* (50:3), Article 44.
- Acquisti, A., and Fong, C. M. 2015. "An Experiment in Hiring Discrimination Via Online Social Networks," Retrieved (January, 19, 2017) from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031979
- Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technology*, G. Danezis and P. Golle (eds.), Cambridge, UK: 6th International Workshop, pp. 36-58.
- Acquisti, A., and Grossklags, J. 2004. "Privacy Attitudes and Privacy Behavior," in *Economics of Information Security*, J. Camp, and R. Lewis (eds.), US: Springer, pp. 165-178.
- Acquisti, A., John, L. K., and Loewenstein, G. 2012. "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research* (49:2), pp. 160-174.
- Acquisti, A., Taylor, C. R., and Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (52:2), pp. 1-64.
- Adjerid, I., Acquisti, A., Loewenstein, G. 2018a. "Choice Architecture, Framing, and Cascaded Privacy Choices," *Management Science* (article in advance), pp. 1-24.
- Adjerid, I., Peer, E., and Acquisti, A. 2018b. "Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making," *MIS Quarterly* (42:2), pp. 465-488.
- Adjerid, I., Samat, S., and Acquisti, A. 2016. "A Query-Theory Perspective of Privacy Decision Making," *The Journal of Legal Studies* (45:S2), pp. S97-S121.
- Agarwal, R., and Karahanna, E. 2000. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage," *MIS Quarterly* (24:4), pp. 665-694.
- Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.
- Alashoor, T., Al-Maidani, N., and Al-Jabri, I. 2018. "The Privacy Calculus under Positive and Negative Mood States," in *Proceedings of the 39th International Conference on Information Systems*, San Francisco, United States.
- Alashoor, T., Fox, G., and Smith, H. J. 2017a. "The Priming Effect of Prominent IS Privacy Concerns Scales on Disclosure Outcomes: An Empirical Examination," in *Proceedings of Pre-ICIS Workshop on Information Security and Privacy*, Seoul, South Korea.
- Alashoor, T., Han, S., and Joseph, R. C. 2017b. "Familiarity with Big Data, Privacy Concerns, and Self-Disclosure Accuracy in Social Networking Websites: An APCO Model," *Communications of the Association for Information Systems* (41), pp. 62-96.
- Alvesson, M., and Kärreman, D. 2007. "Constructing Mystery: Empirical Matters in Theory Development," *Academy of Management Review* (32:4), pp. 1265-1281.
- Alvesson, M., and Sandberg, J. 2011. "Generating Research Questions Through Problematization," *Academy of Management Review* (36:2), pp. 247-271.
- Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469-490.
- Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.
- Baek, Y. M. 2014. "Solving the Privacy Paradox: A Counter-Argument Experimental Approach," *Computers in Human Behavior* (38), pp. 33-42.
- Barnes, S. 2006. "A Privacy Paradox: Social Networking in the United States," *First Monday* (11:9). Retrieved (February, 14, 2018) from <http://firstmonday.org/article/view/1394/1312>

- Barth, S., and de Jong, M. 2017. "The Privacy paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review," *Telematics and Informatics* (34), pp. 1038-1058.
- 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. 1017-1041.
- Bergstrom, B. 2018. "101 Social Media Statistics You Need to Know to Build Your 2018 Strategy," *CoSchedule*. Retrieved (January, 15, 2018) from <https://coschedule.com/blog/social-media-statistics/>
- 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.
- Breward, M., Hassanein, K., and Head, M. 2017. "Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach," *Information Systems Research* (28:4), pp. 760-774.
- Breznitz, D., Murphree, M., and Goodman, S. 2011. "Ubiquitous Data Collection: Rethinking Privacy Debates," *Computer* (44:6), pp. 100-102.
- Bridges, E., and Florsheim, R. 2008. "Hedonic and Utilitarian Shopping Goals: The Online Experience," *Journal of Business research* (61:4), pp. 309-314.
- Buchanan, T., Paine, C., Joinson, A., and Reips, U. 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.
- Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., and Perry, D. 1989. "Maintaining and Restoring Privacy Through Communication in Different Types of Relationships," *Journal of Social and Personal Relationships* (6:2), pp. 131-158.
- Busse, C., Kach, A.P., and Wagner, S. M. 2017. "Boundary Conditions: What They Are, How to Explore Them, Why We Need Them, and When to Consider Them," *Organizational Research Methods* (20:4), pp. 574-609.
- Candela, J. Q. 2017. "Managing Your Identity on Facebook with Face Recognition Technology," *Facebook*. Retrieved (February, 13, 2018) from: <https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/>
- Cao, J., Basoglu, K. A., Sheng, H., and Lowry, P. B. 2015. "A Systematic Review of Social Networks Research in Information Systems: Building a Foundation for Exciting Future Research," *Communications of the Association for Information Systems* (36), pp. 727-758.
- Cavusoglu, H., Phan, T. Q., Cavusoglu, H., and Airoidi, E. M. 2016. "Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook," *Information Systems Research* (27:4), pp. 848-879.
- Chen, A., Lu, Y., Chau, P. Y., and Gupta, S. 2014. "Classifying, Measuring, and Predicting Users' Overall Active Behavior on Social Networking Sites," *Journal of Management Information Systems* (31:3), pp. 213-253.
- Chen, H. T., and Chen, W. 2015. "Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection," *Cyberpsychology, Behavior, and Social Networking* (18:1), pp. 13-19.
- Chen, K., and Rea, A. I. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques," *The Journal of Computer Information Systems* (44:4), pp. 85-92.
- Choi, B. C., Jiang, Z., Xiao, B., and Kim, S. S. 2015. "Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding," *Information Systems Research* (26:4), pp. 675-694.
- Choi, H., Park, J., and Jung, Y. 2018. "The Role of Privacy Fatigue in Online Privacy Behavior," *Computers in Human Behavior* (81), pp. 42-51.

- Chou, T. J., and Ting, C. C. 2003. "The Role of Flow Experience in Cyber-Game Addiction," *CyberPsychology & Behavior*, (6:6), pp. 663-675.
- Cozby, P. C. 1973. "Self-Disclosure: A Literature Review," *Psychological Bulletin* (79:2), pp. 73-91.
- Craig, T., and Ludloff, M. E. 2011. *Privacy and Big Data*, Sebastopol, California: O'Reilly Media, Inc.
- Csikszentmihalyi, M. 1975. *Beyond Boredom and Anxiety*, San Francisco: Jossey-Bass Publishers.
- Csikszentmihalyi, M. 1990. *Flow: The Psychology of Optimal Experience*, New York: Harper & Row.
- 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.
- Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323-342.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1992. "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace," *Journal of applied social psychology* (22:14), pp. 1111-1132.
- Debatin, B., Lovejoy, J. P., Horn, A. K., and Hughes, B. N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* (15:1), pp. 83-108.
- Dinev, T. 2014. "Why Would We Care about Privacy?," *European Journal of Information Systems* (23:2), pp. 97-102.
- Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model," *Behaviour & Information Technology* (23:6), pp. 413-422.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80,100.
- 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.
- D'Souza, G., and Phelps, J. E. 2009. "The Privacy Paradox: The Case of Secondary Disclosure," *Review of Marketing Science* (7:1), pp. 1-29.
- Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., and Madden, M. 2015. "Frequency of Social Media Use," *The Pew Research Center*. Retrieved (February, 14, 2018) from <http://www.pewinternet.org/2015/01/09/frequency-of-social-media-use-2/>
- Ellison, N. B., Steinfield, C., and Lampe, C. 2007. "The Benefits of Facebook "Friends": Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication* (12:4), pp. 1143-1168.
- Gundecha, P., and Liu, H. 2012. "Mining Social Media: A Brief Introduction," *Tutorials in Operations Research* (1:4), pp. 1-17.
- Hargittai, E., and Marwick, A. 2016. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy," *International Journal of Communication* (10), pp. 3737-3757.
- Hong, W., and Thong, J. Y. L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.
- Hurwitz, J., Nugent, A., Halper, F., and Kaufman, M. 2013. *Big Data for Dummies*, Hoboken, New Jersey: John Wiley and Sons, Inc.
- James, T. L., Warkentin, M., and Collignon, S. E. 2015. "A Dual Privacy Decision Model for Online Social Networks," *Information & Management* (52:8), pp. 893-908.
- Jiang, Z., Heng, C. S., and Choi, B. C. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579-595.
- John, L. K., Acquisti, A., and Loewenstein, G. 2010. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* (37:5), pp. 858-873.
- Johns, G. 2006. "The Essential Impact of Context on Organizational Behavior," *Academy of Management Review* (31:2), pp. 386-408.

- Joinson, A. N., and Paine, C. B. 2007. "Self-Disclosure, Privacy and the Internet," in *The Oxford Handbook of Internet Psychology*, A. Joinson, K. McKenna, T. Postmes, and U. Reips (eds.), New York, USA: Oxford University Press Inc., pp. 237-252.
- Kahneman, D. 2011. *Thinking, Fast and Slow*, New York: Farrar, Straus and Giroux.
- Kane, G. C., Alavi, M., Labianca, G., and Borgatti, S. P. 2014. "What's Different about Social Media Networks? A Framework and Research Agenda," *MIS Quarterly* (38:1), pp. 275-304.
- Karwatzki, S., Dytynko, O., Trenz, M., and Veit, D. 2017. "Beyond the Personalization-Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* (34:2), pp. 369-400.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.
- Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., and Abdullat, A. 2015. "The Role of Mobile-Computing Self-Efficacy in Consumer Information Disclosure," *Information Systems Journal* (25:6), pp. 637-667.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior," *International Journal of Human - Computer Studies* (71:12), pp. 1163-1173.
- Ko, H. C. 2013. "The Determinants of Continuous Use of Social Networking Sites: An Empirical Study on Taiwanese Journal-Type Bloggers' Continuous Self-Disclosure Behavior," *Electronic Commerce Research and Applications* (12:2), pp. 103-111.
- Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), pp. 122-134.
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.
- Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture - Intercultural Dynamics of Privacy Calculus," *Business and Information Systems Engineering* (4:3), pp. 127-135.
- Ku, Y. C., Chen, R., and Zhang, H. 2013. "Why Do Users Continue Using Social Networking Sites? An Exploratory Study of Members in the United States and Taiwan," *Information & Management* (50:7), pp. 571-581.
- LaRose, R., Kim, J., and Peng, W. 2010. "Addictive, Compulsive, Problematic, or Just Another Media Habit?," in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Z. Papacharissi (ed.), New York, NY: Routledge, pp. 59-81.
- Leong, P. 2011. "Role of Social Presence and Cognitive Absorption in Online Learning Environments," *Distance Education* (32:1), pp. 5-28.
- Li, H., Luo, X. R., Zhang, J., and Xu, H. 2017. "Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors," *Information & Management* (54:8), pp. 1012-1022.
- Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), pp. 434-445.
- Li, T., and Slee, T. 2014. "The Effects of Information Privacy Concerns on Digitizing Personal Health Records," *Journal of the Association for Information Science and Technology* (65:8), pp. 1541-1554.
- Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28:28), pp. 453-496.
- Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp. 471-481.

- Lin, H. F. 2009. "Examination of Cognitive Absorption Influencing the Intention to Use a Virtual Community," *Behaviour & Information Technology* (28:5), pp. 421-431.
- 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.
- 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.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., and Byers, A. H. 2011. "Big Data: The Next Frontier for Innovation, Competition, and Productivity," *McKinsey Global Institute Report*. Retrieved (February, 14, 2018) from <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>
- Marwick, A. E., and boyd, D. 2014. "Networked Privacy: How Teenagers Negotiate Context in Social Media," *New Media & Society* (16:7), pp. 1051-1067.
- Meredith, S. 2018. "Here's Everything You Need to Know About the Cambridge Analytica Scandal," *CNBC*. Retrieved (June 6, 2018) from <https://www.cnn.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html>
- Miles, B. M., Huberman, A. M., and Saldana, J. 2014. *Qualitative Data Analysis: A Methods Sourcebook*. Thousand Oaks, California: SAGE Publications, Inc.
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76-98.
- Myers, M. D. (2013). *Qualitative Research in Business & Management*. Thousand Oaks, California: SAGE Publications, Inc.
- Nakamura, J., and Csikszentmihalyi, M. 2002. "The Concept of Flow," in *Handbook of Positive Psychology*, C. R. Snyder and S. J. Lopez (eds.), Oxford: Oxford University Press, pp. 89-105.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.
- Omarzu, J. 2000. "A Disclosure Decision Model: Determining How and When Individuals Will Self-Disclose," *Personality and Social Psychology Review* (4:2), pp. 174-185.
- Ozdemir, Z. D., Smith, H. J., and Benamati, J. H. 2017. "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study," *European Journal of Information Systems* (26:6), pp. 642-660.
- Park, S. C., Keil, M., Bock, G. W., and Kim, J. U. 2016. "Winner's Regret in Online C2C Auctions: an Automatic Thinking Perspective," *Information Systems Journal* (26:6), pp. 613-640.
- Peters, A. N., Winschiers-Theophilus, H., and Mennecke, B. E. 2015. "Cultural Influences on Facebook Practices: A Comparative Study of College Students in Namibia and the United States," *Computers in Human Behavior* (49), pp. 259-271.
- Petronio, S. S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*, Albany, NY: SUNY Press.
- Petty, R. E., and Briñol P. 2010. "Attitude Change," in *Advanced Social Psychology: The State of the Science*, R. F. Baumeister and E. J. Finkel (eds.), Oxford, UK: Oxford University Press, pp. 217-259.
- Petty, R. E., and Cacioppo, J. T. 1986. *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*, New York: Springer-Verlag.
- Popper, K. R. 1959. *The Logic of Scientific Discovery*. London and New York: Routledge.
- Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the UK Who Use Online Communities," *European Journal of Information Systems* (19:2), pp. 181-195.
- Rainie, L. 2016. "The State of Privacy in Post-Snowden America," *The Pew Research Center*. Retrieved (January, 16, 2017) from <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>

- Rainie, L. 2018. "Americans' Complicated Feelings about Social Media in an Era of Privacy Concerns," *The Pew Research Center*. Retrieved (April 11, 2018) from <http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>
- Rainie, L., Kiesler, S., Kang, R., and Madden, M. 2013. "Anonymity, Privacy, and Security Online," *The Pew Research Center*. Retrieved (February, 14, 2018) from <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
- Richter, F. 2017. "Facebook Inc. Dominates the Social Media Landscape," *Statista*. Retrieved (January, 15, 2018) from <https://www.statista.com/chart/5194/active-users-of-social-networks-and-messaging-services/>
- Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91:1), pp. 93-114.
- Rouis, S. 2012. "Impact of Cognitive Absorption on Facebook on Students' Achievement," *Cyberpsychology, Behavior and Social Networking* (15:6), pp. 296-303.
- Saadé, R., and Bahli, B. 2005. "The Impact of Cognitive Absorption on Perceived Usefulness and Perceived Ease of Use in On-Line Learning: An Extension of the Technology Acceptance Model," *Information & Management* (42:2), pp. 317-327.
- Schmarzo, B. 2013. *Big Data: Understanding How Data Powers Big Business*, Indianapolis, Indiana: John Wiley & Sons, Inc.
- Simon, H. A. 1982. *Models of Bounded Rationality: Empirically Grounded Economic Reason*. Cambridge, MA: MIT Press.
- Sly, J.L. 2018. "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *The Washington Post*. Retrieved (January, 29, 2018) from https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.39d417d19cc7
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.
- 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.
- Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477-560.
- Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM conference on Electronic Commerce*, Tampa, Florida, USA.
- Statista 2017. "Frequency of Facebook Use in the United States as of October 2017," *Statista*. Retrieved (January, 15, 2018) from <https://www.statista.com/statistics/199266/frequency-of-use-among-facebook-users-in-the-united-states/>
- Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp. 36-49.
- Stutzman, F., Gross, R., and Acquisti, A. 2013. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook," *Journal of Privacy and Confidentiality* (4:2), pp. 7-41.
- Sun, Y., Liu, D., and Wang, N. 2017. "A Three-Way Interaction Model of Information Withholding: Investigating the Role of Information Sensitivity, Prevention Focus, and Interdependent Self-Construct," *Data and Information Management* (1:1), pp. 61-73.
- Taddicken, M. 2014. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure," *Journal of Computer-Mediated Communication* (19:2), pp. 248-273.
- Tamir, D. I., and Mitchell, J. P. 2012. "Disclosing Information about the Self is Intrinsically Rewarding," in *Proceedings of the National Academy of Sciences* (109:21), pp. 8038-8043.

- Tellegen, A., and Atkinson, G. 1974. "Openness to Absorbing and Self-Altering Experiences ("Absorption"), a Trait Related to Hypnotic Susceptibility," *Journal of Abnormal Psychology* (83:3), pp. 268-277.
- Tufekci, Z. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society* (28:1), pp. 20-36.
- Turel, O., and Serenko, A. 2012. "The Benefits and Dangers of Enjoyment with Social Networking Websites," *European Journal of Information Systems* (21:5), pp. 512-528.
- Utz, S., and Kramer, N. 2009. "The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (3:2), Article 2.
- Van de Ven, A. H. 2007. *Engaged Scholarship: A Guide for Organizational and Social Research*. New York: Oxford University Press Inc.
- Varadarajan, S., and Soundarapandian, 2013. "Maximizing Insight from Unstructured Data," *Business Intelligence Journal* (18:3), pp. 17-25.
- Venkatesh, V. 1999. "Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation," *MIS Quarterly* (23:2), pp. 239-260.
- Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157-174.
- Webster, J., and Hackley, P. 1997. "Teaching Effectiveness in Technology-Mediated Distance Learning," *Academy of Management Journal* (40:6), pp. 1282-1309.
- Webster, J., and Ho, H. 1997. "Audience Engagement in Multi-Media Presentations," *ACM SIGMIS Database* (28:2), pp. 63-77.
- Weick, K. E. 1995. "What Theory Is Not, Theorizing Is," *Administrative Science Quarterly* (40:3), pp. 385-390.
- Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431-453.
- Whetten, D. A. 1989. "What Constitutes a Theoretical Contribution?," *Academy of Management Review* (14:4), pp. 490-495.
- Wottrich, V. M., van Reijmersdal, E. A., and Smit, E. G. 2018. "The Privacy Trade-Off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns," *Decision Support Systems* (106), pp. 44-52.
- Xie, W., and Kang, C. 2015. "See You, See Me: Teenagers' Self-Disclosure and Regret of Posting on Social Network Site," *Computers in Human Behavior* (52), pp. 398-407.
- Xu, F., Michael, K., and Chen, X. 2013. "Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model," *Electronic Commerce Research* (13:2), pp. 151-168.
- Xu, H., Teo, H., Tan, B. C., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-174.
- Yin, R. K. 2014. *Case Study Research: Design and Methods*. Thousand Oaks, California: SAGE Publications, Inc.
- Yu, J., Hu, P. J. H., and Cheng, T. H. 2015. "Role of Affect in Self-Disclosure on Social Network Websites: A Test of Two Competing Models," *Journal of Management Information Systems* (32:2), pp. 239-277.
- Yun, H., Lee, G., and Kim, D. 2014. "A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.

APPENDIX A (INTERVIEW PROTOCOL)

Self-Disclosure

- 1- How comprehensive and complete is your Facebook profile?
- 2- Tell us whether you have the following listed on your Facebook profile:
(Real name, work, education, birthdate, email, phone, address, family members, relationship status, places you have visited, details about yourself such as interests, favorite sport, music, and books)
- 3- How often do you update your Facebook profile and what triggers you to make such updates?
- 4- How often do you update your Facebook status? Tell us more about the type of information you share on your status updates.
- 5- When and why do you share information (e.g., status updates, photos, videos, comments, location tag, etc.) on Facebook?

Privacy Concerns

- 1- How concerned are you about the privacy of information you have shared on Facebook?
- 2- Tell us more about your privacy concerns on Facebook, such as type of information you're most concerned about, least concerned about, potential invasions (by schools, governments, employers, third parties, strangers, friends, family members) of your Facebook privacy.

Cognitive Absorption, Self-Disclosure, and Privacy Concerns

- 1- When you use Facebook, do feel that you spend more time on it than you had intended, such that time flies by, or you lose track of time?
- 2- When you use Facebook, how engaged are you with Facebook and the material available on it? For example, do you read your friends' updates, comment on what interests you, add more friends, and share interesting material with others?
- 3- How enjoyable is the time you spend with Facebook?
- 4- When you use Facebook, how curious are you about reading your friends' updates, looking at the photos and videos they share, and writing some comments? For example, do you keep scrolling down to read and look more at your friends' updates, photos, videos, news, etc.
- 5- Can you browse your Facebook Timeline – between now and the past few years – and tell us what kinds of things you have shared or 'liked' in the past.
 - 5a- Would you be concerned about the privacy of that information (for example, it could be misused or used in a way you did not foresee)?
 - 5b- Why did you share that information on Facebook at that time?
- 6- Many Facebook users express high concerns about their privacy but at the same time they disclose a lot of personal information on Facebook, why do you think that people forget about privacy at the time they use Facebook?

Perceived Benefits and Privacy Risks

- 1- What are the main benefits do you get when you use Facebook?
- 2- What are the potential risks to the privacy of your information on Facebook?

Information Sensitivity

- 1- Have you ever thought about sharing something on Facebook but you backed down because you felt that information is too private to be shared on Facebook?
 - 1a- What kind of information was it (e.g., status update, photo, video, comment, or like)?
 - 1b- How often did this happen to you?
- 2- Have you deleted some personal information from your Facebook profile because you thought it might harm you in the future?
 - 2a- What kind of information was it (e.g., status update, photo, video, comment, or like)?
 - 2b- Why did you share that information on Facebook at that time?

Privacy Settings Use

- 1- Do you use Facebook privacy settings to limit the privacy of your profile?
- 2- How public/private is your profile?

APPENDIX B (EXAMPLES OF EVIDENCE)

| Table B1. Additional Examples of Evidence | |
|--|--|
| Phenomenon 1: Cognitive Absorption, Privacy Concerns, and Self-disclosure | |
| <u>Cognitive Absorption</u> | <i>"It's to waste time. Does it make time fly? I don't know... I am more like "let's see what people posted, 'like', 'like', 'like'." [Macey, highly concerned]</i> |
| Temporal dissociation | <i>"Sometimes I look at the time and I am like "wow" I try to get off." [Ethan, highly concerned] "Definitely I lose track of time because there is always something there." [Bob, somewhat concerned] "Sometimes an hour will go by and I will be like okay I need to get off." [Yara, unconcerned at all] "If you have friends who are interested in the same thing, it really gives you something to talk about, because most likely you have had read the same article, because someone posted it and you read it and share it and so on so forth." [Macey, highly concerned]</i> |
| Immersion engagement | <i>"So, I think yes [I get engaged] because it is kind of the way these platforms work. They're based off emersion. So like because I am immersed into a specific technology like I am more interactive there because if there is watching video and then slowly you figure out you got to share it. Just by simply using it you immerse yourself in it." [David, somewhat concerned] "I don't feel like I'm terrible involved in it. I'll read through people's and if I see something that is particularly cool or interesting, I'll certainly 'like' it for certain friend's post, but it's rare that I would comment on something." [Gary, unconcerned at all]</i> |
| Enjoyment | <i>"I think it's pretty enjoyable. Just to see like what everyone is doing and sometimes I read stuff that I don't read like anywhere else. It is enjoyable... because it is not just one person, you can read anything and share all that stuff. I like that." [Macey, highly concerned] "If my feeds are showing advertisements, this is not enjoyment but if a friend is expressing feelings or her opinion about something, or what she likes. Those kinds of things I enjoy." [Phillip, somewhat concerned] "I would say like a 10 on a scale from 1 to 10. But depends on a lot of feedback. I like feedback so more feedback the better and comment on it and stuff. And Yeah [I feel rewarded for that]." [Eric, unconcerned]</i> |
| Control | <i>"I feel like Facebook is always gonna be there, my wife is not, if I can get off, I will get off so that I can control myself... But still, sometimes I get on and my wife checks me like "hey what are you doing, have you done your homework, have you paid the bills?" In a sense, she helps me get back on track." [Ethan, highly concerned]</i> |
| Curiosity | <i>"I am always aware of what I put out... I do make sure what I post on Facebook is positive but is also a reflection of who I am." [Eric, unconcerned] "It's basically why I go on there and yeah [I keep scrolling down to look and read more of my friends' updates, photos and videos]." [Macey, highly concerned] "Usually I get curious... The sense of curiosity is sparked and engaged... I certainly reach out to kinda see what's going on and I wonder what they're doing. Facebook provides that answer." [David, somewhat concerned] "I definitely scroll up and down to see what's happening and if the person is someone who I am really close to and if they have posted something, I go ahead and look at all of them and like or comment or whatever. But if it is someone who I just probably know but I am not that curious about knowing what's going on their lives, I will just probably scroll through it, give it a second." [Rachael, somewhat concerned]</i> |
| Phenomenon 2: Cognitive Absorption and Perceived Benefits and Privacy Risks | |
| | <i>"I thought I was cool [magnified perceived benefits]." [Macey, highly concerned] "I didn't think about it [deactivated privacy concerns] and the kind of consequences it could lead to [undermined perceived risks]." [Ella, somewhat concerned] "Impulsiveness, you kinda do it before you think [deactivated privacy concerns]. It's not just that your friends could see it. Everybody could see it [undermined perceived risks]... I guess if you got to think about it you probably should not post it." [Eric, unconcerned] "The more stuff you have the more friends you have, the cooler you were [magnified perceived benefits]." [Yara, unconcerned at all]</i> |
| Phenomenon 3.1: Cognitive Absorption and Information Sensitivity | |

"It happened like three or four times when me and my friends were partying or stuff like that but I feel like it isn't the appropriate platform for the simple fact that anybody can see it and we have a few family members that are friends with us. So, you know, we rather not be perceived by somebody and keep it ourselves." [Ethan, highly concerned]

"For me, it is entirely political stuff... Facebook is supposed to be a relaxing place. Social media is supposed to be for enjoyment. But when you put your own thoughts that are controversial, it becomes a chore to defend yourself in front of other people." [Mark, somewhat concerned]

"It is just some pictures that would probably compromise me some way. I probably liked it, but then I thought 'oh it probably doesn't speak well about me or probably tells something too much about me.'" [Ella, somewhat concerned]

"It was a contradicting thing about what someone said and it was something that they said pissed me off, and I was going to share something about that. Then, I thought no, it's not worth it. I just didn't do it." [Bob, somewhat concerned]

"I might watch a video, I may or may not 'like' it but if it is too controversial, I won't 'like' it. Because people might see that kind of stuff and say I am radical about something." [Eric, unconcerned]

"Mostly that's with all the political tension going on. I kinda refrain from posting any comments or posts because there can be many backlash against that and there's just no winning... I am kinda looking for a job right now. So, I don't want anyone to think 'oh man, she said this, this wouldn't align with our company culture'" [Yara, unconcerned at all]

Phenomenon 3.2: Temporal Effect

"When I was younger, I didn't care about privacy not I was aware of how much I was giving out. I'd post a lot of things that I probably shouldn't have, pictures included, statuses whatever, Oh God I was posting. And then, I had complaints either from my parents or my family members or even people from my school. They would be like saying negative things about it. Then, one day you just realize that wow, why? Like, I really shouldn't be doing that. That is so immature and now I am at this point where I am like OK, I definitely don't need to post this. I just don't do that anymore... [Reasoning for imprudent self-disclosure:] I think social media intensifies it, made it easier for us to be even dumber. So, maybe if I was with my friends and I was saying stupid stuff but now it is recorded, and now I look at it and I am like I can't believe I was saying these things, who do I think I was? Like, why I was using these words, why am I typing like this? It's just everything about it is like I cannot believe it. I can't believe that I used to act that way." [Macey, highly concerned]

"Now I am more aware, I've seen in the news that your online information could be sold, so I try to be as conservative as possible... [Reasoning for imprudent self-disclosure:] I was either drunk or just excited about the moment, oh let's just put this picture and then I did it. A few years later, I am like "what's this? What have I done? As far as disclosure, I don't really share personal stuff, so I am not so worried about that but I am concerned about my past comments and past stuff." [Ethan, highly concerned]

"When I went to one of my friends profile I saw they had movies and books... So, I went to my profile... and try to fill out those things. My Facebook profile was very comprehensive when I first created it. And then as time went on... Some of it is like really personal stuff. Like home address or work history all of that I do not really feel is appropriate to be on there... I was more active at that time... [Reasoning for imprudent self-disclosure:] A mixture of seeing what friends were doing, when I see friends posting and I see a bunch of 'likes', that's pretty cool because a lot of people saw it. A lot of people gave it thumbs up. So, I tried it myself, and then I got a status and then I got a lot of 'likes' and I got alerts for those 'likes' and I am like wow this is cool... maybe that was part of encouraging thing about Facebook at that time." [Mark, somewhat concerned]

"Actually I was a little bit more active in 2009, "oh" there is here a picture of me drinking, I didn't know that... Yeah. I don't want to have them. Knowing that people can see it and analyze it... it is just something that I wouldn't want other people to see, like my comments and stuff and trying to figure out my psychology... [Reasoning for imprudent self-disclosure:] First of all, I was much younger at that time, and probably didn't even think about it and the kind of consequences it could lead to... So I wasn't even thinking about anything related to privacy back then, even though I was aware of privacy, I always was... I don't think that I ever thought that someone is collecting my information when I click the 'like' button. I actually never thought that when I click like I am actually sharing personal information." [Ella, somewhat concerned]

"Back then it was very instant [Reasoning for imprudent self-disclosure], if I am in a bar, I would post photos and status updates and feeds... So, now, I wouldn't want to share those things anymore on Facebook but then I think I didn't care so much." [Rachael, somewhat concerned]

"I was more engaged on Facebook. Also, all people were more engaged on Facebook as there was no Instagram or Snapchat." [Phillip, somewhat concerned]

"Actually the way I use Facebook changed over time as well. I don't know how many years, it changed dramatically. Right now, the things I share are mostly socially concerned stuff that I have and yeah, and also, I know that companies also watch these stuff." [Bob, somewhat concerned]

"A lot of 'likes' could've been posts. So, I think it can be used in the wrong sense because some of the time it just like 'oh this is my friend'. [Reasoning for imprudent self-disclosure:] when you first started using Facebook, you have a lot of friends. So,

you 'like' all your friends' stuff." [Anna, unconcerned]

"I was more active in 2010 probably because the big social media hub at that time and everyone I knew was using it and I thought of going with everyone else [Reasoning for imprudent self-disclosure]... but if I read a popup any time in my life, I am sure a lot of people would laugh at it and I will be embarrassed." [Yara, unconcerned at all]

CHAPTER 3

Research Essay 2

Too Tired and in Too Good of a Mood to Worry about Privacy: Explaining the Privacy Paradox through the Lens of Effort Level in Cognitive Processing

Abstract

The confluence of Internet-based transactions, growing cybersecurity threats, and technologies such as facial recognition have made information privacy a topic of increasing importance both to consumers and companies that rely on consumers willingly sharing their personal information. Although information privacy has been of interest to researchers for decades and much has been learned, one thing that has perplexed scholars is the privacy paradox which refers to the fact that individuals who profess to be concerned about their privacy sometimes behave in ways that would suggest otherwise. In this paper, we shed light on the privacy paradox by pointing out that an underlying assumption of most studies is that consumers confront privacy decisions by employing high-effort cognitive processes, but that in reality privacy decisions may often be made by individuals who are too tired to use, or insufficiently motivated to employ, high-effort cognitive processes and instead are operating in a low-effort mode of cognitive processing. To examine this possibility and its implications, we conducted two experiments in which we relied on two different means (i.e., cognitive depletion and positive mood) by which low-effort processing can be triggered before presenting participants with an opportunity to disclose private information. We found that privacy concerns were significantly less predictive of actual disclosure behaviors for participants who were employing low-effort cognitive processes, due to a reduced cognitive resource and/or a positive mood state. Our results provide an explanation for the privacy paradox and highlight the importance of studying low-effort cognitive processing in privacy decisions.

Keywords: privacy paradox, privacy concerns, disclosure behavior, elaboration likelihood model, cognitive depletion, mood, enhanced APCO.

INTRODUCTION

It is black Friday. You are in a happy mood with the holidays coming and have had a great time shopping for your loved ones, but you are also mentally drained because there were so many good deals that you had to make some difficult decisions about which items you should purchase. While checking out at the last store, the cashier asks you to provide your phone, email, and mailing address. Assuming you have concerns for privacy, will you provide such personal information? A rational answer to this question is likely to be a definite “No” given your privacy concerns and perhaps your subjective calculus of the risks and benefits of disclosing such personal information. The rational answer, however, implicitly assumes that you have sufficient cognitive capacity and motivation to retrieve and act on your privacy preferences before making the disclosure decision. Yet, the scenario above involved a positive mood state and cognitive resource depletion, both of which may significantly affect cognitive processing and decision-making. We propose that the conditions described in the scenario are common to other contexts and can have significant implications for privacy decisions.¹³

Our objective is to test the assumption of high-effort cognitive processing in privacy decisions, which may be compromised by two commonly occurring conditions (i.e., cognitive resource depletion and positive mood). By investigating these conditions, we provide an explanation for the privacy paradox in which individuals who profess to be concerned about their privacy sometimes behave in ways that would suggest otherwise. Research provides evidence for the privacy paradox as an empirical phenomenon (for review, see Acquisti et al. 2016; Barth and de Jong 2017; Kokolakis 2017). For example, people sign up for loyalty cards, in which they reveal sensitive personal information, even if they have high privacy concerns (Acquisti and Grossklags 2005; also see Acquisti and Gross 2006). Such findings suggest that privacy concerns are a weak predictor of privacy decisions and provide support for the notion that individuals overlook their privacy concerns when making privacy decisions. We argue that the existence of the privacy paradox does not necessarily indicate that individuals do not act on their

¹³ For example, imagine someone who is feeling tired after a long day of work, but he is also in a happy mood because it is Friday and the work week is over. He decides to check social media right after work where he might start sharing different kinds of personal information in the form of “Likes”, comments, and posts while paying little attention to his dispositional privacy concerns, if any.

privacy concerns. Rather, its existence provides evidence for some unobserved boundary conditions under which the relation between privacy concerns and privacy decisions may break down. In other words, individuals overlook their privacy concerns under certain conditions only.

In this regard, the current literature lacks a systematic approach that can be applied to explore the conditions under which privacy paradoxical decisions may occur, impeding the field's ability to explain the phenomenon. A number of other factors have contributed to the lack of progress in this area. First, researchers have examined privacy decisions from two different perspectives: the normative perspective and the behavioral perspective. The normative perspective assumes individuals are rational decision makers who act on their privacy beliefs and perceptions to optimize their privacy decisions (Culnan and Armstrong 1999; Dinev and Hart 2006; Smith et al. 2011). Research based on this perspective advances theory that is consistent with classical economic models (e.g., privacy calculus) and tends to employ self-reported measures of privacy beliefs and disclosure outcomes. In contrast, the behavioral perspective which has emerged more recently suggests that numerous cognitive biases and heuristics can significantly shape privacy decisions, and hence, it is unrealistic to assume individual rationality (Acquisti 2004; Acquisti et al. 2016, 2017). Research based on this perspective advances theory that is consistent with behavioral economics principles and tends to employ measures of actual privacy decisions in experimental settings. Notably, the normative perspective is more attentive to privacy beliefs (e.g., privacy concerns) and their effect on self-reported outcomes (e.g., intention to disclose) (Dinev and Hart 2006; Son and Kim 2008). In comparison, the behavioral perspective is more focused on contextual cues (e.g., framing and default choices) and their effect on actual decisions (e.g., disclosure behaviors) (Acquisti et al. 2012; Adjerid et al. 2016, 2018b; John et al. 2010; Tsai et al. 2011).¹⁴ Overall, accounting for privacy beliefs is a unique characteristic defining the normative literature, whereas highlighting the role of conditional factors and measuring actual privacy decisions are merits of the behavioral literature. Substantial contributions have been made by each perspective. However, we believe that an approach that

¹⁴ Some studies in the normative literature also examined contextual factors, but their outcome measures were based on intentions or willingness (e.g., Anderson and Agarwal 2011; Angst and Agarwal 2009; Lowry et al. 2012).

utilizes the positive features of each perspective has yet to emerge to advance theory on privacy decisions, especially with regard to explaining the privacy paradox. Accordingly, we account for privacy beliefs (i.e., privacy concerns) and actual privacy decisions (i.e., disclosure behaviors) and we investigate how conditional factors affect the relationship between privacy concerns and disclosure behaviors in order to explain the privacy paradox.

Second, prior literature on disclosure behaviors has tended to focus either on cognition or affect. For example, in one study Alter and Oppenheimer (2009) showed that cognitive disfluency (a form of low-effort cognitive processing) can affect disclosure of personal information. In another study, Forgas (2011) showed that positive moods (a form of affect) can affect disclosure of personal information. While these studies have certainly contributed to our understanding, it has been suggested that both cognition and affect can influence privacy decisions. As Farahmand (2017) states, “privacy decisions [e.g., disclosure behaviors]... are the outcomes of the collaboration and competition between affective and cognitive assessments in the human mind.” (p. 69, [bracket added]). Thus, exploring cognition without considering affect, or vice versa, renders an incomplete picture as cognition and affect are inseparable components of the decision making process (Dolan 2002; Homburg et al. 2006; Sun and Zhang 2006). Accordingly, we consider both components in the current study to advance this literature.

Third, it is unclear how the effort level in cognitive processing, which can be influenced by cognitive factors (e.g., demanding tasks) and/or affective factors (e.g., mood changes), influences disclosure behaviors particularly in the presence of privacy concerns. For instance, some evidence suggests that exerting cognitive effort leads to lower disclosure (Alter and Oppenheimer 2009). However, other findings suggest no association between cognitive effort and disclosure (Balebako et al. 2013). With these mixed findings in mind, it is also important to note that disclosure behaviors are significantly influenced by individuals’ dispositional privacy concerns (Smith et al. 2011). Accordingly, studies that attempted to explain and predict disclosure behaviors through cognition or affect (Alter and Oppenheimer 2009; Balebako et al. 2013; Forgas 2011) have a distinct limitation because they did not account for privacy concerns. In addition, although privacy concerns should be accounted for, we know that privacy

paradoxical decisions occur indicating that privacy concerns might not necessarily be a significant predictor of disclosure behaviors. Psychological theories (Petty and Cacioppo 1986; Petty and Briñol 2010) suggest that under certain conditions, where cognitive processing is diminished due to cognitive and/or affective factors, individuals are less likely to make informed decisions that are consistent with their beliefs. Thus, to explain and predict disclosure behaviors, it is important to consider the level of effort associated with individuals' cognitive processing while accounting for their dispositional privacy concerns. In this study, we use the lens of effort level in cognitive processing and we present evidence that explains the privacy paradox in a systematic way. In doing so, we demonstrate that the privacy paradox manifests under certain conditions in which the effort level in cognitive processing is low but disappears under other conditions in which the effort level in cognitive processing is high. Such systematic investigation is timely considering the emerging literature on the privacy paradox.

We adopt the elaboration likelihood model (ELM) (Petty and Cacioppo 1986) as the foundation for our research. According to the ELM, there are two processing routes: one requiring high-effort (the central route) and the other reflecting low-effort processing (the peripheral route). Many factors can influence whether an individual engages in higher effort central route processing or follows heuristic processing along the peripheral route (Petty and Briñol 2010). In this study, we focus on cognitive resources and mood states, both of which can affect the processing effort in privacy decisions. Our rationale for examining the effects of both cognitive resources and mood states is that: (1) they often operate together across a wide variety of different contexts (Middlewood et al. 2016) and 2) there is limited research examining the interactive effect of cognition and affect in privacy contexts (Farahmand 2017).

Dual-process models like the ELM provide an appropriate theoretical lens to test the assumption of high-effort processing in privacy decisions (Lowry et al. 2012). When people expend considerable cognitive effort in decision making, they apply knowledge and act in ways consistent with their pre-existing beliefs (McConnell and Rydell 2014; Petty and Briñol 2010). Thus, if people believe that privacy is important and that it should be guarded closely, they are especially likely to behave in ways to protect

private information when they have sufficient cognitive resources and opportunity to direct behavior in accordance with their beliefs. However, if people's ability to engage in effortful information processing is reduced, privacy behaviors will be guided more by factors unrelated to people's privacy beliefs (Dinev et al. 2015).

Essentially, we examined conditions under which people's ability to engage in effortful cognitive processing is compromised, anticipating that these circumstances will weaken the relationship between privacy concerns and disclosure behaviors, hence providing empirical evidence for the privacy paradox. When people's cognitive processing is not compromised, we anticipated that privacy concerns would predict disclosure behaviors in accordance with the findings from many published studies that stronger privacy concerns reduce people's disclosure behaviors. Thus, our primary research question is: *Do conditions that reduce effortful cognitive processing attenuate the relationship between privacy concerns and disclosure behaviors?* To address this question, we explored two ways in which one's ability to engage in elaborative information processing can be compromised: (1) cognitive depletion and (2) positive mood. Based on two experiments, we show that reductions in cognitive effort triggered by depleting tasks and/or positive moods render the association between privacy concerns and disclosure behaviors insignificant.

This study makes five important contributions. First, unlike most other studies in the privacy research stream, it investigates decision-making under conditions of low-effort cognitive processing, and hence, provides insights for privacy theory when privacy concerns are less related to disclosure behaviors. In doing so, we present systematic evidence for explaining and predicting occurrences of the privacy paradox. Such investigation holds important implications for users, organizations, and policy makers, which we discuss further in the implication section. Second, the study distinguishes between conditions that are both external (i.e., depleting cognitive tasks) and internal (i.e., mood states) to the individual. Thus, we address a recurring limitation in prior research by considering the effects of both cognitive and affective conditions on privacy decisions (Farahmand 2017). While a recent theoretical framework highlighted the role of cognitive depletion and mood in privacy decisions (Dinev et al. 2015), the

framework overlooks the interaction between cognition and affect. Moreover, there is no empirical evidence to sort out whether theoretical relationships suggested by Dinev et al. (2015) hold up under scrutiny (Sutton and Staw 1995, p. 383). Thus, in addition to testing a number of propositions suggested by Dinev et al.'s (2015) enhanced Antecedents – Privacy Concerns – Outcomes (APCO) model, we theorize and test the joint effect of cognitive depletion and mood on the relation between privacy concerns and disclosure. Third, in addition to capturing individuals' privacy concerns, our experiments measure actual disclosure decisions rather than self-reported behaviors or stated intentions, which are the usual measures of disclosure in the normative literature. Fourth, our study contributes to the psychology literature by demonstrating how cognitive demands and mood states influence the relationship between attitude and behavior. Finally, in our second experiment we present a newly developed approach for manipulating cognitive depletion and mood state simultaneously, which represents a methodological contribution.

BACKGROUND AND HYPOTHESES

In this section, we provide background information to derive four hypotheses. We begin by reviewing relevant research and the privacy paradox. The first hypothesis is best viewed as a replication of findings from numerous previous studies that, *ceteris paribus*, greater privacy concerns reduce disclosure behaviors. The rationale for replicating this hypothesis is to set up a systematic approach for testing and explaining the privacy paradox. Next, we offer a brief theoretical discussion of why low-effort cognitive processing should weaken the relation between privacy concerns and disclosure behaviors followed by a derivation of our new hypotheses.

Privacy Concerns and Information Disclosure

Privacy concerns refer to a dispositional belief that reflects the loss of control over personal information (Bélanger and Crossler 2011; Culnan and Bies 2003; Solove 2006; Westin 2003), and could significantly influence privacy decisions (Smith et al. 1996; Smith et al. 2011). Several studies have shown that individuals who have high privacy concerns are less willing to purchase products online, to use social

media, to adopt electronic health records, or to share personal information on the Internet (Angst and Agarwal 2009; Dinev and Hart 2006; Hui et al. 2007; Jiang et al. 2013; Xu et al. 2010).

Information disclosure refers to the breadth and depth of revelations individuals make in a voluntary way (Krasnova et al. 2010; Posey et al. 2010). From a theoretical perspective, the relationship between privacy concerns and disclosure behaviors has been largely based on the attitude-intention link suggested by the theory of planned behavior (Ajzen 1991).¹⁵ As a result, the majority of studies in the normative literature relied on a dependent variable that does not necessarily reflect actual behaviors (e.g., intention to disclose) (Smith et al. 2011; Yun et al. 2014). Nevertheless, current findings from different disciplines strongly support a negative association between privacy concerns and disclosure-related outcomes (for review, see Li 2011; Smith et al. 2011; Yun et al. 2014). In particular, individuals who have high privacy concerns are less willing to disclose personal information. Although there are a few empirical studies in this (normative) literature that measured actual disclosure (Hui et al. 2007; Keith et al. 2015; Sutanto et al. 2013), we replicate this hypothesis in order to present evidence for and explain the privacy paradox in a systematic way.

Hypothesis 1 (H1): *Individuals with high levels of privacy concern will be less likely to disclose personal information.*

The Privacy Paradox

To the extent that exceptions to H1 can be documented, they would provide support for the privacy paradox, which is generally viewed as a mismatch between an individual's stated privacy concerns and privacy decisions or behaviors, such as disclosure.¹⁶ Spiekermann et al.'s (2001) study is one of the earliest in which a mismatch between stated privacy concerns and disclosure was observed. In their study, participants interacted with an experimental agent (an anthropomorphic bot in an online shopping store) during which their privacy concerns did not determine their disclosure of purchasing preferences to the agent. Acquisti and Grossklags's (2005) study also presented evidence supporting the privacy paradox.

¹⁵ For a review of other theories adopted in this literature, see Li (2012).

¹⁶ This appears to be the generally accepted definition of the privacy paradox (Smith et al. 2011). Although there are occasional interpretations of the paradox as a mismatch between stated intentions and actual behaviors (e.g., Keith et al. 2015; Norberg et al. 2007; Pavlou 2011), our purpose is to address the paradox between privacy concerns and disclosure behaviors because 1) it is the more generally used definition by privacy scholars and 2) the paradox between intentions and behaviors is a broad phenomenon that is not limited to the context of privacy.

Their study reported that a large majority of privacy fundamentalists signed up for a loyalty card in which they revealed sensitive identifying information. Both studies, however, also showed a significant association between privacy concerns and privacy decisions. For example, privacy concerns were significantly associated with disclosure of personal information outside the online shopping environment (Spiekermann et al. 2001) and with privacy-protective behaviors (Acquisti and Grossklags 2005).

A number of theoretical and empirical explanations have been proposed to explain the privacy paradox, by both the normative and behavioral literature (Acquisti 2004; Acquisti and Grossklags 2005; Dinev and Hart 2006). Two studies have recently reviewed the literature on the privacy paradox (Barth and de Jong 2017; Kokolakis 2017). However, a solid conclusion about the causes of the privacy paradox has not yet emerged for several reasons. First, the two distinct literatures have been examining privacy decisions from two different theoretical and methodological perspectives, making it difficult to arrive at a dominant inference. As put by Adjerid et al. (2018b), “comparisons between the results produced within the two literatures are *post hoc*, requiring meta-analysis across studies with diverse modeling assumptions and empirical methodologies” (p. 466). The second reason which further illustrates the divergence of these literatures pertains to the approach adopted to test and explain the privacy paradox. The privacy paradox refers to a mismatch between *privacy concerns* and *privacy decisions*. Accordingly, to present evidence for and/or to explain the privacy paradox, it is necessary to measure two focal constructs, namely privacy concerns and privacy decisions (condition 1). Once this condition is met, a test for the privacy paradox can be executed. If a weak, negligible, or null association between privacy concerns and privacy decisions is observed, then one can claim supporting evidence for a privacy paradox (condition 2). These are two necessary conditions that must be satisfied before making attempts to explain why privacy concerns are a weak predictor of privacy decisions (i.e., the privacy paradox). Unfortunately, most studies tend to assume that the privacy paradox exists and proceed to explain it without meeting these two necessary conditions. As a result, attempts to identify the causes of the privacy paradox have been, to a large extent, unsystematic.

For instance, the majority of studies in the normative literature measured privacy concerns, but they relied on dependent variables that do not necessarily reflect actual privacy decisions, mainly intention-like outcomes (e.g., Choi et al. 2018; Dinev and Hart 2006; Karwatzki et al. 2017; Kehr et al. 2015; Ku et al. 2013; Li et al. 2017; Mothersbaugh et al. 2012; Sun et al. 2017; Taddicken 2014; Wakefield 2013; Woodruff et al. 2014; Yu et al. 2015). Thus, condition 1 is only partially satisfied in this literature as intention outcomes were measured instead of actual privacy decisions. In contrast, the majority of studies in the behavioral literature measured actual privacy decisions, but they overlooked or were unable to capture privacy concerns, or their objectives were toward other privacy phenomena (Acquisti et al. 2012, 2013; Adjerid et al. 2016, 2018a; John et al. 2010; Tsai et al. 2011; Tucker 2014). Thus, condition 1 is also only partially satisfied in this literature as privacy concerns were not measured. We argue that the absence of either one of these two constructs, which define the meaning of the privacy paradox, led to imprecise extrapolations about the causes of the privacy paradox and hence indefinite conclusions (Barth and de Jong 2017; Kokolakis 2017).

Nonetheless, a few studies have met both conditions. Their findings suggest that privacy concerns are significantly associated with privacy decisions in some cases (Adjerid et al. 2018b; Hui et al. 2007; Keith et al. 2015; Spiekermann et al. 2001) but not others (Sutanto et al. 2013; Spiekermann et al. 2001).¹⁷

Having articulated the necessary conditions for presenting evidence for the privacy paradox, we propose that an empirical and systematic approach to explaining the privacy paradox should focus on the boundary conditions or moderators of the relationship between privacy concerns and privacy decisions. Specifically, we refer to conditional factors that will enable us to predict the circumstances under which privacy concerns are strongly or weakly associated with privacy decisions. Establishing boundary conditions has been discussed by theorists and empiricists as a vital tool for enhancing the generalizability

¹⁷ Although our literature review might suggest weak support for the existence of the privacy paradox, we caution against such an interpretation. First, studies that do not measure actual privacy decisions present tentative support for the existence of the privacy paradox. For instance, research shows that individuals weigh affect, enjoyment, or social capital much more than they weigh privacy concerns (Debatin et al. 2009; Kehr et al. 2015; Wakefield 2013; Sun et al. 2017; Yu et al. 2015). In the context of electronic health records, Anderson and Agarwal (2011) show that the effect of privacy concerns on willingness to share personal information is conditional on the type of information, intended purpose, or requesting stakeholder. Similarly, behavioral research indicates that a number of biases and heuristics can significantly affect privacy decisions (Acquisti et al. 2016, 2017). Together, such findings provide plausible evidence for the privacy paradox. However, they remain imprecise and unsystematic given their individual limitations.

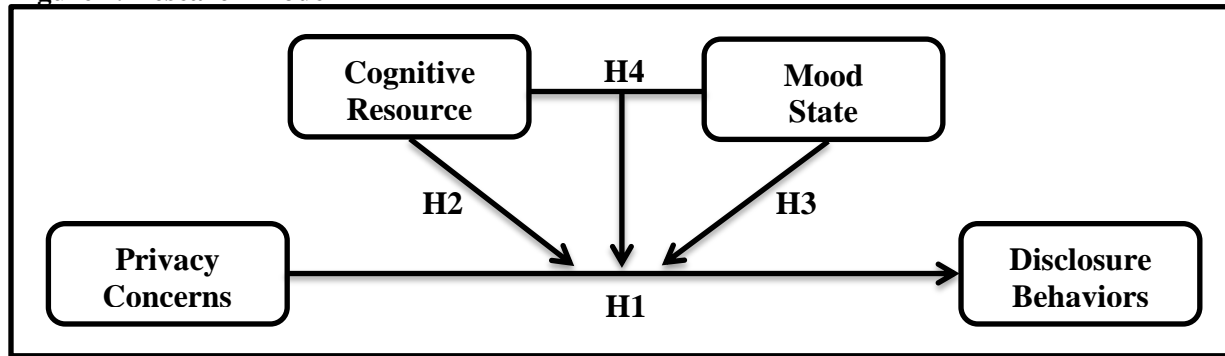
of a theory and resolving paradoxical phenomenon (Busse et al. 2017; Edwards and Berry 2010; Whetten 1989). We believe that such a systematic approach will advance privacy theory in general and enrich our understanding of the privacy paradox. Next, we build on the ELM and discuss the level of effort in cognitive processing as a generic boundary condition that can explain the privacy paradox.

Elaboration Likelihood Model (ELM)

Our research design is grounded on the ELM (Petty and Cacioppo 1981, 1986; Petty and Wegener 1998). The ELM has been embraced as a prominent psychological theory that explains differences in two important routes to decision-making through attitude: the central and peripheral routes. As explained by Petty and Cacioppo (1981), the central route is more likely to include a thoughtful consideration of the merits of the information, whereas the peripheral route is likely to be based on a simple cue and not on scrutiny of the true merit of the information presented. Following Dinev et al. (2015), we refer to the former as “high-effort” cognitive processing and the latter as “low-effort” cognitive processing.

In order to employ high-effort cognitive processes, the ELM holds that an individual must be both motivated to process and have the ability to process relevant information (Petty and Cacioppo 1981; Petty and Wegener 1998). For example, if people are cognitively depleted or performing tasks when mentally fatigued, they are less likely to engage in high-effort information processing (Bodenhausen 1990; Petty and Cacioppo 1981). Thus, to the extent that people experience conditions that are cognitively depleting, they are less motivated to behave in ways that reflect their existing bases of knowledge. One’s ability to process is determined by many factors such as the extent to which one can devote effortful attention to decision-related information when pursuing an action. To the extent that one is low on either motivation or ability to process relevant information, one will not engage in elaborative information processing before acting (e.g., reflecting on beliefs to inform behaviors), and thus one’s actions will be more strongly directed by peripheral cues. In this study, we theorize that triggering low-effort processing, whether as a result of depleted cognitive resources or from being in a positive mood state, will lead individuals’ predisposed privacy concerns to be less predictive of their disclosure behaviors. Figure 1 depicts our research model.

Figure 1. Research Model



Cognitive Resource and Mood State

Cognitively demanding tasks can deplete people’s working memory capacity, which can reduce their ability to engage in high-effort information processing on subsequent tasks (Baddeley and Hitch 1974; Engle 2002; Miyake and Shah 1999). Just as running a marathon can exhaust an athlete and lead to less effort being expended on a subsequent run, so too can a cognitively taxing activity reduce effortful information processing in a later judgment and decision making task (Beilock et al. 2007; Muraven and Baumeister 2000). Using techniques (to be described) to manipulate participants into either a low or high depletion state, we theorized that participants in a high depletion condition should, when later asked to disclose personal information, be less able to act on their privacy concern beliefs. As a result, the usual linkage between privacy concerns and disclosure behaviors (H1) will be weakened for highly depleted individuals because they do not have enough cognitive capacity to enact privacy-related behaviors that are consistent with their long-term goals (e.g., protection of personal information). In other words, the predictive power of privacy concerns will be weak (strong) when individuals engage in a low-effort (high-effort) cognitive processing resulting from a depleted (non-depleted) cognitive state.

Hypothesis 2 (H2): *Cognitive resource depletion will moderate the negative relationship between privacy concerns and disclosure behaviors, such that the level of privacy concern will be less (more) predictive of disclosure behaviors for cognitively depleted (non-depleted) individuals.*

We also relied on a second path by which effortful information processing can be disrupted: mood state. Mood is an affective state that resides within the person (hence, an internal condition) and reflects a diffuse positive or negative feeling without a clear cause to the individual (Forgas 1995; Morris

1989; Schwarz and Clore 1988, 2007; Zhang 2013).¹⁸ It has been widely shown that mood states influence decision making and behavior (Clark and Isen 1982; Forgas 1995, 2017; Isen et al. 1978; Schwarz 1990; Schwarz and Clore 1988, 2007), including those involving attitude-to-behavior processes (Bless et al. 1990; Petty et al. 1993; Petty and Wegener 1998). In particular, when people are in a positive mood, they show less effortful information processing and greater reliance on heuristics in their behavior (Bless et al. 1990; Bodenhausen et al. 1994; Park and Banaji 2000). In short, experiencing a positive mood signals that “everything is okay,” and thus individuals are less interested in thoughtful analysis of their circumstances and as a result they do not typically engage in effortful evaluation (Schwarz and Clore 1988, 2007; Wegener and Petty 1994).

There is some support in the literature consistent with the notion that an individual’s affective state impacts their perception of privacy beliefs and potential risks (Kehr et al. 2015; Wakefield 2013; Yu et al. 2015). For instance, enjoyment with a website was found to positively predict privacy protection perceptions and to negatively predict privacy risk perceptions (Li et al. 2011). Another study found that positively induced affect led to underestimations of potential privacy threats (Kehr et al. 2015). These studies, however, did not measure privacy decisions, examine the moderating effect of affect, or consider the level of cognitive processing.

More broadly, our reasoning is consistent with research in psychology suggesting that “moods serve as information” that can influence how people think in cognitive tasks (Clark and Isen 1982; Frijda 1988, 2007, 2010; Sanna et al. 1999). According to this literature, it would be expected that individuals are more likely to disclose personal information when they are in a more positive mood state as they are relying on a more low-effort thinking (Forgas 2011). Accordingly, we anticipated that people experiencing relatively positive mood states would be less likely to rely on their privacy beliefs when presented with a request to disclose private information.

¹⁸ Affect or core affect is an umbrella term for both moods and emotions (Forgas 1995; Zhang 2013). Moods are “low-intensity, diffuse and relatively enduring affective states without a salient antecedent cause and therefore little cognitive content (e.g. feeling good or feeling bad),” whereas *emotions* “are more intense, short-lived and usually have a definite cause and clear cognitive content” (Forgas 1995, p. 41). In this study we focus on moods because they are more common and normally subconscious, and individuals are generally unaware of their effects, whereas emotions are context-specific, conscious feelings, and individuals are often aware of them when making decisions (Forgas 1995, 2013).

Hypothesis 3 (H3): *Mood state will moderate the negative relationship between privacy concerns and disclosure behaviors, such that the level of privacy concern will be less (more) predictive of disclosure behaviors for individuals in a positive (negative) mood state.*

As Figure 1 depicts, the negative relationship between privacy concerns and disclosure behaviors (H1) should be weakened when people employ low-effort processes either because of cognitive depletion (H2) or positive mood states (H3). Thus, as the level of cognitive effort is diminished either by cognitive resource depletion or positive mood states, there is less motivation to apply one's privacy beliefs to a behavioral context where private information might be disclosed. It is also possible that an interaction may exist between cognitive depletion and positive mood states that would result in even lower effort processing. That is, the simultaneous presence of a positive mood state in an individual who is already depleted of cognitive resources might result in a state of especially inadequate cognitive capacity being available, producing the greatest disruption to the relationship between privacy concerns and disclosure behavior. Thus, we also anticipated a 3-way interaction between privacy concerns, cognitive resource, and mood state whereby the presence of cognitive depletion and positive mood would be especially powerful in robbing individuals of their ability to engage in high-effort processing, thus resulting in disclosure behaviors that are inconsistent with stated privacy concerns. However, a sufficient cognitive resource (i.e., non-depleted resource) coupled with a negative mood state, reflecting high-effort processing, will give rise to disclosure behaviors that are commensurate with individuals' privacy concerns. In summary, the presence of cognitive resource depletion and/or a positive mood state (i.e., reflecting low-effort cognitive processing) will result in a weak association between privacy concerns and disclosure behaviors. However, the presence of a sufficient cognitive resource coupled with a negative mood state (i.e., reflecting high-effort cognitive processing) will result in a strong association between privacy concerns and disclosure behaviors.

Hypothesis 4 (H4): *There will be a 3-way interaction between privacy concerns, cognitive resource, and mood state, such that the level of privacy concern will be less predictive of disclosure behaviors for individuals in a depleted condition and/or a positive mood state; however, the level of privacy concern will be more predictive of disclosure behaviors for individuals in a non-depleted condition coupled with a negative mood state.*

EXPERIMENT 1

Method

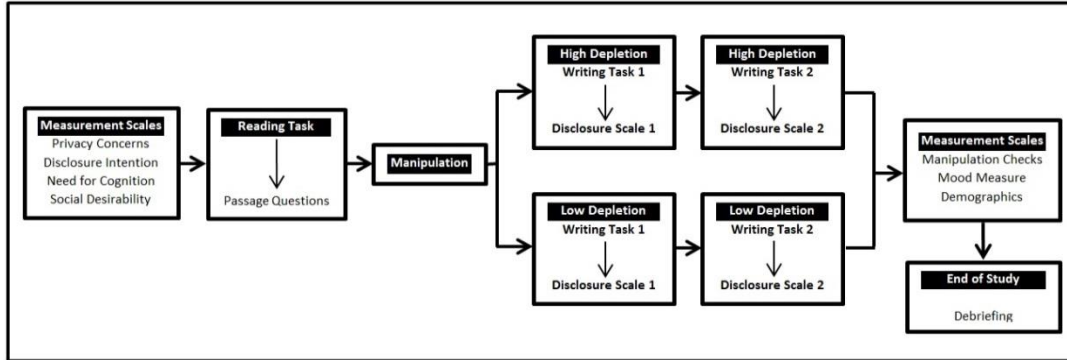
We used two consecutive depletion tasks in a randomized experimental design to induce high or low depletion. Each depletion task was followed by a set of requests for participants to disclose personal information. We used two depletion tasks to ensure that the depletion effect lasted long enough to affect the disclosure decision. We developed a new scale to measure actual disclosure behavior. Our approach is similar to that used by many other privacy scholars (e.g., Acquisti et al. 2012; Adjerid et al. 2018b; Marreiros et al. 2017; Norberg et al. 2007). Developing a new scale was necessary, however, because our context was different. We used established measures for privacy concerns and mood (Dinev and Hart 2006; Mayer and Gaschke 1988). Data were collected via Amazon Mechanical Turk (AMT) and participants could earn up to \$3.00 depending on their performance. The final sample included 150 participants after applying exclusion criteria (i.e., failing attention checks or failing to complete the experimental task) to ensure the quality of responses. The mean age of the participants was 38.2 years and 48.7% were female.

Procedure

We chose the context of a mobile health application (app) and created a cover story involving it to enable realistic disclosure behavior. Figure 2 depicts the sequence of tasks involved in experiment 1. First, participants were asked to respond to four scales: privacy concerns, disclosure intentions, need for cognition, and social desirability. Next, participants were given instructions through which they were led to believe that the tasks involved (i.e., reading, writing, and personal information requests) were central to the app development project which served as our cover story. This procedure was essential to enable measuring actual disclosure after manipulating the depletion state as described below. After reading the

cover story, participants were asked to read a short passage and then asked to provide correct answers to three questions following the passage. These questions were used as an attention check.¹⁹

Figure 2. Flowchart of Experiment 1’s Instrument



Next, participants were randomly assigned to either a low or high depletion condition and asked to perform a commonly used depletion task (Schmeichel 2007). In the first writing task, participants were asked to write a short essay about common health issues without using any word that contains the letters “A and N,” which is a fairly difficulty task [high depletion condition] or “X and Z,” which is a fairly easy task [low depletion condition]. After this writing task, all participants were presented with the first set of 12 disclosure items (e.g., “*In an average day, how often do you pass gas (flatulence)?*”) (see Appendix B.1 for the entire list of items). Participants were given an option to refuse to provide an answer to any item by choosing “*I prefer not to provide this information.*” Next, participants were given instructions for the second writing task. This time, participants were asked to write about one good habit and one bad habit. Those assigned to the high (low) depletion condition in the first writing task were given another difficult (easy) writing task, that involved not using the letters “E and N” (“Q and Z”). Next, all participants were presented with the second set of disclosure items (see Appendix B.1). Finally, participants were asked to answer manipulation check questions, report their mood state,²⁰ provide demographic information, and then debriefed.

¹⁹ The reading task was also used to conceal the main purpose of the study and to enable a realistic measure of actual disclosure behavior at a later stage of the experiment. It also served to reduce the possibility that the privacy concerns scale which was used early in the experiment could result in a privacy priming effect (Alashoor et al. 2017).

²⁰ In the depletion literature, mood is measured either after the depletion task (Gino et al. 2011) or after the performance task (disclosure decision in our case) (Barber and Smit 2014). We chose to measure mood at the end of the experiment to avoid attenuation of the depletion effect, and because mood changes can interact with the depletion state to affect subsequent task performance (Hagger et al. 2010).

Manipulation Check

Three items were used to check the depletion manipulation (e.g., “*how difficult were the writing tasks?*” (1 *Not at all difficult* ... 7 *Extremely difficult*)). Factor analysis and reliability statistics showed convergence of the three items (Cronbach’s $\alpha = .949$) and a mean score was computed. A *t*-test ($t = -21.89$; $df = 148$) indicated a significant mean difference between the high ($n = 72$; $mean = 5.89$; $s.d. = 0.89$) and low ($n = 78$; $mean = 2.45$; $s.d. = 1.01$) depletion conditions ($p < .001$), indicating that the depletion manipulation was successful.

Measurement Validation

Our main predictors were privacy concerns, cognitive resource depletion, and mood state. Depletion was dummy coded (high depletion = 1 and low depletion = 0). For constructs that were assessed using multiple items, exploratory factor analysis (EFA) was conducted to verify psychometric properties. The results show strong support for convergent and discriminant validity and all Cronbach’s α are well above the .70 threshold (see Appendix A.1, Table A.1).

Privacy concern was measured using four items (Dinev and Hart 2006) with a 5-point Likert scale (Cronbach’s $\alpha = .958$), and a mean score was computed. Mood was assessed using the Brief Mood Introspection Scale (BMIS) comprised of 16 items (1 *Definitely do not feel* ... 7 *Definitely feel*) (Mayer and Gaschke 1988). In the BMIS, eight adjectives (*lively, peppy, active, happy, loving, caring, calm, and content*) reflect positive mood whereas the other eight (*drowsy, tired, nervous, gloomy, fed up, sad, jittery, and grouchy*) reflect negative mood. The initial factor analysis, however, revealed three factors. The eight positive adjectives, except calm, loaded well on one factor. Six of the negative adjectives loaded well on a second factor while two adjectives (i.e., drowsy and tired) loaded on a third factor. This result was anticipated considering the nature of our study in which the loadings for drowsy and tired would be influenced by the reading and writing tasks. Therefore, we dropped these two items from our mood measure. We also dropped one positive item (i.e., calm) because it cross-loaded on two factors. Following Sanna et al. (1999), we created a mood index after reverse coding the six negative adjectives (Cronbach’s $\alpha = .924$) and averaging them with the ratings of the seven positive adjectives (Cronbach’s $\alpha = .945$).

We also measured three other variables (i.e., need for cognition, disclosure intention, and social desirability) to control for their effect. For instance, individuals with high need for cognition normally exert high effort in cognitive tasks (such as our reading and writing tasks) and hence they would be more likely to consume their cognitive capacity by the time they are presented with requests for personal information. As a result, they may be more likely to share personal information because of reduced cognitive resources. Need for cognition was measured using seventeen items (Cronbach's $\alpha = .956$). A mean score was computed after recoding the reversed items. Individuals with high disclosure intention are more likely to share personal information; therefore, we control for this variable which was measured based on three items (Cronbach's $\alpha = .960$). A mean score was computed after reverse coding the first item. The social desirability scale assesses individuals' tendency to appear socially desirable. It is expected that those with high social desirability would be less willing to share personal information that reflects undesirable traits, beliefs, or behaviors. Social desirability was measured using seventeen items. A score for social desirability was computed following the procedure suggested by Stöber (2001).²¹

Dependent Variable

Consistent with prior privacy research (e.g., Acquisti et al. 2012), we computed the total sum of the number of items for which each participant provided information. We used a log transformation considering that our measure of disclosure behavior is a count variable exhibiting a non-normal distribution.²² Table 3 shows the correlation matrix along with descriptive statistics.

Table 3. Experiment 1 – Correlation Matrix

| | <i>min</i> | <i>max</i> | <i>mean</i> | <i>s.d.</i> | 1 | 2 | 3 | 4 | 5 | 6 |
|---------------------------|------------|------------|-------------|-------------|-------|-------|------|-------|-------|---|
| 1- log(Disclosure)* | 2.30 | 3.14 | 3.089 | 0.130 | 1 | | | | | |
| 2- Privacy Concerns | 1.00 | 5.00 | 3.645 | 1.096 | -.061 | 1 | | | | |
| 3- Mood** | 1.46 | 7.00 | 5.157 | 1.160 | .309 | -.012 | 1 | | | |
| 4- Need for Cognition | 1.17 | 5.00 | 3.636 | 0.808 | .124 | .185 | .311 | 1 | | |
| 5- Disclosure Intention** | 1.00 | 7.00 | 4.044 | 1.688 | .126 | -.526 | .188 | -.155 | 1 | |
| 6- Social Desirability | 0.00 | 16.00 | 8.093 | 4.008 | -.036 | .080 | .303 | .185 | -.012 | 1 |

* Descriptive statistics for non-transformed disclosure: *min* = 10, *max* = 23, *mean* = 22.120, *s.d.* = 2.314. The variations in this measurement are very similar to those found in Acquisti et al. (2012, Study 1A), Hui et al. (2007), Marreiros et al. (2017), and Norberg et al. (2007).

** A high (low) score in mood reflects a positive (negative) mood. A high (low) score in disclosure intention reflects high (low) intention to disclose personal information.

²¹ Each 'true' response on items 2, 3, 4, 7, 8, 9, 11, 12, 13, and 15 and each 'false' response on items 1, 5, 6, 10, 14, and 16 are given 1 point and then points are summed across items (Stöber 2001).

²² The substantive conclusions of the results reported below remain consistent when using the original count variable.

Results

Table 4 presents the results of the final model after conducting a series of weighted least squares (WLS) and ordinary least squares (OLS) regression analyses (Appendix A.2 presents preliminary analysis, rationale for using WLS regression, and robustness checks).²³ The control variables were dropped from the final model because they did not improve the model and were not statistically significant. We use Model_{WLS} (Table 4) to test our hypotheses. However, because the model includes a 3-way interaction term, we use marginal effects (i.e., simple slopes) instead of the coefficient estimates from Model_{WLS} to test H1, H2, and H3. We use the coefficient estimate of the 3-way interaction term from the same model to test H4 (we illustrate the appropriateness of this approach in Appendix A.2). However, to directly test each possible prediction from H4, we probe the marginal effect to test the significance of privacy concerns under each condition.

Hypothesis 1 (H1) predicted a negative relation between privacy concerns and disclosure behaviors. Model_{WLS} shows a significant negative effect of privacy concerns ($\beta_{PrivacyConcerns} = -.088$; $s.e. = .018$; $p < .001$). This estimate, however, does not provide an appropriate test for the main effect of privacy concerns on disclosure behaviors (see Appendix A.2). This is because we are unable to hold everything else constant or at the mean level due to inclusion of interaction terms with a dichotomous variable (i.e., *DepletionXPrivacyConcerns*, *DepletionXMood*, and *DepletionXPrivacyConcernsXMood*) (Dawson 2014). Therefore, we test H1 by probing the privacy concerns' marginal effect (Williams 2012), which takes into account both depletion conditions while holding mood at the mean. In particular, the marginal effect takes the numerical derivative of the expected disclosure with respect to privacy concerns for each depletion condition while mood is at the mean level. The marginal effect approach (as compared to the hierarchical regression approach) accounts for the fact that all necessary terms are included in the model (i.e., assumed correct specification) and, hence, it provides unbiased estimates. The marginal effect (*ME*) result indicates

²³ We used WLS to correct for heteroskedasticity in the OLS model. After applying several robustness checks, the results from the WLS model remained consistent with those from the OLS model (for more details, see Appendix A.2).

a significant negative main effect of privacy concerns on disclosure behaviors ($\beta_{PrivacyConcerns_ME} = -.064$; $s.e. = .014$; $p < .001$). Thus, H1 is supported.

Table 4. Regression Results; Dependent Variable: log(Disclosure)

| | Model _{WLS} |
|--|----------------------|
| | β (s.e.) |
| Constant | 3.066*** (.020) |
| Depletion (high) | .009 (.032) |
| PrivacyConcerns | -.088*** (.018) |
| Mood† | .042** (.013) |
| DepletionXPrivacyConcerns | .075** (.026) |
| PrivacyConcernsXMood | .076*** (.011) |
| DepletionXMood | -.039* (.017) |
| DepletionXPrivacyConcernsXMood | -.060*** (.014) |
| F value | 23.41*** |
| R^2_{OLS} (Adjusted R^2_{OLS}) †† | 16.60% (12.48%) |

n.s. not significant; * $p < .05$; ** $p < .01$; *** $p < .001$

† A high (low) score in mood reflects a positive (negative) mood.

†† R^2 obtained from WLS is not meaningful in interpreting the explanatory power of the model, because it indicates how much variation in the weighted dependent variable is explained by the weighted independent variables, instead of indicating variation explained by the original variables (Wooldridge 2009). For ease of interpretation, we only report OLS R^2 as there is no agreed upon pseudo R^2 for WLS (Willett and Singer 1988).

Hypothesis 2 (H2) predicted that the negative effect of privacy concerns will be less (more) predictive for participants in the high (low) depletion condition. Similarly, hypothesis 3 (H3) predicted that the negative effect of privacy concerns will be less (more) predictive for participants in a positive (negative) mood state. Model_{WLS} indicates a significant positive effect of both interaction terms ($\beta_{DepletionXPrivacyConcerns} = .075$; $s.e. = .026$; $p < .01$; $\beta_{PrivacyConcernsXMood} = .076$; $s.e. = .011$; $p < .001$). However, we cannot rely solely on these estimates to test H2 and H3 and therefore we estimate the marginal effects. With regard to H2, the results indicate that the negative slope for privacy concerns is significant under low depletion ($\beta_{PrivacyConcerns_under_LowDepletion_ME} = -.158$; $s.e. = .023$; $p < .001$) but insignificant under high depletion ($\beta_{PrivacyConcerns_under_HighDepletion_ME} = -.027$; $s.e. = .019$; $p > .05$) (see Panel A in Figure 3). Thus, H2 is supported. With regard to H3, the results indicate that the negative slope for privacy concerns is significant under negative mood ($\beta_{PrivacyConcerns_under_Neg.Mood_ME} = -.102$; $s.e. = .016$; $p < .001$) but insignificant under positive mood ($\beta_{PrivacyConcerns_under_Pos.Mood_ME} = .002$; $s.e. = .015$; $p > .05$) (see Panel B in

Figure 3).²⁴ Thus, H3 is supported. In summary, these results suggest that the negative effect of privacy concerns is significantly attenuated under conditions of high depletion or positive mood. Figure 3 depicts this attenuation effect under low vs. high depletion (Panel A) and negative vs. positive mood (Panel B).

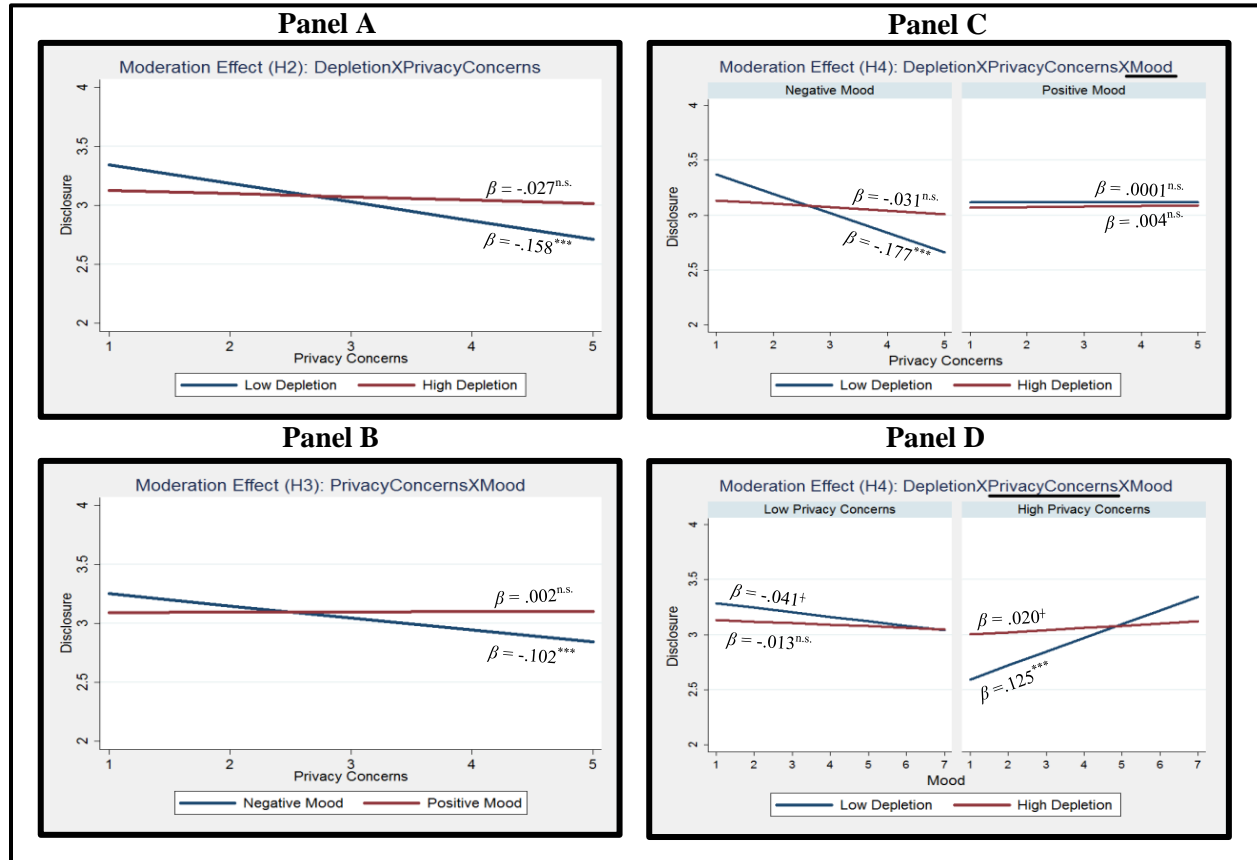
Hypothesis 4 (H4) predicted a 3-way interaction between privacy concerns, cognitive resource depletion, and mood state. Model $_{WLS}$, which provides an omnibus test for this hypothesis, indicates a significant negative effect of the 3-way interaction term ($\beta_{Depletion \times PrivacyConcerns \times Mood} = -.060$; $s.e. = .014$; $p < .001$). To further probe this 3-way interaction and to appropriately test each of the four predictions from H4, we test all possible marginal effects. Figure 3 visualizes this 3-way interaction by mood (Panel C) and by privacy concerns (Panel D).²⁵ Through Panel C, we can interpret the results of the attenuation effect while holding both depletion and mood at different levels.²⁶ Under positive mood and regardless of the depletion condition, the privacy concerns slopes are both positive but not significantly different from zero ($\beta_{PrivacyConcerns_under_LowDepletion\&Pos.Mood_ME} = .0001$; $s.e. = .019$; $p > .05$; $\beta_{PrivacyConcerns_under_HighDepletion\&Pos.Mood_ME} = .004$; $s.e. = .023$; $p > .05$). Under negative mood and low depletion, however, the privacy concerns slope is negative and significant ($\beta_{PrivacyConcerns_under_LowDepletion\&Neg.Mood_ME} = -.177$; $s.e. = .025$; $p < .001$). Under negative mood and high depletion, the privacy concerns slope is negative but not significantly different from zero ($\beta_{PrivacyConcerns_under_HighDepletion\&Neg.Mood_ME} = -.031$; $s.e. = .019$; $p > .05$).

²⁴ The values used to test this moderation effect are -1 *s.d.* below (for negative mood) and +1 *s.d.* above (for positive mood) the mean. Both privacy concerns and mood were mean centered before creating the interaction terms.

²⁵ In Panel D, -1 *s.d.* below (for low privacy concerns) and +1 *s.d.* above (for high privacy concerns) the mean were used to test the effect of mood on disclosure at different levels of privacy concerns.

²⁶ Panel C and its marginal effects provide the most suitable empirical test of our proposed research model. Although we do not hypothesize about the moderation effect of privacy concerns on the relationship between mood and disclosure behavior, we included Panel D to provide further information. In particular, Panel D shows the effect of mood on disclosure while holding both depletion and privacy concerns at different levels. Panel D shows that mood has a significant positive effect on disclosure under low depletion and high privacy concerns ($p < .001$). This effect is marginal under high depletion and high privacy concerns ($p < .10$). While these results are in line with mood theories, for brevity, we do not discuss Panel D in detail, but we include the marginal effects in Figure 3, Panel D.

Figure 3. WLS Post-Estimations (Simple Slope Tests)



We also conducted pairwise comparisons of these marginal effects depicted in Panel C. We use the conservative *Bonferroni* correction as we are comparing more than two slopes in a *post-hoc* test. The *Bonferroni* test indicates significant differences. First, the negative privacy concerns slopes under negative mood are significantly different from each other ($\beta_{Neg.Mood_LowDepletion_vs_Neg.Mood_HighDepletion} = .145$; $s.e. = .032$; $p < .001$). Second, the negative privacy concerns slope under negative mood and low depletion is significantly different from the positive privacy concerns slope under positive mood and low depletion ($\beta_{Neg.Mood_LowDepletion_vs_Pos.Mood_LowDepletion} = .177$; $s.e. = .026$; $p < .001$). Last, the negative privacy concerns slope under negative mood and low depletion is significantly different from the positive privacy concerns slope under positive mood and high depletion ($\beta_{Neg.Mood_LowDepletion_vs_Pos.Mood_HighDepletion} = .177$; $s.e. = .026$; $p < .001$). These results provide full support for the predictions of H4, such that the negative effect of privacy concerns is significant only under the condition of low depletion coupled with a negative mood state (i.e., high-effort cognitive processing).

Discussion

In summary, the results provide compelling support for the notion that the negative effect of privacy concerns is only pronounced under low depletion coupled with negative mood. Said differently, high cognitive depletion and/or positive mood will predict high disclosure behaviors regardless of privacy concerns. In other words, privacy concerns do not play any significant role in predicting disclosure behaviors when individuals' level of effort is low due to depleted cognitive resource and/or a positive mood state. Thus, the privacy paradox is observed for conditions in which individuals rely on low-effort but not high-effort cognitive processing.

EXPERIMENT 2

Building on the results of experiment 1, we conducted a second experiment in which we manipulated not only depletion, but also mood. In order to accomplish this, we developed a new task for experiment 2 which enabled us to manipulate both depletion and mood simultaneously, allowing us to make stronger causal inferences as mood was self-reported in experiment 1. Experiment 2 also adds robustness by demonstrating that the results of experiment 1 can be replicated using a different measure of disclosure behaviors, a different depletion manipulation, and a completely different experimental scenario.

One reason for using a different disclosure scale in experiment 2 is that the disclosure scale in experiment 1 exhibited a low variance which restricted our analytical approach (i.e., it was not feasible to run different analyses using a set of highly sensitive items vs. a set of less-sensitive items due to the low variance observed).²⁷ By moving to a different approach we were able to deepen our understanding of the effect of privacy concerns on disclosure (i.e., privacy concerns may have a stronger (weaker) effect on disclosure of highly (less) sensitive personal information) (Acquisti et al. 2012).

Prior to conducting experiment 2, we ran a pilot test to develop a new disclosure scale that would yield additional variance and we also measured the sensitivity associated with each item (see Appendix B.2). The results from the pilot, as will be described below, enabled us to assess the sensitivity of each

²⁷ Note that low variance reduces statistical power, and hence detecting a significant moderation effect with a low variance in experiment 1's disclosure scale provided a conservative test of the moderation effect (Aguinis et al. 2017, p. 669).

disclosure category in an objective manner. Hence, we provide a richer understanding of our research model as we can test the model using various categories for disclosure behaviors (i.e., demographic, contact, financial, health, and other personal information), which exhibit variation in their sensitivity level.

Method

We developed a new task to manipulate cognitive resource depletion and mood state simultaneously. The task was followed by a set of items to measure disclosure behaviors. This disclosure scale was pilot tested with AMT workers in which 199 participants rated the sensitivity of sharing each item (e.g., year of birth, gender, email domain, zip code, etc.) if they were asked to do so in the context of an AMT study (*1 Not at all sensitive ... 5 Extremely sensitive*). We adapted the privacy concerns scale used in experiment 1. Data for the actual experiment was collected from AMT and participants could earn up to \$0.80 depending on their performance. After excluding those who failed the attention check, did not complete the experimental task, or admitted to have falsified any personal information, the final sample size was 153 (Mean age = 39.55 years, 52.9% female).

Procedure

AMT workers were invited to participate in a study titled “cognitive tasks and mood states.” They were informed that they would complete a writing task followed by a number of survey questions. First, participants were asked to complete a writing task which was designed to induce, at the same time, high or low depletion and positive or negative mood state. The task required participants to simply type [low depletion condition] or decipher [high depletion condition] a set of either positive [positive mood condition] or negative [negative mood condition] statements. The statements were presented in a photo format so that participants would have to actually type their answers. For example, participants in the low depletion and positive mood condition were presented with a set of positive statements (e.g., “*I have only two kinds of days: happy and hysterically happy*”) and were asked to simply type the statements in a field box. Those in the high depletion and positive mood condition were presented with the same statements but with each word shown in the opposite direction (e.g., “*I evah ylno owt sdnik fo syad: yppah dna*”).

yllaciretsyh yppah”). Thus, participants in the high depletion condition had to exert more cognitive effort in deciphering each word. A set of negative statements were used for the negative mood condition (e.g., “*I have only two kinds of days: sad and suicidal sad*” [low depletion] and “*I evah ylno owt sdnik fo syad: das dna ladicius das*” [high depletion]). Participants were randomly assigned to one of the four treatment conditions. After the writing task, participants were asked to respond to manipulation check questions. Then, participants were asked to respond to a set of 21 items (e.g., *year of birth, gender, phone area code, zip code, number of bank accounts owned, number of credit cards owned, health status, risky diseases, religion, sexual orientation, etc.*). Participants were given an option to refuse to provide an answer to any item by choosing “*I prefer not to provide this information.*” Next, participants were asked whether they falsified any personal information, to provide qualitative feedback to tell us why they decided not to provide any of the information asked, and to respond to the privacy concerns scale.²⁸ Finally, participants were debriefed (see Appendix B.2 for the entire instrument).

Manipulation Check

The same three items used in experiment 1 to check the depletion manipulation were again used. Factor analysis and reliability statistics showed convergence of the three items (Cronbach’s $\alpha = .950$). A mean score was computed, and the *t*-test ($t = -5.58$; $df = 151$) results indicated a significant mean difference between the high ($n = 72$; $mean = 3.58$; $s.d. = 1.72$) and low ($n = 81$; $mean = 2.14$; $s.d. = 1.45$) depletion conditions ($p < .001$), indicating that the depletion manipulation was successful. We used the BMIS as a manipulation check for mood state. After creating a mood index, consistent with the method used in experiment 1, we tested whether the mood manipulation was successful. The *t*-test ($t = -4.67$; $df = 151$) results indicated a significant mean difference between the positive ($n = 84$; $mean = 5.11$; $s.d. = 1.27$) and negative ($n = 69$; $mean = 4.15$; $s.d. = 1.24$) mood conditions ($p < .001$), indicating that the mood manipulation was successful. As a robustness check, we tested whether the depletion manipulation unintentionally influenced mood state and whether the mood manipulation unintentionally influenced

²⁸ There was high consistency between the qualitative feedback and the privacy concerns score. Those who decided not to disclose any, some, or all personal information used privacy concerns in their qualitative feedback as a justification and they also scored higher on the privacy concerns scale. Such observation confirms that dispositional privacy concerns impact disclosure behaviors, and not vice versa.

cognitive depletion. The *t*-test results confirmed that there was no confounding effect (i.e., the depletion [mood] manipulation did not significantly influence mood state [cognitive depletion]). Therefore, we concluded that our new task successfully manipulated both cognitive depletion and mood state as intended.

Independent Variables

Although the manipulation check results were positive, we cannot claim that the two manipulated variables are absolutely exogenous (i.e., depletion [mood] manipulation had zero effect on mood state [cognitive depletion]) because both were manipulated simultaneously. It is possible that participants in the high depletion and positive mood condition, because they exerted more cognitive effort, experienced a less positive mood than participants in the low depletion and positive mood condition who exerted lower cognitive effort. This also applies to the other conditions. For this reason, we do not treat cognitive depletion and mood state as separate variables. Rather, our independent variable, or “treatment,” consists of four categories, each one represents one of the four conditions (low depletion & negative mood = 0; high depletion & negative mood = 1; low depletion & positive mood = 2; high depletion & positive mood = 3). Privacy concern was computed using the same method as in experiment 1 (Cronbach’s $\alpha = .959$). Finally, because we did not fix the time spent on completing the task as we did in experiment 1, we control for this variable in the statistical model.

Dependent Variable

Consistent with experiment 1, our main dependent variable is computed based on the total sum of the number of items disclosed. We also utilized the sensitivity ratings we gathered from the pilot test which revealed that items related to finance (i.e., yearly income, name of bank, # of bank accounts owned, and # of credit cards owned) were rated as more sensitive (*mean* = 3.14; *s.d.* = 1.31) than health items (*mean* = 2.51; *s.d.* = 1.31), contact items (*mean* = 2.50; *s.d.* = 1.28), demographic items (*mean* = 1.73; *s.d.* = 1.11), or others (*mean* = 1.92; *s.d.* = 1.20). Based on these ratings, it appears that finance items are the most sensitive items, contact and health items are somewhat sensitive, and the demographic and other miscellaneous items are the least sensitive items. Therefore, we test the research model using four proxies

for the dependent variable: 1) all items as was done in experiment 1, 2) highly sensitive items [finance items], 3) moderately sensitive items [contact and health items], and 4) least sensitive items [demographics and others]. Table 5 shows the correlation matrix for all variables along with their descriptive statistics.

Table 5. Experiment 2 – Correlation Matrix

| | <i>min</i> | <i>max</i> | <i>mean</i> | <i>s.d.</i> | 1 | 2 | 3 | 4 | 5 | 6 |
|--|------------|------------|-------------|-------------|-------|-------|-------|-------|------|---|
| 1- Disclosure (all items) | 0.00 | 21.00 | 15.562 | 5.295 | 1 | | | | | |
| 2- Disclosure (highly sensitive items) | 0.00 | 4.00 | 2.013 | 1.499 | .825 | 1 | | | | |
| 3- Disclosure (moderately sensitive items) | 0.00 | 7.00 | 4.869 | 2.335 | .921 | .719 | 1 | | | |
| 4- Disclosure (least sensitive items) | 0.00 | 10.00 | 8.679 | 2.208 | .862 | .539 | .662 | 1 | | |
| 5- Privacy Concerns | 1.00 | 7.00 | 4.338 | 1.717 | -.263 | -.277 | -.195 | -.236 | 1 | |
| 6- Task Time (in minutes) | 1.14 | 15.24 | 3.618 | 2.123 | .086 | .158 | .025 | .073 | .006 | 1 |

Results

We conducted a series of OLS multiple regressions.²⁹ We tested the following model for each disclosure proxy:

$$Disclosure_i = \beta_0 + \beta_1 PrivacyConcerns_i + \beta_2 Treatment_i + \beta_3 PrivacyConcernsXTreatment_i + \beta_4 TaskTime_i + u_i$$

Based on this model, we can test H1 and H4.³⁰ For brevity, we only present the marginal effect results as they provide a direct test for the main effect of privacy concern and its effect on disclosure behaviors under each of the four conditions (Appendix A.3 presents the regression results). According to Table 6, the results show support for H1 across all models. In addition, the pattern that was observed in experiment 1 – where the effect of privacy concerns was significant (insignificant) under the low (high) depletion and negative (positive) mood condition – continues to be supported across all models. In particular, as postulated in H4, privacy concerns can significantly predict disclosure behaviors when individuals are able to employ high-effort processes (i.e., low depletion coupled with a negative mood state). In contrast, the predictive power of privacy concerns is very weak when the effort level is low due to a depleted cognitive resource and/or a positive mood state. Thus, H4 is supported according to Model 1

²⁹ The homoskedasticity of the variance of residuals was not violated. Therefore, we relied on OLS.

³⁰ Testing H2 and H3 requires modeling cognitive depletion and mood state individually as was done in experiment 1. However, for the reasons discussed above, we model the four conditions in one categorical variable. Nevertheless, we analyzed the results based on the same model used in experiment 1. The marginal effect results provided support for H1, H2, H3, and H4. In fact, the marginal effects from the 3-way interaction between privacy concerns, cognitive depletion, and mood state are exactly the same as those presented in Table 6. This suggests that inferences based on either approach are statistically the same.

and Model 3, whose disclosure measures are comparable to that used in experiment 1 (i.e., the sensitivity level is balanced as in experiment 1).

When we categorized disclosure into highly sensitive (Model 2) and least sensitive items (Model 4), the general conclusion that the effort level is reduced due to either a depleted cognitive resource and/or a positive mood state still applies, but with a minor exception. In particular, Model 4 still shows a significant effect of privacy concerns under high depletion and negative mood ($\beta = -.591$; $p < .05$). This result may suggest that a negative mood state (even with a depleted cognitive resource) may not cause individuals to overlook their privacy concerns when asked to share less-sensitive information.

Table 6. Marginal Effect (Simple Slope Tests) Results

| | Model 1 (All Items) | Model 2 (Highly Sensitive Items) | Model 3 (Moderately Sensitive Items) | Model 4 (Least Sensitive Items) |
|---|-------------------------------|--|--|---|
| <i>PrivacyConcerns</i> (Main Effect; across all conditions) | -.859** (.262) | -.260** (.078) | -.259* (.127) | -.339*** (.092) |
| <i>PrivacyConcerns_under_LowDepletion&NegativeMood</i> | -1.445*** (.350) | -.432*** (.100) | -.531*** (.147) | -.481** (.152) |
| <i>PrivacyConcerns_under_HighDepletion&NegativeMood</i> | -1.133 (.670) | -.315 (.221) | -.226 (.340) | -.591* (.228) |
| <i>PrivacyConcerns_under_LowDepletion&PositiveMood</i> | -.867 (.622) | -.309 (.168) | -.173 (.300) | -.385 (.222) |
| <i>PrivacyConcerns_under_HighDepletion&PositiveMood</i> | -.088 (.408) | -.004 (.129) | -.129 (.198) | .044 (.127) |
| R^2_{OLS} | 11.68% | 15.02% | 6.62% | 10.53% |
| (Adjusted R^2_{OLS}) | (6.78%) | (10.30%) | (1.44%) | (5.56%) |

* $p < .05$; ** $p < .01$; *** $p < .001$

Discussion

The results from experiment 2 provide confirming evidence that while privacy concerns can significantly predict disclosure behaviors when individuals are able to employ high-effort processes, privacy concerns may not be predictive of disclosure behaviors when individuals employ low-effort processes due to a depleted cognitive resource and/or a positive mood state. Consistent with experiment 1, the privacy paradox appears when individuals operate in a low-effort mode of cognitive processing, but disappears when individuals operate in a high-effort mode of cognitive processing.

GENERAL DISCUSSION

The purpose of this study was to examine privacy behaviors under low- vs. high-effort processing. In a recent theoretical paper, Dinev et al. (2015) proposed that some relationships within the original APCO model (Smith et al. 2011) could be disrupted when people engage in low-effort processing. Our results support their proposition that if high-effort processing is present, privacy-relevant information will be processed in a manner consistent with the tenets of the original APCO model. However, if low-effort processing is present, the negative relation between privacy concerns and disclosure behaviors can break down.

We focused on cognitive resource and mood state and their combined effect. While we found a significant negative association between privacy concerns and disclosure behaviors, this relationship did not hold when individuals were 1) cognitively depleted and in a positive mood, 2) cognitively depleted and in a negative mood, or 3) cognitively non-depleted and in a positive mood. This finding was supported in both experiments when we measured disclosure based on the total sum of the disclosure items. These three cases reflect conditions under which people's ability to exert high-effort processing is likely to be compromised. Indeed, greater privacy concerns were associated with less disclosure only when individuals had sufficient cognitive resources (non-depleted) coupled with a negative mood state. These results are consistent with our theorizing based on the ELM, that reduced cognitive resources or positive moods are likely to lead individuals to engage in low-effort processing whereas sufficient cognitive resources coupled with negative moods lead individuals to engage in high-effort processing (Petty and Cacioppo 1981). Our theoretical approach and empirical findings provide a systematic explanation to the privacy paradox phenomenon: the privacy paradox is likely (unlikely) to be observed when the effort level in cognitive processing is reduced (sufficient) due to cognitive and/or affective factors.

Theoretical Implications

Our study contributes to the privacy literature by challenging a widely embraced assumption (i.e., high-effort cognitive processing) in published privacy research while addressing a number of issues in the

extant literature. Previous research found that disfluency resulting from demanding tasks lead to lower disclosure (Alter and Oppenheimer 2009). However, our findings show otherwise. As discussed in the introduction, predicting disclosure behaviors without accounting for privacy concerns could lead to inaccurate inferences. Based on two experiments in which we manipulated cognitive resources using different demanding tasks while measuring privacy concerns, we show that a demanding task leads individuals to overlook their dispositional privacy concerns and become more likely to disclose personal information. To further strengthen our investigation, we accounted for affect which concurrently interacts with cognition in the decision making process (Dolan 2002). Thus, we respond to Farahmand's (2017) call to examine the combined effect of cognition and affect in privacy decisions. The findings suggest that a demanding cognitive task coupled with a positive mood can be even more powerful in robbing individuals of their ability to engage in high-effort processing. Our findings corroborate Dinev et al.'s (2015) enhanced APCO model which suggests that "as processing effort moves from high to low, the impact of extraneous influences becomes greater, possibly to the point that they dominate decision making" (p. 643). We further show that not only external influences (i.e., cognitive depletion) but also internal factors (i.e., mood state) can alter privacy decision making by influencing the cognitive processes that individuals expend. These results add to the existing body of knowledge about privacy theory in general and shed considerable light on the privacy paradox in particular.

The literature has shown wide support for the negative relation between privacy concerns and disclosure outcomes, including intention to disclose, self-report of past disclosure behavior, and in some cases actual disclosure. However, some research has pointed to a privacy paradox, where individuals' privacy concerns are not necessarily predictive of actual disclosure behaviors. In the past, it has been suggested that deviations from the negative relationship between privacy concerns and disclosure might be explained by a number of factors (e.g., relying on intentions instead of measuring actual behaviors, sample characteristics, cultural factors, contextual or situational factors). However, much of this work did not look specifically at how such factors moderate or bound the relationship between privacy concerns and disclosure behaviors, a relationship that defines the paradox. More problematic, prior studies aimed at

explaining the privacy paradox were based on models that were limited in terms of meeting the necessary conditions (i.e., measuring both privacy concerns and privacy decisions and showing evidence for a weak association between these constructs) needed to explain the privacy paradox and this may explain the inconsistent findings concerning the existence of the privacy paradox. As we articulated, it is important to first present valid empirical evidence for the privacy paradox (condition 1 and 2). Then, to explain why the paradox is observed, one needs to identify the conditions that led to such observation. In this study, we showed a number of circumstances under which the privacy paradox can be observed (i.e., reduced cognitive resources and/or positive moods) and we explained such paradoxical decisions as stemming from a reliance on low-effort cognitive processes. The systematic approach we followed can hopefully guide other researchers interested in identifying additional causes of paradoxical privacy decisions.

This study also contributes to the depletion literature as we showed that the depletion effect plays a significant role in attenuating the relationship between privacy concerns and disclosure behaviors. Another contribution to this literature is our examination of how both cognition and affect interact to influence behavior, which supports Hagger et al.'s (2010) suggestion that the decrease in performance in self-control tasks could be due to both depletion and mood effects. We also make a methodological contribution by developing and introducing a new task that manipulates mood and depletion simultaneously which can be applied in future depletion research.

Our findings relating to mood are consistent with predictions suggested by the affect infusion model (Forgas 1995, 2013, 2017). Although analyzing our data from a pure affect perspective was not the main objective, our results are in line with the notion that a positive (negative) mood is associated with higher (lower) level of disclosure, consistent with Forgas's (2011) findings. Still, our study provides additional insights in that the effect of positive mood occurs even in the presence of privacy concerns. Our participants adopted a heuristic (low-effort) processing strategy when they were in a positive mood whereas those in a negative mood adopted a substantive (high-effort) processing strategy.

Our overall theoretical contribution involves both theory testing (i.e., testing the enhanced APCO model) and theory building (i.e., identifying a new moderating effect) (Colquitt and Zapata-Phelan 2007,

p. 1284). In their discussion of the importance of empirical support, Sutton and Staw (1995) emphasize that “subsequent research will of course be necessary to sort out whether the theoretical statements hold up under scrutiny, or whether they will join the long list of theories that only deserve to be true” (p. 383). Given the lack of empirical support for the enhanced APCO model, we advance this model by testing its main theoretical statements while theorizing and testing the joint effect of cognition and affect.

Limitations and Future Research

Our study has some limitations that must be considered when interpreting the findings. First, the statistical generalizability of the findings is limited to the AMT population. AMT has been shown to have advantages over traditional samples, such as college students (Buhrmester et al. 2011; Lowry et al. 2016; Peer et al. 2014); yet, future research is needed to replicate our findings in other populations.

Second, we experimentally manipulated the cognitive capacity expended via the depletion tasks (experiment 1) and both depletion and mood (experiment 2). However, the depletion effect in this study still remains an indirect measure of the cognitive processing level, a limitation that applies to all studies in the depletion dual-task paradigm (Hagger et al. 2010). Nonetheless, cognitive neuroscience research shows that low self-control is associated with low levels of neural recruitment (Hu et al. 2015), which suggests that the depletion effect could reduce the neural activity in the brain and, hence, lead to low-effort processing. Future research can replicate the depletion effect using other demanding tasks (Hagger et al. 2010) while applying advance techniques (e.g., fMRI) to directly measure cognitive processing. It would also be insightful to test how self-control as a trait interacts with the depletion effect to affect the relationship between privacy concerns and disclosure behaviors. It is conceivable that individuals with a high self-control personality are less vulnerable to the adverse effect of depletion. This could have theoretical and practical implications for counteracting the depletion effect in privacy decisions. Another promising research area is to identify ways to reduce the unfavorable effect of demanding tasks and/or positive affect, and hence reversing the privacy paradox. For example, whether privacy alerts prior to the behavioral task are capable of counteracting the effect of reduced cognitive processing is an empirical question worth investigating. Thus, nudges in the form of “distracting pop-up alerts” may capture

people's attention at critical moments, increasing their motivation to attend more carefully before committing to privacy disclosures and encouraging central route processing at key moments in the decision making stream (Acquisti et al. 2017; Petty and Briñol 2010).

Third, we only focused on two conditions that could disrupt the relationship between privacy concerns and disclosure behaviors. Many other factors could directly affect the cognitive effort level that could in turn moderate this relation. Future research is needed to examine these factors (e.g., specific emotions, time constraints, motivations; see Dinev et al. 2015) and their moderating role in order to identify other boundary conditions for the theoretical link between privacy concerns and disclosure behaviors. Furthermore, many heuristics (see Cialdini 2009) used in consumer behavior such as “limited time offers” and “excessive fine print” will also reduce central route processing, and as such, the effect of these techniques may be worth investigating when it comes to people's privacy disclosures.

Finally, we are unable to rule out an alternative explanation that the negative mood state was associated with informed disclosure decision resulting from specific motivation to repair the mood state rather than employment of high-effort processing. In other words, sometimes people in negative moods can distract themselves with other thoughts to get their mind off their negative mood, and these absorption effects (e.g., Chen et al. 2007; Erber and Tesser 1992) could have led negative mood participants to think more about privacy in the current work. That being said, the underlying mechanism involving mood (i.e., more thought among those experiencing negative moods, less thought among those in positive moods) would still be supported but just in the service of other goals. Future research can build upon this work by controlling both depletion and mood in an experimental design while testing the mood-repair alternative hypothesis.

Practical Implications

The results of our study suggest several implications for individuals who are deciding whether to disclose information and for managers who may be responsible for solicitation of personal information. Both individuals and managers should be aware of the importance of various factors that may influence disclosure decisions.

Individuals facing disclosure decisions should recognize that their cognitive resources and mood could impact their decision making. In particular, individuals may be more inclined to disclose information if they are cognitively depleted or in a positive mood even if they have privacy concerns, and they should consider mechanisms that would increase their cognitive resources in such situations (e.g., taking a break before committing to a disclosure action in order to reduce fatigue). At the same time, it is conceivable that a sufficient cognitive resource or an especially negative mood state could lead them to over-examine a disclosure decision or to decline an information disclosure request that was actually innocuous. Thus, especially for individuals who recognize that their level of cognitive awareness is leading them to under- or over-analyze a situation or that they are in a strong mood state as they are rendering a privacy decision, it may be desirable to postpone the decision until those transient factors have dissipated. This is especially important when it comes to disclosure because we live in a world where such actions and their consequences often cannot be undone.

Managers of companies that request personal information from data subjects such as current or prospective customers (e.g., through social media or e-commerce sites) should not assume that consumers are always embracing high-effort processing when making privacy decisions. They could be cognitively fatigued or in an especially good mood, for example, which would reduce their level of cognitive effort as they make their disclosure decisions. If a company is serious about protecting consumers' privacy, its managers should prefer to have (potential) data subjects employing a high-effort cognitive processing mode when making decisions.

However, for companies who may not be quite as committed to protecting consumers' privacy our research raises an ethical quandary: should the company ever take advantage of the fact that specific manipulations can be used to get consumers to lower their guard when responding to disclosure requests? We believe that such manipulations are inappropriate because they violate an implied social contract between data subjects and entities requesting information from them. While a philosophical discourse on this point is beyond our scope and relies on deep analysis of competing theories of the social

responsibility of business (see Smith and Hasnas 1999), we urge managers to tread carefully as they consider their options.

CONCLUSION

Although a growing stream of studies has emerged to examine various factors and contexts associated with privacy decisions, most prior research has tacitly assumed that individuals' decisions are based on high-effort cognitive processing. Little previous attention has been paid to factors that may lead individuals to adopt low-effort cognitive processing and the effect that it can have on disclosure behavior. In this study, we found that employing low-effort cognitive processes due to cognitively depleting tasks and/or positive moods leads to privacy paradoxical decisions, such that individuals' stated privacy concerns did not predict their disclosure behaviors. We hope that this study will lead to additional research in this important stream of privacy decisions under conditions of lower cognitive effort.

REFERENCES

- Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the 5th ACM Conference on Electronic Commerce*, pp. 21-29.
- Acquisti, A., Adjerid, I., and Brandimarte, L. 2013. "Gone in 15 Seconds: The Limits of Privacy Transparency and Control," *IEEE Security & Privacy* (11:4), pp. 72-74.
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., and Wilson, S. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys* (50:3), Article 44.
- Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technology*, G. Danezis and P. Golle (eds.), Cambridge, UK: 6th International Workshop, pp. 36-58.
- Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26-33.
- Acquisti, A., John, L. K., and Loewenstein, G. 2012. "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research* (49:2), pp. 160-174.
- Acquisti, A., Taylor, C. R., and Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (52:2), pp. 1-64.
- Adjerid, I., Acquisti, A., Loewenstein, G. 2018a. "Choice Architecture, Framing, and Cascaded Privacy Choices," *Management Science* (article in advance), pp. 1-24.
- Adjerid, I., Peer, E., and Acquisti, A. 2018b. "Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making," *MIS Quarterly* (42:2), pp. 465-488.
- Adjerid, I., Samat, S., and Acquisti, A. 2016. "A Query-Theory Perspective of Privacy Decision Making," *The Journal of Legal Studies* (45:S2), pp. S97-S121.
- Aguinis, H., Edwards, J. R., and Bradley, K. J. 2017 "Improving Our Understanding of Moderation and Mediation in Strategic Management Research," *Organizational Research Methods* (20:4), pp. 665-685.
- Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.
- Alashoor, T., Fox, G., and Smith, H. J. 2017. "The Priming Effect of Prominent IS Privacy Concerns Scales on Disclosure Outcomes: An Empirical Examination," in *Proceedings of Pre-ICIS Workshop on Information Security and Privacy*, Seoul, South Korea.
- Alter, A. L., and Oppenheimer, D. M. 2009 "Suppressing Secrecy Through Metacognitive Ease: Cognitive Fluency Encourages Self-Disclosure," *Psychological Science* (20:11), pp. 1414-1420.
- Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469-490.
- Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.
- Baddeley, A. D., and Hitch, G. 1974. "Working Memory," in *The Psychology of Learning and Motivation*, Vol. 8, Academic Press, 47-89.
- Balebako, R., Peer, E., Brandimarte, L., Cranor, L. F., and Acquisti, A. 2013. "Is It the Typeset or the Type of Statistics? Disfluent Font and Self-Disclosure," *Learning from Authoritative Security Experiment Results*. Retrieved from <https://www.usenix.org/system/files/2013-laser-balebako.pdf>
- Barber, L. K., and Smit, B. W. 2014. "Using the Networked Fire Chief for Ego-Depletion Research: Measuring Dynamic Decision-Making Effort and Performance," *The Journal of Social Psychology* (154:5), pp. 379-383.

- Barth, S., and de Jong, M. 2017. "The Privacy paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review," *Telematics and Informatics* (34), pp. 1038-1058.
- Beilock, S. L., Rydell, R. J., and McConnell, A. R. 2007. "Stereotype Threat and Working Memory: Mechanisms, Alleviation, and Spillover," *Journal of Experimental Psychology* (136:2), pp. 256-276.
- 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. 1017-1041.
- Bless, H., Bohner, G., Schwarz, N., and Strack, F. 1990. "Mood and Persuasion: A Cognitive Response Analysis," *Personality and Social Psychology Bulletin* (16:2), pp. 331-345.
- Bodenhausen, G. V. 1990. "Stereotypes as Judgmental Heuristics: Evidence of Circadian Variations in Discrimination," *Psychological Science* (1:5), pp. 319-322.
- Bodenhausen, G. V., Kramer, G. P., and Susser, K. 1994 "Happiness and Stereotypic Thinking in Social Judgment," *Journal of Personality and Social Psychology* (66:4), pp. 621-632
- Buhrmester, M., Kwang, T., and Gosling, S. D. 2011. "Amazon's Mechanical Turk a New Source of Inexpensive, Yet High-Quality, Data?," *Perspectives on Psychological Science* (6:1), pp. 3-5.
- Busse, C., Kach, A. P., and Wagner, S. M. 2017. "Boundary Conditions: What They Are, How to Explore Them, Why We Need Them, and When to Consider Them," *Organizational Research Methods* (20:4), pp. 574-609.
- Chen, L., Zhou, S., and Bryant, J. 2007. "Temporal Changes in Mood Repair Through Music Consumption: Effects of Mood, Mood Saliences, and Individual Differences," *Media Psychology* (9:3), pp. 695-713.
- Choi, H., Park, J., and Jung, Y. 2018. "The Role of Privacy Fatigue in Online Privacy Behavior," *Computers in Human Behavior* (81), pp. 42-51.
- Cialdini, R. B. 2009. *Influence: Science and Practice*, Boston: Pearson Education.
- Clark, M. S., and Isen, A. M. 1982. "Toward Understanding the Relationship Between Feeling States and Social Behavior," in *Cognitive Social Psychology*, A. H. Hastorf and A. M. Isen (eds.), New York: Elsevier, pp. 73-108.
- Colquitt, J. A., and Zapata-Phelan, C. P. 2007. "Trends in Theory Building and Theory Testing: A Five-Decade Study of the Academy Of Management Journal," *Academy of Management Journal* (50:6), pp. 1281-1303.
- 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.
- Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323-342.
- Dawson, J. F. 2014. "Moderation in Management Research: What, Why, When, and How," *Journal of Business and Psychology* (29:1), pp. 1-19.
- Debatin, B., Lovejoy, J. P., Horn, A. K., and Hughes, B. N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* (15:1), pp. 83-108.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80,100.
- 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.
- Dolan, R. J. 2002. "Emotion, Cognition, and Behavior," *Science* (298:5596), pp. 1191-1194.
- Edwards, J. R., and Berry, J. W. 2010. "The Presence of Something or the Absence of Nothing: Increasing Theoretical Precision in Management Research," *Organizational Research Methods* (13:4), pp. 668-689.
- Engle, R. W. 2002. "Working Memory Capacity as Executive Attention," *Current Directions in Psychological Science* (11:1), pp. 19-23.

- Erber, R., and Tesser, A. 1992. "Task Effort and the Regulation of Mood: The Absorption Hypothesis," *Journal of Experimental Social Psychology* (28:4), pp. 339-359.
- Farahmand, F. 2017. "Decision and Experienced Utility: Computational Applications in Privacy Decision Making," *IEEE Security & Privacy* (15:6), pp. 68-72.
- Forgas, J. P. 1995. "Mood and Judgment: The Affect Infusion Model (AIM)," *Psychological Bulletin* (117:1), pp. 39-66.
- Forgas, J. P. 2011. "Affective Influences on Self-Disclosure: Mood Effects on the Intimacy and Reciprocity of Disclosing Personal Information," *Journal of Personality and Social Psychology* (100:3), pp. 449-461.
- Forgas, J. P. 2013. "Don't Worry, be Sad! On the Cognitive, Motivational, and Interpersonal Benefits of Negative Mood," *Current Directions in Psychological Science* (22:3), pp. 225-232.
- Forgas, J. P. 2017. "Can Sadness be Good for You?: On the Cognitive, Motivational, and Interpersonal Benefits of Negative Affect," *Australian Psychologist* (52:1), pp. 3-13.
- Frijda, N. H. 1988. "The Laws of Emotion," *American Psychologist* (43:5), pp. 349-358.
- Frijda, N. H. 2007. *The Laws of Emotion*, New Jersey: Lawrence Erlbaum Associates Publishers.
- Frijda, N. H. 2010. "Impulsive Action and Motivation," *Biological Psychology* (84:3), pp. 570-579.
- Gino, F., Schweitzer, M. E., Mead, N. L., and Ariely, D. 2011. "Unable to Resist Temptation: How Self-Control Depletion Promotes Unethical Behavior," *Organizational Behavior and Human Decision Processes* (115:2), pp. 191-203.
- Hagger, M. S., Wood, C., Stiff, C., and Chatzisarantis, N. L. 2010. "Ego Depletion and the Strength Model of Self-Control: A Meta-Analysis," *Psychological Bulletin* (136:4), pp. 495-525.
- Homburg, C., Koschate, N., and Hoyer, W. D. 2006. "The Role of Cognition and Affect in the Formation of Customer Satisfaction: A Dynamic Perspective," *Journal of Marketing* (70:3), pp. 21-31.
- Hu, Q., West, R., and Smarandescu, L. 2015a. "The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective," *Journal of Management Information Systems* (31:4), pp. 6-48.
- Hui, K. L., Teo, H. H., and Lee, S. Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19-33.
- Isen, A. M., Shalcker, T. E., Clark, M., and Karp, L. 1978. "Affect, Accessibility of Material in Memory, and Behavior: A Cognitive Loop?," *Journal of Personality and Social Psychology* (36:1), pp. 1-12.
- Jiang, Z., Heng, C. S., and Choi, B. C. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579-595.
- John, L. K., Acquisti, A., and Loewenstein, G. 2010. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* (37:5), pp. 858-873.
- Karwatzki, S., Dytnenko, O., Trenz, M., and Veit, D. 2017. "Beyond the Personalization-Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* (34:2), pp. 369-400.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.
- Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., and Abdullat, A. 2015. "The Role of Mobile-Computing Self-Efficacy in Consumer Information Disclosure," *Information Systems Journal* (25:6), pp. 637-667.
- Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), pp. 122-134.
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

- Ku, Y. C., Chen, R., and Zhang, H. 2013. "Why Do Users Continue Using Social Networking Sites? An Exploratory Study of Members in the United States and Taiwan," *Information & Management* (50:7), pp. 571-581.
- Li, H., Luo, X. R., Zhang, J., and Xu, H. 2017. "Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors," *Information & Management* (54:8), pp. 1012-1022.
- Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), pp. 434-445.
- Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28:28), pp. 453-496.
- Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp. 471-481.
- Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. 2016. "'Cargo Cult' Science in Traditional Organization and Information Systems Survey Research: A Case for Using Nontraditional Methods of Data Collection, Including Mechanical Turk and Online Panels," *The Journal of Strategic Information Systems* (25:3), pp. 232-240.
- Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers," *Journal of the Association for Information Science and Technology* (63:4), pp. 755-776.
- Marreiros, H., Tonin, M., Vlassopoulos, M., and Schraefel, M. C. 2017. "'Now That You Mention It': A Survey Experiment on Information, Inattention and Online Privacy," *Journal of Economic Behavior & Organization* (140), pp. 1-17.
- Mayer, J. D., and Gaschke, Y. N. 1988. "The Experience and Meta-Experience of Mood," *Journal of Personality and Social Psychology* (55:1), pp. 102-111.
- McConnell, A. R., and Rydell, R. J. 2014. "The Systems of Evaluation Model: A Dual-Systems Approach to Attitudes," in *Dual Process Theories of the Social Mind*, J. W. Sherman, B. Gawronski, and Y. Trope (eds.), New York: Guilford, pp. 204-217.
- Middlewood, B. L., Gallegos, J., and Gasper, K. 2016. "Embracing the Unusual: Feeling Tired and Happy is Associated with Greater Acceptance of Atypical Ideas," *Creativity Research Journal* (28:3), pp. 310-317.
- Miyake, A., and Shah, P. 1999. *Models of Working Memory: Mechanisms of Active Maintenance and Executive Control*, New York: Cambridge University Press.
- Morris, W. N. 1989. *Mood: The Frame of Mind*, New York: Springer-Verlag.
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76-98.
- Muraven, M., and Baumeister, R. F. 2000. "Self-Regulation and Depletion of Limited Resources: Does Self-Control Resemble A Muscle?," *Psychological Bulletin* (126:2), pp. 247-259.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.
- Park, J., and Banaji, M. R. 2000. "Mood and Heuristics: The Influence of Happy and Sad States on Sensitivity and Bias in Stereotyping," *Journal of Personality and Social Psychology* (78:6), pp. 1005-1023.
- Pavlou, P. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly* (35:4), pp. 977-988.
- Peer, E., Vosgerau, J., and Acquisti, A. 2014. "Reputation as a Sufficient Condition for Data Quality on Amazon Mechanical Turk," *Behavior Research Methods* (46:4), pp. 1023-1031.

- Petty, R. E., and Briñol, P. 2010. "Attitude Change," in *Advanced Social Psychology: The State of the Science*, R. F. Baumeister and E. J. Finkel (eds.), Oxford, UK: Oxford University Press, pp. 217-259.
- Petty, R. E., and Cacioppo, J. T. 1981. *Attitudes and Persuasion: Classic and Contemporary Approaches*, Dubuque: William C. Brown.
- Petty, R. E., and Cacioppo, J. T. 1986. *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*, New York: Springer-Verlag.
- Petty, R. E., and Wegener, D. T. 1998. *Attitude Change: Multiple Roles of Persuasion Variables*, New York: McGraw-Hill.
- Petty, R. E., Schumann, D. W., Richman, S. A., and Strathman, A. J. 1993. "Positive Mood and Persuasion: Different Roles for Affect Under High and Low Elaboration Conditions," *Journal of Personality and Social Psychology* (64:1), pp. 5-20.
- Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the UK Who Use Online Communities," *European Journal of Information Systems* (19:2), pp. 181-195.
- Sanna, L. J., Turley-Ames, K. J., and Meier, S. 1999. "Mood, Self-esteem, and Simulated Alternatives: Thought-Provoking Affective Influences on Counterfactual Direction," *Journal of Personality and Social Psychology* (76:4), pp. 543-558.
- Schmeichel, B. J. 2007. "Attention Control, Memory Updating, and Emotion Regulation Temporarily Reduce the Capacity for Executive Control," *Journal of Experimental Psychology: General* (136:2), pp. 241-255.
- Schwarz, N. 1990. "Feelings as Information: Informational and Motivational Functions of Affective States," in *Handbook of Motivation and Cognition: Foundation of Social Behavior*, E. T. Higgins and R. M. Sorrentino (eds.), New York: Guilford Press, pp. 527-561.
- Schwarz, N., and Clore, G. L. 1988. "How Do I Feel About It? Informative Functions of Affective States," in *Affect, Cognition, and Social Behavior*, K. Fiedler and J. Forgas (eds.), Toronto: Hogrefe International, pp. 44-62.
- Schwarz, N., and Clore, G. L. 2007. "Feelings and Phenomenal Experiences," in *Social Psychology: Handbook of Basic Principles*, A. Kruglanski and E. T. Higgins (eds.), New York: Guilford Press, pp. 385-407.
- Smith, H. J., and Hasnas, J. 1999. "Ethics and Information Systems: The Corporate Domain," *MIS Quarterly* (23:1), pp. 109-127.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.
- 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.
- Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477-560.
- 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.
- Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM conference on Electronic Commerce*, Tampa, Florida, USA.
- Stöber, J. 2001. "The Social Desirability Scale-17 (SDS-17): Convergent Validity, Discriminant Validity, and Relationship with Age," *European Journal of Psychological Assessment* (17:3), pp. 222-232.
- Sun, H., and Zhang, P. 2006. "The Role of Affect in IS Research: A Critical Survey and a Research Model," in *Human-Computer Interaction and Management Information Systems: Foundations P*. Zhang and D. Galletta (eds.), Armonk, New York: M. E. Sharpe, pp. 295-329.
- Sun, Y., Liu, D., and Wang, N. 2017. "A Three-Way Interaction Model of Information Withholding: Investigating the Role of Information Sensitivity, Prevention Focus, and Interdependent Self-Construal," *Data and Information Management* (1:1), pp. 61-73.

- Sutanto, J., Palme, E., Tan, C. H., and Phang, C. W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly* (37:4), pp. 1141-1164.
- Sutton, R. I., and Staw, B. M. 1995. "What Theory Is Not," *Administrative Science Quarterly* (40:3), pp. 371-384.
- Taddicken, M. 2014. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure," *Journal of Computer-Mediated Communication* (19:2), pp. 248-273.
- Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268.
- Tucker, C. E. 2014. "Social Networks, Personalized Advertising, and Privacy Controls," *Journal of Marketing Research* (51:5), pp. 546-562.
- Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157-174.
- Wegener, D. T., and Petty, R. E. 1994. "Mood Management Across Affective States: The Hedonic Contingency Hypothesis," *Journal of Personality and Social Psychology* (66:6), pp. 1034-1048.
- Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431-453.
- Whetten, D. A. 1989. "What Constitutes a Theoretical Contribution?," *Academy of Management Review* (14:4), pp. 490-495.
- Willett, J. B., and Singer, J. D. 1988. "Another Cautionary Note About R²: Its Use in Weighted Least-Squares Regression Analysis," *The American Statistician* (42:3), pp. 236-238.
- Williams, R. 2012. "Using the Margins Command to Estimate and Interpret Adjusted Predictions and Marginal Effects," *The Stata Journal* (12:2), pp. 308-331.
- Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., and Acquisti, A. 2014. "Would a Privacy Fundamentalist Sell Their DNA for \$1000... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences," in *Symposium on Usable Privacy and Security (SOUPS)* 5: pp. 1-18.
- Wooldridge, J. M. 2009. *Introductory Econometrics: A Modern Approach*, Canada: South-Western Cengage Learning.
- Xu, H., Teo, H., Tan, B. C., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-174.
- Yu, J., Hu, P. J. H., and Cheng, T. H. 2015. "Role of Affect in Self-Disclosure on Social Network Websites: A Test of Two Competing Models," *Journal of Management Information Systems* (32:2), pp. 239-277.
- Yun, H., Lee, G., and Kim, D. 2014. "A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.
- Zhang, P. 2013. "The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the ICT Context," *MIS Quarterly* (37:1), pp. 247-274.

APPENDIX A: METHOD AND ANALYSIS

Appendix A.1: Experiment 1's Exploratory Factor Analysis

Table A.1 Exploratory Factor Analysis: Maximum Likelihood Extraction with Varimax Rotation

| | 1 | 2 | 3 | 4 | 5 | 6 |
|-------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| | $\alpha = .956$ | $\alpha = .945$ | $\alpha = .924$ | $\alpha = .958$ | $\alpha = .949$ | $\alpha = .960$ |
| Need for Cognition_1 | .750 | .179 | .012 | .036 | -.030 | -.043 |
| Need for Cognition_2 | .758 | .383 | -.030 | .058 | -.018 | -.073 |
| Need for Cognition_3r | .825 | .101 | .163 | .080 | .058 | -.061 |
| Need for Cognition_4r | .833 | .117 | .095 | .023 | -.041 | -.096 |
| Need for Cognition_5r | .779 | -.007 | .253 | .050 | -.065 | -.095 |
| Need for Cognition_6 | .759 | .196 | .000 | .029 | .018 | -.054 |
| Need for Cognition_7r | .789 | .089 | .191 | .019 | -.060 | -.162 |
| Need for Cognition_8r | .632 | .062 | -.041 | .048 | -.144 | .005 |
| Need for Cognition_9r | .739 | .010 | .119 | .034 | -.067 | -.019 |
| Need for Cognition_10 | .776 | .169 | .113 | .054 | .046 | .052 |
| Need for Cognition_11 | .742 | .252 | .033 | .099 | .108 | -.100 |
| Need for Cognition_12r | .770 | .017 | .175 | .153 | .012 | -.014 |
| Need for Cognition_13 | .634 | .140 | -.095 | .149 | .099 | .076 |
| Need for Cognition_14 | .672 | .099 | -.042 | .114 | .002 | .025 |
| Need for Cognition_15 | .759 | .126 | -.002 | .078 | .032 | -.011 |
| Need for Cognition_16r | .569 | .028 | .288 | -.070 | -.068 | -.082 |
| Need for Cognition_17r | .714 | -.138 | .094 | .089 | -.062 | .057 |
| Lively | .229 | .873 | .029 | -.077 | -.047 | -.048 |
| Peppy | .195 | .865 | .013 | -.023 | -.026 | -.013 |
| Active | .141 | .810 | .105 | .014 | -.005 | .025 |
| Happy | .227 | .799 | .288 | .112 | -.069 | .058 |
| Loving | .110 | .810 | .066 | .136 | -.076 | .088 |
| Content | .038 | .715 | .294 | .001 | -.145 | .119 |
| Caring | .141 | .832 | .045 | .100 | -.090 | .024 |
| Nervous | .143 | -.033 | .670 | .036 | -.196 | .117 |
| Gloomy | .129 | .153 | .894 | -.062 | .043 | .002 |
| Fed up | .056 | .251 | .851 | -.047 | -.082 | .094 |
| Sad | .054 | .109 | .783 | -.043 | -.025 | .030 |
| Jittery | .205 | -.030 | .668 | -.003 | -.133 | .074 |
| Grouchy | .066 | .274 | .821 | -.056 | -.129 | .039 |
| Privacy Concerns_1 | .132 | .091 | -.015 | .908 | -.005 | -.188 |
| Privacy Concerns_2 | .128 | .065 | .016 | .867 | .044 | -.269 |
| Privacy Concerns_3 | .154 | .046 | -.055 | .903 | -.010 | -.209 |
| Privacy Concerns_4 | .192 | .045 | -.093 | .855 | .013 | -.196 |
| Manipulation Check_1 | .054 | -.082 | -.139 | .008 | .930 | -.022 |
| Manipulation Check_2 | -.019 | -.182 | -.165 | .031 | .875 | .045 |
| Manipulation Check_3 | .001 | -.099 | -.151 | .003 | .911 | -.076 |
| Disclosure Intention_1r | -.111 | .075 | .177 | -.339 | -.037 | .820 |
| Disclosure Intention_2 | -.087 | .090 | .140 | -.330 | .007 | .877 |
| Disclosure Intention_3 | -.104 | .081 | .070 | -.361 | -.041 | .880 |

Note: items noted with “r” were reversed coded. Cronbach’s α was the measure for construct reliability.

Appendix A.2: Experiment 1's Preliminary Analysis, Control Variables, and Robustness Checks³¹

We argued for a main effect hypothesis (H1) along with two 2-way interaction hypotheses (H2 and H3) and a 3-way interaction hypothesis (H4). We used regression techniques to test these hypotheses. Traditionally, a hierarchical regression approach is used when researchers are testing a main effect hypothesis along with interaction effect hypotheses. For instance, an ordinary least squares (OLS) hierarchical regression approach would suggest a first step using the following model to test H1:

$$\log(\text{Disclosure})_i = \beta_0 + \beta_1 \text{Depletion}_i + \beta_2 \text{PrivacyConcerns}_i + \beta_3 \text{Mood}_i + u_i \quad \text{Model}_{\text{OLS}} \text{ 1 (Step 1)}$$

Based on this approach, β_2 must be significantly different from zero to provide support for H1. Next, this approach would suggest a second step using the following model to test H2 and H3:

$$\log(\text{Disclosure})_i = \beta_0 + \beta_1 \text{Depletion}_i + \beta_2 \text{PrivacyConcerns}_i + \beta_3 \text{Mood}_i + \beta_4 \text{DepletionXPrivacyConcerns}_i + \beta_5 \text{PrivacyConcernsXMood}_i + u_i \quad \text{Model}_{\text{OLS}} \text{ 2 (Step 2)}$$

Then, if β_4 and β_5 are significantly different from zero, H2 and H3 would be supported. The last step would be to use the following model to test H4:

$$\log(\text{Disclosure})_i = \beta_0 + \beta_1 \text{Depletion}_i + \beta_2 \text{PrivacyConcerns}_i + \beta_3 \text{Mood}_i + \beta_4 \text{DepletionXPrivacyConcerns}_i + \beta_5 \text{PrivacyConcernsXMood}_i + \beta_6 \text{DepletionXMood}_i + \beta_7 \text{DepletionXPrivacyConcernsXMood}_i + u_i \quad \text{Model}_{\text{OLS}} \text{ 3 (Step 3)}$$

Based on this approach, if β_7 is significantly different from zero, then H4 is supported.

While Step 3 provides an appropriate (although omnibus) test for H4, we argue against the hierarchical regression approach because testing H1, H2, and H3 is unjustified when the highest level interaction term (the 3-way interaction in our case) is significant. According to Dawson and Richter (2006), a separate step (i.e., hierarchical regression) approach is not essential when testing interaction terms (p. 917). We assert that the hierarchical regression approach could also lead to inaccurate or even erroneous inferences based on significance tests, such as p -values, and confidence intervals. In particular, if we find support for a significant 3-way interaction in Model_{OLS} 3 (Step 3), then relying on Model_{OLS} 1 (Step 1) to test H1 and Model_{OLS} 2 (Step 2) to test H2 and H3 is prone to making inferences based on misspecified models. In other words, there is functional form misspecification in Model_{OLS} 1 (Step 1) and Model_{OLS} 2 (Step 2) due to exclusion of a significant higher level term (the 3-way interaction). Functional form misspecification would mean that the Gauss-Markov zero conditional mean $E(u|x_1, x_2, \dots, x_k) = 0$ assumption is unsatisfied which could in turn lead to biased estimates and biased standard errors (Dawson 2014; Wooldridge 2009). For this reason, we use marginal effects, aka simple slope tests, to test H1, H2, and H3 (Dawson 2014; Dawson and Richter 2006; Kingsley et al. 2017; Williams 2012).

We started with OLS regression to test Model_{OLS} 3 (Step 3), hereafter Model_{OLS} 3. The two variables, *PrivacyConcerns* and *Mood*, were mean-centered before we created the interaction terms (Aiken and West 1991). We examined whether the assumption of homoskedastic variance of residuals

³¹ Although the main purpose of our study is not methodological, we believe it is important to clarify the issues with using hierarchical regression approach considering its wide adoption in IS research involving interaction terms. For more information about the approach we use, see Dawson (2014) and Dawson and Richter (2006). For examples, visit <http://stats.idre.ucla.edu/stata/faq/how-can-i-understand-a-3-way-continuous-interaction-stata-12/>

was satisfied. Homoskedasticity is one of the Gauss-Markov assumptions necessary to make inferences based on p -values and confidence intervals obtained from OLS. The Breusch-Pagan and White tests, whose null hypotheses are homoscedastic variance of residuals, were used to test this assumption. The Breusch-Pagan test revealed a significant result ($\chi^2(1) = 71.23; p < .0001$), suggesting that the variance of residuals in Model_{OLS} 3 is driven by a multiplicative function of one or more of the explanatory variables. The White test, which is a special case of the Breusch-Pagan test, did not reveal a significant result ($\chi^2(17) = 25.58; p > .05$). Although the White test indicated no significant heteroskedasticity in Model_{OLS} 3, caution needs to be taken before relying on its result. The power of the White test to detect significant heteroskedasticity is undermined due to its consumption of too many degrees of freedom relative to our sample size (for more details, see Wooldridge 2009, p. 275). Therefore, the Breusch-Pagan test is more reliable in this case as it is robust against the number of degrees of freedom consumed and hence has more power to detect significant heteroskedasticity. Under heteroskedasticity, OLS coefficient estimates are still unbiased assuming that other Gauss-Markov assumptions are satisfied. However, OLS is not the Best Linear Unbiased Estimator (BLUE) anymore because its standard errors are biased which in turn lead to unreliable significance tests. To fix the heteroskedasticity problem, we relied on weighted least squares (WLS) regression.³²

Estimators obtained from WLS are a special case of generalized least squares (GLS) estimators. WLS is more efficient than OLS if the form of variance is correctly specified (Chatterjee and Hadi 2015; Wooldridge 2009). The form of variance can be specified as a function of explanatory variables and/or some form of the predicted values. The main goal is to minimize the weighted sum of squared residuals, where each squared residual is weighted by $1/w_i$ (Wooldridge 2009). The main idea of WLS is that observations with high error variance are given less weight in the estimation process. To specify the weight function, researchers can use their intuition and knowledge to identify the explanatory variables driving the variance of residuals (Chatterjee and Hadi 2015). Another systematic approach is to examine the scatter plots of the squared residuals versus the predicted values and all explanatory variables obtained from the initial unweighted OLS regression (Chatterjee and Hadi 2015; Berry and Feldman 1985; Wooldridge 2009). We followed the systematic approach and diagnosed all residual plots. After examining the residual plots, it appeared that the variance of residuals is somewhat dependent on some form of the *Mood's* variance. We implemented several weight functions aimed at eliminating heteroskedasticity from Model_{OLS} and chose the following function, which resolved the heteroskedasticity problem right above the 5% significance level.³³

$$w_i = \frac{\hat{y}_i}{Mood_i^2}$$

w_i is the weight function where $w_i > 0$, \hat{y}_i is the predicted values from Model_{OLS}, and $Mood_i$ represents the observations from the mood index after mean centering. The Breusch-Pagan test revealed a non-significant result for this model ($\chi^2(1) = 3.59; p = .058$), suggesting that this weighted model (Model_{WLS}) satisfies the homoskedasticity assumption. Taylor and Todd (1995) suggest that a minimum sample size of $1.5 * K * (K + 1)$, where K is the number of variables, is required for WLS estimation. Our sample size satisfies this requirement. They also state that “WLS does not require the data to be multivariate normal” (Taylor and Todd 1995, p. 158), which makes our use of WLS more appropriate than OLS considering

³² Another option is to use robust standard errors which do not assume homoskedasticity. Considering our sample size, however, using OLS with robust standard errors could also lead to unreliable inferences based on significance tests. This is due to the fact that the distribution of the robust standard errors is unknown for small samples. In OLS, “the robust standard errors and the robust t statistics are justified only as the sample size becomes large” (Wooldridge 2009, p. 268). While identifying the weight function in WLS is more difficult to implement than using robust standard errors, when the weight function is correctly specified, WLS is superior to robust standard errors (Berry and Feldman 1985; Wooldridge 2009). We decided to pursue the more conservative analysis (i.e., WLS) instead of using robust standard errors after OLS. Still, robust standard errors can be used as a robustness check after WLS as they allow the weight function to be arbitrarily misspecified (Wooldridge 2009), and we discuss this in the robustness checks section.

³³ Several other arbitrary weight functions were able to eliminate heteroskedasticity to a large extent. However, we observed that eliminating heteroskedasticity beyond the necessary level could lead to misleading results as the nature of the original variances was significantly impacted.

the normality issue in our data. Accordingly, we resumed the analysis by weighting the OLS model by the specified function (i.e., w_i) and the following model was used to test the hypotheses:

$$\frac{\log(\text{Disclosure})_i}{w_i} = \frac{\beta_0}{w_i} + \beta_1 \frac{\text{Depletion}_i}{w_i} + \beta_2 \frac{\text{PrivacyConcerns}_i}{w_i} + \beta_3 \frac{\text{Mood}_i}{w_i} + \beta_4 \frac{\text{DepletionXPrivacyConcerns}_i}{w_i} + \beta_5 \frac{\text{PrivacyConcernsXMood}_i}{w_i} + \beta_6 \frac{\text{DepletionXMood}_i}{w_i} + \beta_7 \frac{\text{DepletionXPrivacyConcernsXMood}_i}{w_i} + \frac{u_i}{w_i} \quad (\text{Model}_{\text{WLS}} 1)$$

Table A.2.1 presents a series of regression results. Model_{WLS} 1 is the final model reported in the article to test our hypotheses. The control variables are included in Model_{WLS} 2; although this model shows significant results for the control variables, the robustness checks (see next paragraph) did not support these results. We also report OLS results (Model_{OLS} 3 and Model_{OLS} 4) along with WLS results after robust standard errors (Model_{WLS} 5 and Model_{WLS} 6). These later models are used as robustness checks that are essential to evaluate Model_{WLS} 1.

Control Variables

Model_{WLS} 2 in Table A.2.1 presents the WLS estimates after controlling for need for cognition, disclosure intention, and social desirability. To make sure that our inferences are precise, we ran the Breusch-Pagan test again to test whether adding the control variables resulted in heteroskedastic variance of residuals. Table A.2.1 indicates that the Breusch-Pagan test revealed insignificant results for Model_{WLS} 2, suggesting that adding the controls did not impact the homoskedastic nature of our original WLS model (i.e., Model_{WLS} 1). Our hypothesis tests are still consistent after adding the control variables. Note that need for cognition and social desirability are significant. However, caution needs to be taken before making a conclusion about these two control variables. One reason is that OLS regression did not indicate significant estimates for these two control variables (Table A.2.1, Model_{OLS} 4), but this is not essential to refute these results since the pattern is consistent between OLS and WLS. More important is that after running WLS with robust standard errors, both need for cognition and social desirability are not significant anymore (Table A.2.1, Model_{WLS} 6); this model provides a robust test of these variables and hence we rely on it and declare no support for a significant effect of need for condition and social desirability. Next, we discuss some robustness checks which also clarify why relying on robust standard errors after WLS is important.

Robustness Checks: WLS versus OLS

Does our main conclusion based on the results from WLS regression change if we ignore the heteroskedasticity issue altogether and rely on OLS? If the results from WLS and OLS are in complete disagreement, this would be indicative of functional form misspecification (Wooldridge 2009). Above, we discussed the problematic use of the hierarchical regression approach and why it could lead to inaccurate inferences. In fact, we conducted several other analyses using the hierarchical regression approach and the resulting disagreement between WLS and OLS in Model_{OLS} 1 (Step 1) and Model_{OLS} 2 (Step 2) confirmed its inappropriateness in testing H1, H2, and H3.³⁴

³⁴ Before running the hierarchical regression approach, we tested for heteroskedasticity in Model_{OLS} 1 (Step 1) and Model_{OLS} 2 (Step 2). Noteworthy, Model_{OLS} 3 (Step 3) which we assume as the correctly specified model indicated the least heteroskedasticity ($\chi^2(1) = 71.23$) compared to Model_{OLS} 1's ($\chi^2(1) = 99.35$) and Model_{OLS} 2's ($\chi^2(1) = 97.67$). A Chi-square difference test indicated that Model_{OLS} 3's heteroskedasticity is significantly lower than Model_{OLS} 1's ($\chi^2_{\text{diff}}(4) = 28.12$; $p < .001$) and Model_{OLS} 2's ($\chi^2_{\text{diff}}(2) = 26.44$; $p < .001$). This suggests that Model_{OLS} 3 is the most appropriately specified model, simply because exclusion of significant interaction terms can lead not only to

Table A.2.1 Regression Results
Dependent Variable: log(Disclosure)

| | Model 1 | Model 2 | Model 3 | Model 4 | Model 5 | Model 6 |
|---|----------------------|----------------------|--------------------|--------------------|-----------------------------|--------------------|
| | WLS | WLS | OLS | OLS | WLS | WLS |
| | β | β | β | β | β | β |
| | (s.e.) | (s.e.) | (s.e.) | (s.e.) | (robust s.e.) | (robust s.e.) |
| <i>Constant</i> | 3.066*** (.020) | 3.004*** (.076) | 3.086*** (.014) | 3.053*** (.064) | 3.066*** (.029) | 3.004*** (.129) |
| <i>Depletion (high)</i> | .009 (.032) | .014 (.030) | .003 (.020) | .002 (.020) | .009 (.037) | .014 (.037) |
| <i>PrivacyConcerns</i> | -.088*** (.018) | -.093*** (.020) | -.028* (.014) | -.022 (.015) | -.088** (.028) | -.093** (.032) |
| <i>Mood</i> | .042** (.013) | .046** (.014) | .036** (.012) | .038** (.013) | .042 [†] (.021) | .046* (.021) |
| <i>DepletionXPrivacyConcerns</i> | .075** (.026) | .075** (.026) | .026 (.018) | .024 (.019) | .075* (.036) | .075* (.037) |
| <i>PrivacyConcernsXMood</i> | .076*** (.011) | .074*** (.010) | .038** (.012) | .036** (.012) | .076*** (.021) | .074*** (.020) |
| <i>DepletionXMood</i> | -.039* (.017) | -.043* (.016) | -.008 (.018) | -.012 (.018) | -.039 (.026) | -.043 (.027) |
| <i>DepletionXPrivacyConcernsXMood</i> | -.060*** (.014) | -.057*** (.013) | -.040* (.016) | -.040* (.016) | -.060* (.029) | -.057* (.024) |
| Control Variables | | | | | | |
| <i>NeedForCognition</i> | - | .043** (.013) | - | .011 (.013) | - | .043 (.026) |
| <i>DisclosureIntention</i> | - | -.001 (.009) | - | -.005 (.007) | - | -.001 (.012) |
| <i>SocialDesirability</i> | - | -.010** (.003) | - | -.004 (.002) | - | -.010 (.005) |
| <i>Breusch – Pagan Test, $\chi^2(1)$</i> | 3.59 ^{n.s.} | 2.11 ^{n.s.} | 71.23*** | 73.96*** | - | - |
| <i>F value</i> | 23.41*** | 21.12*** | 4.04*** | 3.18** | 3.41** | 2.79** |

[†] $p < .1$; * $p < .05$; ** $p < .01$; *** $p < .001$; Model_{WLS} 1 is the final model reported in the article.

According to Wooldridge (2009), “OLS and WLS estimates can be substantially different. This is not such a big problem... The issue is whether their difference is enough to change important conclusions” (p. 286). Although our results show some minor differences in the patterns of some estimates, such as the slopes under high depletion in Panel C and Panel G (Figure A.2.1), these differences are negligible because they are exhibiting relatively similar magnitudes and more importantly they are not significant. A serious problem in the model occurs when WLS and OLS indicate significant estimates that differ in sign or are practically large (Wooldridge 2009). Table A.2.1 and Figure A.2.1 demonstrate that our main conclusion is the same when comparing WLS with OLS (compare Model_{WLS} 1 vs. Model_{OLS} 3; Model_{WLS} 2 vs. Model_{OLS} 4 in Table A.2.1; and Panels A-D vs. Panels E-H in Figure A.2.1). Because there is high convergence between the WLS and OLS results suggesting that the

biased estimates but also strong heteroskedasticity (Wooldridge 2009). This argument was further supported when we compared WLS with OLS based on the hierarchical regression approach. In particular, only minor convergence was indicated between WLS and OLS in Step 1 and Step 2, suggesting that both Model_{OLS} 1 (Step 1) and Model_{OLS} 2 (Step 2) are subject to functional form misspecification. Therefore, using the hierarchical approach would have led us to make inaccurate inferences.

functional form was correctly specified (Chatterjee and Hadi 2015; Wooldridge 2009), we concluded that the WLS results are more efficient and reliable than OLS whose significance tests are unreliable due to heteroskedasticity.³⁵

Using robust standard errors after WLS is a final robustness check to test the difference between WLS and OLS. We report WLS with robust standard errors before (Model_{WLS} 5) and after (Model_{WLS} 6) including the control variables. Our main results still remain consistent.³⁶ Note that the two control variables (i.e., need for cognition and social desirability) are not significant anymore after using the robust standard errors. We conducted an F test to test the joint significance of the three control variables in Model_{OLS} 4 and Model_{WLS} 6. The F test results indicated that these variables are not jointly significant in both Model_{OLS} 4 ($F(3, 139) = 1.15; p > .05$) and Model_{WLS} 6 ($F(3, 139) = 2.06; p > .05$). This suggests that the fit of these models after including the control variables do not improve significantly. The F values for these models actually dropped a bit after adding the control variables (see Table A.2.1). These results accordingly provide support for dropping the control variables and hence relying on those models without the control variables (Wooldridge 2009).

Another important utility of using robust standard errors after WLS is to test whether the weight function is misspecified (Wooldridge 2009). In particular, the robust standard errors allow the weight function to be arbitrarily misspecified. Because our results from Model_{WLS} 5 are consistent with those in Model_{WLS} 1, we concluded that the weight function applied is robust and correctly specified.

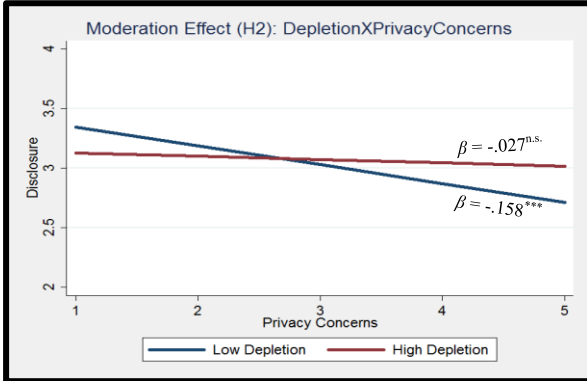
³⁵ We further tested the possibility that our functional form is misspecified due to exclusion of the nonlinear variables *PrivacyConcerns*² and *Mood*² which could have caused the heteroskedasticity issue in the first place (i.e., Model_{OLS} 3). According to the Breusch-Pagan test, adding these quadratic terms did not significantly reduce heteroskedasticity ($\chi^2(1) = 68.49$) compared to the unweighted OLS Model_{OLS} 3 ($\chi^2(1) = 71.23$); ($\chi^2_{diff}(2) = 2.74; p > .05$). The inclusion of the quadratic terms to Model_{OLS} 3 “provides a conservative test of the interaction – if the [*DepletionXPrivacyConcernsXMood*] term is still significant despite the inclusion of the other terms, then there is likely to be a true moderating effect above and beyond any curvilinear effects” (Dawson 2014, p. 15 – [parentheses added]). However, “if both curvilinear and interaction terms are found to be significant, then it would often make sense to test for curvilinear moderation” (Dawson 2014, p. 15). An F test for joint significance indicated that the quadratic terms are not jointly significant ($F(2, 140) = 2.27; p > .05$) while the 3-way interaction terms is still significant. Therefore, we concluded that our linear model was correctly specified.

³⁶ We repeated all tests for marginal effects with robust standard errors based on Model_{WLS} 5 and the results remain consistent.

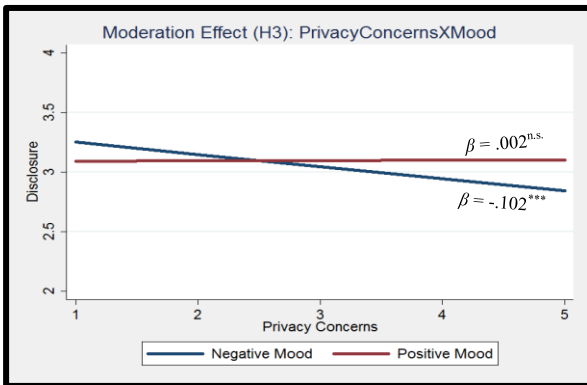
Figure A.2.1. WLS and OLS Post-Estimations.

Weighted Least Squares (WLS) Post-Estimations

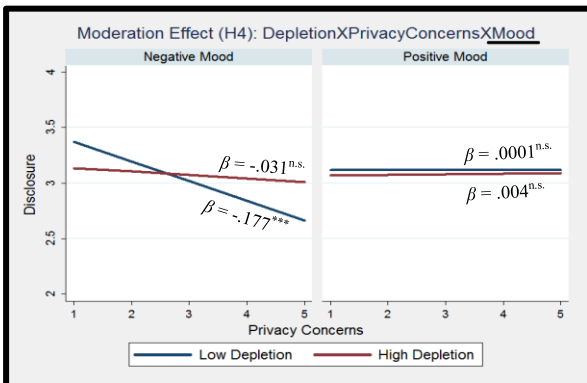
Panel A



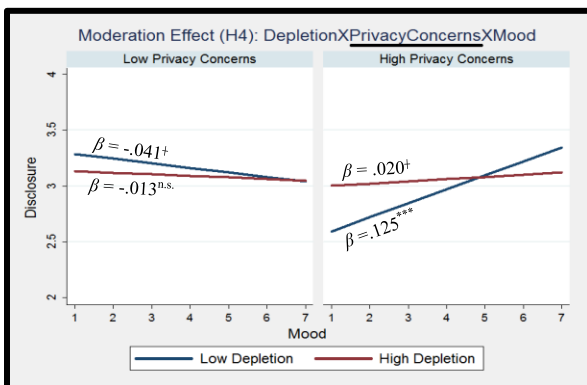
Panel B



Panel C

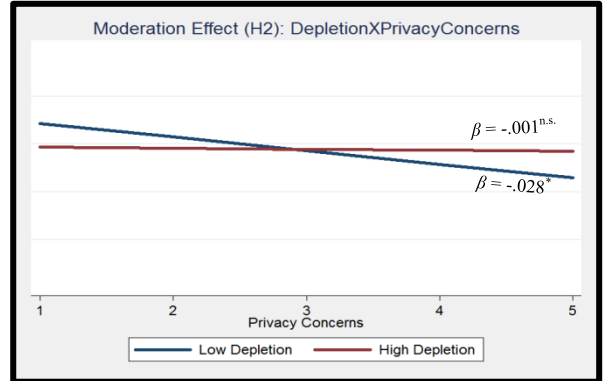


Panel D

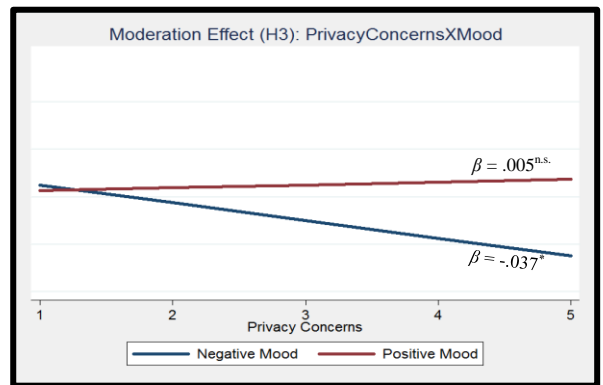


Ordinary Least Squares (OLS) Post-Estimations

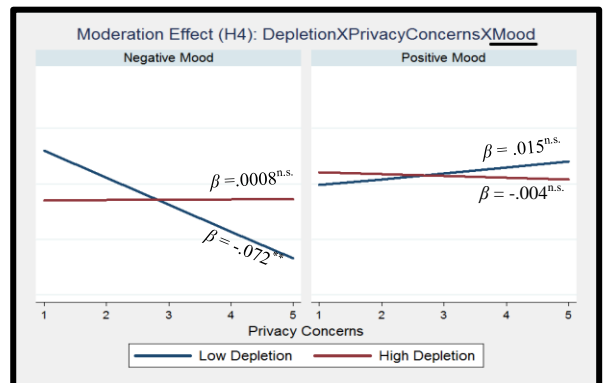
Panel E



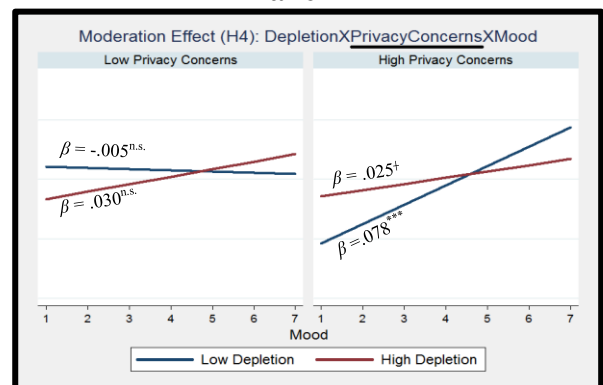
Panel F



Panel G



Panel H



Appendix A.3: Experiment 2's OLS Regression Results

Table A.3 Regression Results; Dependent Variable: Disclosure

| | Model 1 (All items) | Model 2 (Highly sensitive items) | Model 3 (Moderately sensitive items) | Model 4 (Least sensitive items) |
|---|-------------------------------|--|--|---|
| | β | β | β | β |
| <i>Constant</i> | 15.063*** (1.013) | 1.630*** (.285) | 5.090*** (.446) | 8.342*** (.409) |
| <i>PrivacyConcerns</i> | -1.445*** (.350) | -.432*** (.100) | -.531*** (.147) | -.481** (.152) |
| Treatment | | | | |
| <i>HighDepletion&NegativeMood</i> | .346 (1.215) | .163 (.369) | -.165 (.560) | .348 (.493) |
| <i>LowDepletion&PositiveMood</i> | -1.052 (1.154) | -.207 (.311) | -.630 (.508) | -.214 (.496) |
| <i>HighDepletion&PositiveMood</i> | -.332 (1.085) | -.184 (.311) | -.402 (.503) | .255 (.441) |
| Interaction Terms | | | | |
| <i>PrivacyConcernsXHighDepletion&NegativeMood</i> | .312 (.756) | .117 (.244) | .304 (.371) | -.109 (.272) |
| <i>PrivacyConcernsXLowDepletion&PositiveMood</i> | .577 (.714) | .123 (.196) | .358 (.334) | .096 (.270) |
| <i>PrivacyConcernsXHighDepletion&PositiveMood</i> | 1.356* (.544) | .428* (.165) | .401 (.249) | .525* (.200) |
| Control Variables | | | | |
| <i>Task_Time</i> | .003 (.003) | .002* (.000) | .000 (.001) | .001 (.001) |
| <i>F value</i> | 3.90*** | 4.18*** | 3.66*** | 3.60*** |

† $p < .1$; * $p < .05$; ** $p < .01$; *** $p < .001$. *LowDepletion&NegativeMood* is the reference category.

Note: The results indicate a significant moderation effect such that the negative effect of privacy concerns on disclosure behaviors is significantly weaker under the high depletion and positive mood condition relative to the low depletion and negative mood condition (i.e., reference category). This is supported across all models (Model 1: $\beta_{PrivacyConcernsXHighDepletion\&PositiveMood} = 1.356$; $s.e. = .544$; $p < .05$; Model 2: $\beta_{PrivacyConcernsXHighDepletion\&PositiveMood} = .428$; $s.e. = .165$; $p < .05$; Model 4: $\beta_{PrivacyConcernsXHighDepletion\&PositiveMood} = .525$; $s.e. = .200$; $p < .05$), except Model 3 which does not show a significant moderation effect (Model 3: $\beta_{PrivacyConcernsXHighDepletion\&PositiveMood} = .401$; $s.e. = .249$; $p > .05$). Nevertheless, these results do not inform us about the significance of the negative effect of privacy concerns under each condition. They simply indicate whether the difference between each of the three slopes (i.e., interaction terms) and the slope for privacy concerns under low depletion and negative mood (i.e., reference category) is significantly different from zero. Therefore, to test our hypothesis (i.e., H4) more directly, we probe the marginal effects for the four slopes (for more details, see Kingsley et al. 2017). As presented in the article, the marginal effect results indicate that the negative effect of privacy concerns is significant under the low depletion and negative mood condition, but insignificant under the high depletion and positive mood condition, across all models. Such findings provide additional support for experiment 1's findings which revealed that the level of privacy concern is more (less) predictive of disclosure behaviors for individuals in a non-depleted condition coupled with a negative mood state (a depleted condition coupled with a positive mood state).

Appendix A: References

- Aiken, L. S., and West, S. G. 1991. *Multiple Regression: Testing and interpreting interactions*, CA: Sage, Newbury Park.
- Berry, W. D., and Feldman, S. 1985. *Multiple Regression in Practice*, Thousand Oaks, California: Sage Publications, Inc.
- Chatterjee, S., and Hadi, A. S. 2015 *Regression Analysis by Example*, New Jersey: John Wiley & Sons, Inc.
- Dawson, J. F. 2014. "Moderation in Management Research: What, Why, When, and How," *Journal of Business and Psychology* (29:1), pp. 1-19.
- Dawson, J. F., and Richter, A. W. 2006. "Probing Three-Way Interactions in Moderated Multiple Regression: Development and Application of a Slope Difference Test," *Journal of Applied Psychology* (91:4), pp. 917-926.
- Kingsley, A. F., Noordewier, T. G., and Bergh, R. G. V. 2017. "Overstating and Understating Interaction Results in International Business Research," *Journal of World Business* (52:2), pp. 286-295.
- Taylor, S., and Todd, P. A. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2), pp. 144-176.
- Williams, R. 2012. "Using the Margins Command to Estimate and Interpret Adjusted Predictions and Marginal Effects," *The Stata Journal* (12:2), pp, 308-331.
- Wooldridge, J. M. 2009. *Introductory Econometrics: A Modern Approach*, Canada: South-Western Cengage Learning.

APPENDIX B: STUDY INSTRUMENTS

(*reversed items)

Appendix B.1: Experiment 1's Instrument

Privacy Concerns Scale (Dinev and Hart 2006) (1 Strongly disagree ... 5 Strongly agree)

For each of the following, please indicate how much you agree or disagree with the statement. We are interested in your opinion whether or not you currently use mobile health apps.

- 1- I am concerned that the information I submit to mobile health applications could be misused.
- 2- I am concerned that others can find private information about me from mobile health applications.
- 3- I am concerned about providing personal information to mobile health applications, because of what others might do with it.
- 4- I am concerned about providing personal information to mobile health applications, because it could be used in a way I did not foresee.

Disclosure Intention (Malhotra et al. 2004)

Specify the extent to which you would reveal your personal information to use mobile health applications:

(1 Willing ... 7 Unwilling)*

(1 Unlikely ... 7 Likely)

(1 Not probable ... 7 Probable)

Need for Cognition (Cacioppo and Petty 1982) (1 Strongly disagree ... 5 Strongly agree)

- 1- I would prefer complex to simple problems.
- 2- I like to have the responsibility of handling a situation that requires a lot of thinking.
- 3- Thinking is not my idea of fun.*
- 4- I would rather do something that requires little thought than something that is sure to challenge my thinking abilities.*
- 5- I try to anticipate and avoid situations where there is likely chance I will have to think in depth about something.*
- 6- I find satisfaction in deliberating hard and for long hours.
- 7- I only think as hard as I have to.*
- 8- I prefer to think about small, daily projects to long-term ones.*
- 9- I like tasks that require little thought once I've learned them.*
- 10- The idea of relying on thought to make my way to the top appeals to me.
- 11- I really enjoy a task that involves coming up with new solutions to problems.
- 12- Learning new ways to think doesn't excite me very much.*
- 13- I prefer my life to be filled with puzzles that I must solve.
- 14- The notion of thinking abstractly is appealing to me.
- 15- I would prefer a task that is intellectual, difficult, and important to one that is somewhat important but does not require much thought.
- 16- I feel relief rather than satisfaction after completing a task that required a lot of mental effort.*
- 17- It's enough for me that something gets the job done; I don't care how or why it works.*
- 18- I usually end up deliberating about issues even when they do not affect me personally. (this item was dropped in the final analysis)

Social Desirability (Stöber 2001) (True ... False)

- 1- I sometimes litter.
- 2- I always admit my mistakes openly and face the potential negative consequences.
- 3- In traffic I am always polite and considerate of others.

- 4- I have tried illegal drugs (for example, marijuana, cocaine, etc.)
- 5- I always accept others' opinions, even when they don't agree with my own.
- 6- I take out my bad moods on others now and then.
- 7- There has been an occasion when I took advantage of someone else.
- 8- In conversations I always listen attentively and let others finish their sentences.
- 9- I never hesitate to help someone in case of emergency.
- 10- When I have made a promise, I keep it – no ifs, ands, or buts.
- 11- I occasionally speak badly of others behind their back.
- 12- I would never live off other people.
- 13- I always stay friendly and courteous with other people, even when I am stressed out.
- 14- During arguments I always stay objective and matter-of-fact.
- 15- There has been at least one occasion when I failed to return an item that I borrowed.
- 16- I always eat a healthy diet.
- 17- Sometimes I only help because I expect something in return.

Study Instructions (Cover Story)

“This study is part of a mobile health application (“app”) development project. The mobile app is developed to predict individuals’ learning abilities based on their health status and habits. We will briefly test your reading and writing skills. We will also ask for some personal information about your health and habits. The personal information you provide might be used by the mobile app developer.”

Reading Task Instructions

“Next, you will be presented with a short passage that you are asked to read. You will be asked to answer three questions after you finish reading. Please read carefully because part of your bonus will depend on whether you answer the questions correctly.”³⁷

Reading Task and Questions³⁸

Writing Task#1 Instructions (Schmeichel 2007)

“This task requires you to write a short essay about one or two common health issues in your country. You are asked NOT to use any word that contains both the letters (*A and N [high depletion]; X and Z [low depletion]*) in your essay. You will have 6 minutes to finish this task. You will be automatically directed to the next section after 6 minutes.

A large portion of the \$2.00 bonus will depend on the number of words you type and the quality of your essay. Type as much as you can with NO words containing both the letters (*A and N [high depletion]; X and Z [low depletion]*). Time countdown begins as you proceed to the next page. These instructions will also appear in the next page.”³⁹

Disclosure Measurement (Set# 1) (developed)

- 1- What is your weight in lbs.?
[Weight: ____; I prefer not to provide this information]
- 2- What is your height in feet and inches?
[Height: ____; I prefer not to provide this information]
- 3- In the course of an average week, how much time do you spend in strenuous exercise (cardiovascular or muscular)?

³⁷ In the consent form, participants were told that they will receive \$1.00 for completing the study. Participants were also told that they have a chance to receive a bonus payment of \$2.00 depending on their performance. They were informed that instructions on how to complete the tasks properly will be provided and they were promised the bonus payment if they followed the instructions and completed the study. We adopted this value-inducement approach to ensure participants’ involvement in the study.

³⁸ The reading passage and its questions can be requested from the first author.

³⁹ The rationale for using value inducement in the writing tasks (i.e., the bonus depends on the quality of the essay) is similar to that used in the reading task, which is to ensure participants’ involvement in the task.

- [Number of hours: ____; I prefer not to provide this information]
- 4- How many times did you visit a doctor in the past 3 months?
[Number of times: ____; I prefer not to provide this information]
- 5- Do you take medications prescribed by a doctor on a regular basis?
[Yes; No; I prefer not to provide this information]
- 6- In a typical day, how many times do you urinate?
[Number of times: ____; I prefer not to provide this information]
- 7- In an average day, how often do you pass gas (flatulence)?
[Never; Rarely; Sometimes; Often; Very often; I prefer not to provide this information]
- 8- Do you have diabetes?
[Yes; No; I prefer not to provide this information]
- 9- Do you use birth control (e.g., pregnancy pills for females and condom for males)?
[Yes; No; I prefer not to provide this information]
- 10- During the last 12 months, how many alcoholic drinks did you have on a typical day when you drank alcohol?
[Number: ____; I prefer not to provide this information]
- 11- Do you have any chronic disease?
[Yes, specify ____; No; I prefer not to provide this information]
- 12- Have you or any of your significant others suffered from the health issue(s) you have mentioned in the writing task?
[Yes; No; I prefer not to provide this information]

Writing Task#2 Instructions (Schmeichel 2007)

“This task requires you to write another short essay about one good habit and one bad habit. You are asked NOT to use any word that contains both the letters (*E and N [high depletion]; Q and Z [low depletion]*) in your essay. You will have 6 minutes to finish this task. You will be automatically directed to the next section after 6 minutes.

A large portion of the \$2.00 bonus will depend on the number of words you type and the quality of your essay. Type as much as you can with NO words containing both the letters (*E and N [high depletion]; Q and Z [low depletion]*). Time countdown begins as you proceed to the next page. These instructions will also appear in the next page.”

Disclosure Measurement (Set# 2) (developed)

- 1- Do you ever take an elevator to go up or down one floor in a building?
[Yes; No; I prefer not to provide this information]
- 2- How many hours of sleep do you get on a normal night during the weekdays?
[Number of hours: ____; I prefer not to provide this information]
- 3- How many hours of sleep do you get on a normal weekend night?
[Number of hours: ____; I prefer not to provide this information]
- 4- Do you smoke cigarettes (regularly or occasionally)?
[Yes; No; I prefer not to provide this information]
- 5- Do you currently follow dietary restrictions?
[Yes; No; I prefer not to provide this information]
- 6- In an average day, how often do you pick your nose?
[Never; Rarely; Sometimes; Often; Very often; I prefer not to provide this information]
- 7- How often do you wash your hands after picking your nose?
[Never; Rarely; Sometimes; Often; Very often; I prefer not to provide this information]
- 8- How often do you pick your nose in public?
[Never; Rarely; Sometimes; Often; Very often; I prefer not to provide this information]
- 9- How often do you wash your hands after using the restroom?
[Never; Rarely; Sometimes; Often; Very often; I prefer not to provide this information]

10- What is your sexual orientation?

[Sexual orientation: _____; I prefer not to provide this information]

11- In an average week, how often do you spend time looking at / pornographic material?

[Never; Rarely; Sometimes; Often; Very often; I prefer not to provide this information]

Depletion Manipulation Check (developed)

We would like to know how you feel about the writing skills tests.

- | | |
|--|--|
| 1- How difficult was the writing task? | <i>(1 Not at all difficult ... 7 Very difficult)</i> |
| 2- How challenging was the writing task? | <i>(1 Not at all challenging ... 7 Very challenging)</i> |
| 3- How taxing was the writing task? | <i>(1 Not at all taxing ... 7 Very taxing)</i> |

The BMIS (The Brief Mood Introspection Scale) (Mayer and Gaschke 1988)

Indicate how well each adjective or phrase describes your present mood.

(1 Definitely do not feel ... 7 Definitely feel)

- 1- Lively
- 2- Peppy
- 3- Active
- 4- Happy
- 5- Loving
- 6- Caring
- 7- Drowsy
- 8- Tired
- 9- Nervous
- 10- Calm
- 11- Gloomy
- 12- Fed up
- 13- Sad
- 14- Jittery
- 15- Grouchy
- 16- Content

Appendix B.2: Experiment 2's Pilot Test and Instrument

Pilot Test

This pilot test was conducted to assess the sensitivity of each item in the new disclosure behavior scale.

Sensitivity Ratings (developed) (1 Not at all sensitive ... 5 Extremely sensitive)

Many other MTurk studies request you to provide personal data, which might be related to your demographics, contact information, location, health, finances, or other categories.

Please note that we are NOT asking you to provide any personal data. For each data type below, how sensitive would you rate a request from an MTurk study asking you to disclose this information?

1. Year of birth
2. Gender
3. Ethnicity
4. Email domain (Note: not your email account, just the domain, e.g., Hotmail, Yahoo, Gmail, etc.)
5. First 3-digits (area code) of your cell phone number
6. State you live in
7. Zip code
8. Yearly income
9. Name of the bank with which you hold your main account
10. Number of bank accounts you have
11. Number of credit cards you have
12. Health status
13. Fitness level
14. Risky diseases you have
15. Religion
16. Political preference
17. Sexual preference
18. Number of siblings you have
19. Whether you are a parent
20. Marital status
21. Employment status

Experiment 2's Instrument

Writing Task (developed)⁴⁰

Using the keyboard, type each of the phrases appearing in the gray box by writing each word in the opposite direction (i.e., backward). Example:

Original Phrase: "m'I a lacinahceM kruT rekroW."

Correct Answer: "I'm a Mechanical Turk Worker."

High Depletion & Positive Mood Condition

ehT tsom tnatropmi gniht si ot yojne ruoy efil – ot eb yppah – ti si lla taht srettam.
eB yppah rof siht tmemom. sihT tmemom si ruoy efil. yojnE ti, leef ti, esuaceb ti si gnineppah won.
uoY t'nac yub ssenippah tub uoy nac yub eci maerc. dnA taht si dnik fo eht emas gniht.
erehT era os ynam lufituaeb snosaer ot eb yppah. eB uoy. oD uoy. roF uoy.
I evah ylno owt sdnik fo syad: yppah dna yllaciretsyh yppah.
efiL si trohs. elimS elihw uoy llits evah hteet.

High Depletion & Negative Mood Condition

efiL si das. niaP dna gnireffus era lla dnuora su.
oN rettam woh drah uoy yrt, ll'uoy netfo liaf.
sA uoy ega, uoy lliw revocsid sehca dna sniap taht uoy reven dah erofeb.
efiL si drah. nehT uoy eid. nehT yeht worht trid ni ruoy ecaf. nehT eht smrow tae uoy.
noisserpeD si ekil a ssenivaeh uoy t'nac reve epacse; s'ti ni ruoy senob dna ruoy doolb.
I evah ylno owt sdnik fo syad: das dna ladicius das.
efiL si trohs dna htaed smia ylno ecno, tub reven sessim.

Using the keyboard, type each of the phrases appearing in the gray box exactly as they appear. Example:

Original Phrase: "I'm a Mechanical Turk Worker."

Correct Answer: "I'm a Mechanical Turk Worker."

Low Depletion & Positive Mood Condition

The most important thing is to enjoy your life – to be happy – it is all that matters.
Be happy for this moment. This moment is your life. Enjoy it, feel it, because it is happening now.
You can't buy happiness but you can buy ice cream. And that is kind of the same thing.
There are so many beautiful reasons to be happy. Be you. Do you. For you.
I have only two kinds of days: happy and hysterically happy.
Life is short. Smile while you still have teeth.

Low Depletion & Negative Mood Condition

Life is sad. Pain and suffering are all around us.
No matter how hard you try, you'll often fail.
As you age, you will discover aches and pains that you never had before.
Life is hard. Then you die. Then they throw dirt in your face. Then the worms eat you.
Depression is like a heaviness you can't ever escape; it's in your bones and your blood.
I have only two kinds of days: sad and suicidal sad.
Life is short and death aims only once, but never misses.

⁴⁰ Participants who were randomly assigned to the negative mood condition were debriefed at the end with positive statements (i.e., the same statements used in the positive mood condition) to alleviate any potential risk that may arise from the negative mood manipulation.

Mood Manipulation Check (BMIS, Mayer and Gaschke 1988)

How do you feel after completing the writing task?

(1 Definitely do not feel ... 7 Definitely feel)

- 1- Lively
- 2- Peppy
- 3- Active
- 4- Happy
- 5- Loving
- 6- Caring
- 7- Drowsy
- 8- Tired
- 9- Nervous
- 10- Calm
- 11- Gloomy
- 12- Fed up
- 13- Sad
- 14- Jittery
- 15- Grouchy
- 16- Content

Depletion Manipulation Check (developed)

The writing task was:

- 1- *(1 Not at all difficult ... 7 Very difficult)*
- 2- *(1 Not at all challenging ... 7 Very challenging)*
- 3- *(1 Not at all taxing ... 7 Very taxing)*

Disclosure Behavior (developed)

Please respond to the following questions. Your payment will not be affected if you decide not to provide your information.

- 1- What is your year of birth?
[Answer: ____; I prefer not to provide this information]
- 2- What is your gender?
[Male; Female; Other; I prefer not to provide this information]
- 3- What is your ethnicity?
[White or Caucasian; Black or African American; Other; I prefer not to provide this information]
- 4- What is the domain for your main email account (hotmail.com, gmail.com, yahoo.com, etc.)?
[Answer: ____; I prefer not to provide this information]
- 5- What is the area code (first 3-digits) of your cell phone number?
[Answer: ____; I prefer not to provide this information]
- 6- Which state do you live in?
[Answer: ____; I prefer not to provide this information]
- 7- What is your zip code?
[Answer: ____; I prefer not to provide this information]
- 8- What is your yearly income?
[Answer: ____; I prefer not to provide this information]
- 9- What is the name of the bank with which you hold your main bank account?
[Answer: ____; I prefer not to provide this information]
- 10- How many bank accounts do you have?
[Answer: ____; I prefer not to provide this information]
- 11- How many credit cards do you have?
[Answer: ____; I prefer not to provide this information]

- 12- Describe your health status in a few words:
[Answer: _____; I prefer not to provide this information]
- 13- Describe your fitness level in a few words:
[Answer: _____; I prefer not to provide this information]
- 14- List any risky diseases you have:
[Answer: _____; I prefer not to provide this information]
- 15- What is your religion?
[Answer: _____; I prefer not to provide this information]
- 16- What is your political preference?
[Answer: _____; I prefer not to provide this information]
- 17- What is your sexual orientation?
[Answer: _____; I prefer not to provide this information]
- 18- How many siblings do you have?
[Answer: _____; I prefer not to provide this information]
- 19- Are you a parent?
[Yes; No; I prefer not to provide this information]
- 20- Are you married?
[Yes; No; I prefer not to provide this information]
- 21- Do you have a job other than MTurk?
[Yes; No; I prefer not to provide this information]

Falsification of Personal Information (developed)

How much of the personal information you provided was false?
[None; A little; A moderate amount; A lot; All]

Qualitative Feedback

If you decided not to provide any of the personal information we asked for, please tell us why:
Answer: _____

Privacy Concerns Scale (Dinev and Hart 2006) (1 Strongly disagree ... 5 Strongly agree)

For each of the following, please indicate how much you agree or disagree with the statement.

- 1- I am concerned that the personal information I submit to MTurk studies could be misused.
- 2- I am concerned that others can find private information about me from MTurk studies.
- 3- I am concerned about providing personal information to MTurk studies, because of what others might do with it.
- 4- I am concerned about providing personal information to MTurk studies, because it could be used in a way I did not foresee.

CHAPTER 4

Research Essay 3

Exploring Data Donations for Medical Research in the Face of Privacy Concerns

Abstract

It is only in the past few years that the medical community has recognized the promise of data donations, whereby individuals are encouraged to donate their data for medical research. Data donations could lead to a revolutionary change in advancing medical research. The change, however, will likely be hindered due to individuals' privacy concerns. We draw upon related research and recent privacy theories and distinguish between normative (i.e., privacy controls and ease of donation) and non-normative (i.e., empathic concern and social nudging) factors that can be leveraged by the medical community to increase data donations despite the presence of significant privacy concerns. We conducted two experiments using screen mockups of a mobile app designed for data donation. The findings indicated that the negative effect of privacy concerns on data donation can be mitigated by providing donors with granular privacy controls “and/or” inducing their empathic concern (experiment 1). With granular privacy controls being provided to donors and their empathic concern being induced, we also found that the negative effect of privacy concerns on data donation can be further mitigated by providing donors with an automatic data donation method “or” applying social nudging techniques (experiment 2). We discuss the theoretical, practical, and ethical implications of these findings.

Keywords: data donation, public health, privacy concerns, information disclosure, privacy paradox, health information technology, enhanced APCO, cognitive effort, elaboration likelihood model, experiment.

INTRODUCTION

Inspired by the idea of organ donation, the medical community is promoting data donation, whereby individuals are encouraged to donate their personal information for medical research (Shaw et al. 2015, 2016; Taylor and Mandl 2015; Topol 2015). This practice, which could promote healthcare innovation, is gaining traction and there are a number of initiatives in this area. Britain's National Health Service (NHS) project is one example of how large-scale data donations can advance medical research and chronic disease prevention.⁴¹ The NHS goal was to establish the world's biggest database for medical research (Topol 2015). According to a beneficiary of NHS who survived cancer twice, "I have seen firsthand how our health records can help improve people's lives. I might not be alive today if researchers had not been able to access the data in the health records of other cancer patients to produce the most effective treatments and the best care for me, and by making my own records available to researchers I know I am helping other patients in the future" (Topol 2015, p. 226). The NHS initiative succeeded in discovering new treatments by capitalizing on massive patient-based data accumulated in clinical settings.

Advocates for data donation, however, emphasize that not only clinical data but also broader health and lifestyle data are needed in order to advance medical knowledge. Data donation has been a subject of attention at medical conferences and webinars, and it has received media attention as well (Garber 2015; Lipset 2015; Payne 2017; Weintraub 2015).⁴² It was also mentioned in the precision medicine initiative announced by the Obama administration in 2015.⁴³ Advocates for data donation assert that the cumulative impact of data donations on public health and the health of future generations could be substantial (Mandl et al. 2015; Shaw et al. 2015, 2016; Taylor and Mandl 2015; Topol 2015).

Although little is known about the drivers and inhibitors of data donation decisions, a number of healthcare organizations have already pushed the concept into practice. For example, Open Humans, sponsored by multiple non-profit healthcare organizations, is a data donation project that was launched in

⁴¹ <https://www.england.nhs.uk/ourwork/tsd/care-data/>

⁴² <http://hdexplore.calit2.net/>

<http://andrewiggins.com/citizen-science-health-data-donation-health-data-exploration-project-2016/>

<http://www.academyhealth.org/blog/2017-04/how-communities-are-testing-new-strategies-address-social-determinants-health>

⁴³ <https://obamawhitehouse.archives.gov/the-press-office/2016/02/25/fact-sheet-obama-administration-announces-key-actions-accelerate>

2015.⁴⁴ OurDataHelps is a non-profit organization that has recently launched a data donation project sponsored by Qntfy, a provider of public health technologies.⁴⁵ While these two projects are still active and running, several other initiatives were either shut down (datadonors.org and donatehealthdata.com) or never completed (donateyourdata.info). It is unclear why some projects in this area have already failed, but one reason may have to do with individuals' concerns about information privacy especially as it relates to medical information. For example, the NHS initiative resulted in privacy concerns being voiced (Ashford 2016; Knapton 2016). Data donation advocates agree that such initiatives are infeasible unless privacy issues are addressed (Mandl et al. 2015; Mies 2013; Shaw et al. 2016; Taylor and Mandl 2015; Topol 2015). Such issues include individuals' privacy beliefs (i.e., privacy concerns), privacy systems and standards, and privacy regulations. To the best of our knowledge, neither Information Systems (IS) nor privacy scholars have explored this promising domain. The current study is the first to address privacy issues in this novel context.

The decision to donate data involves disclosure of a broad set of personal information (related to both health and non-health aspects), some of which may be highly sensitive information. From the donors' perspective, the perceived benefits of donating personal information are minimal as donors do not seek an immediate materialistic outcome, whereas potential privacy risks are substantial as anonymity of the donors' data is never guaranteed (Topol 2015). As a result, acting against one's own privacy preferences is essential for the success of this innovation (Taylor and Mandl 2015; Topol 2015). Given that health policymakers are highly interested in promoting data donations whereas individuals are highly interested in protecting their personal information, it is imperative to reconcile these opposing interests to enhance the sustainability of data donation projects. Our objective is to explore factors aimed at mitigating the negative effect of individuals' privacy concerns in order to improve the outcomes of data donation projects. The research question we address is:

RQ: *How can data donation organizations increase data donations despite the presence of significant privacy concerns?*

⁴⁴ <https://www.openhumans.org/>

⁴⁵ <https://ourdatahelps.org/> <https://qntfy.com/>

We draw upon the enhanced Antecedents – Privacy Concerns – Outcomes (APCO) model as our theoretical basis (Dinev et al. 2015). This model is grounded in behavioral economics principles (Acquisti et al. 2016; Kahneman 2011) and dual-process theories, such as the Elaboration Likelihood Model (ELM) (Petty and Briñol 2010; Petty and Cacioppo 1986). The enhanced APCO model proposes that non-normative factors (e.g., emotions and peripheral cues) play a significant role in privacy decisions (e.g., data donation). These factors influence the amount of cognitive effort individuals expend in processing relevant information. Prior empirical findings show that privacy concerned individuals are less willing to give out personal information (Li 2011; Smith et al. 2011; Yun et al. 2014), from which it can be inferred that higher privacy concerns will be associated with lower data donations. However, the enhanced APCO model suggests that this negative relationship could be weakened by inducing low-effort cognitive processing (through non-normative factors) under which individuals rely on judgmental heuristics rather than engaging in an effortful rational analysis of privacy decisions. There are many factors that could stimulate low-effort processing (Dinev et al. 2015). For instance, an aroused emotional state, a condition known to reduce cognitive processing (Bless et al. 1990; Schwarz and Clore 2007; Wegener and Petty 1994) could affect individuals' privacy decisions. In this study, we are interested in testing whether the negative effect of privacy concerns on data donation decisions could be weakened by inducing non-normative factors. Drawing on the enhanced APCO model and the theory of altruistic motivation, we focus on empathic concern and social nudging as two non-normative factors.

In contrast, normative factors can stimulate high-effort cognitive processing through which individuals deliberate and engage in an effortful analysis of privacy decisions. For instance, the level of privacy control and protection are among many other normative factors. Individuals use these factors to make informed privacy decisions (Dinev and Hart 2006). When individuals perceive low privacy control and protection, they feel at higher risk and become less willing to disclose information (Adjerid et al. 2018; Li et al. 2014). In contrast, when they perceive high control and protection, especially with a high level of convenience, individuals feel safe and are more willing to give out personal information. This

latter scenario is plausible even in the presence of high privacy concerns (Li and Slee 2014). Provided that individuals have enough cognitive capacity to engage in this mental process, they are more likely to make informed privacy decisions. In other words, during the disclosure decision process, individuals may prudently relax their privacy concerns when they perceive low privacy risk accompanied by privacy assurances particularly when they also perceive convenience in the decision process. In this study, we are interested in testing whether the negative effect of privacy concerns on data donation decisions could further be weakened by inducing normative factors that have the potential to stimulate informed privacy decision making. Building on the privacy and donation literatures, we focus on privacy controls and ease of donation as two normative factors.

Although recent research has shown that both non-normative and normative factors could directly affect privacy decisions (Adjerid et al. 2016; Adjerid et al. 2018), it is unknown how these two types of factors interact together to affect privacy decisions. Also, it is unknown how they can moderate the relationship between privacy concerns and privacy decisions. To address this theoretical gap and advance the knowledge in this domain, we develop a research model in which we predict a negative relationship between privacy concerns and data donation. Then, we explain how non-normative factors (i.e., empathic concern and social nudging) and normative factors (i.e., privacy controls and ease of donation) moderate the negative relationship between privacy concerns and data donation. We also theorize a three-way interaction between privacy concerns, non-normative factors, and normative factors. As we develop our hypotheses, we draw upon related research and theories to explain why certain non-normative (normative) factors could lead to uninformed (informed) data donation decisions. Then, we test the research model based on two experiments. Our findings indicate that the negative effect of privacy concerns on data donation can be mitigated by providing donors with granular privacy controls “and/or” inducing their empathic concern (experiment 1). With granular privacy controls being provided to donors and their empathic concern being induced, we also find that the negative effect of privacy concerns on data donation can be further mitigated by providing donors with an automatic convenient data donation method “or” applying social nudging techniques (experiment 2).

This study presents important theoretical and practical contributions. First, adoption of innovative healthcare information systems is markedly increasing (Topol 2015), but there are challenges ahead. For instance, while data donations could lead to a revolutionary change in detecting, predicting, and preventing chronic diseases and advancing medical research overall, the change will likely be hindered due to privacy issues at the individual level. Thus, we focus on privacy at the individual level where there is a dearth of research in the healthcare domain (Kohli and Tan 2016; Romanow et al. 2012). In so doing, we extend this nascent literature while providing practical implications to help improve the outcomes of data donation projects. Second, we distinguish between normative and non-normative factors and test their effect on privacy-related decisions. This allows us to empirically test a number of hypotheses derived from the recently proposed enhanced APCO model (Dinev et al. 2015).

Third, we extend recent research that emphasizes the role of both normative and non-normative factors in privacy-related decisions (Adjerid et al. 2018). In particular, we test the moderating effect of normative and non-normative factors on the relationship between privacy concerns and disclosure decisions. Thus, we provide insights for privacy theory by identifying some boundary conditions under which the relationship between privacy concerns and disclosure decisions might not hold (i.e., the privacy paradox).

Fourth, it is worth noting that previous privacy research in the context of healthcare has assumed implicitly or explicitly that individuals have a choice in allowing their health data to be digitized, stored, and shared (Electronic Health Records - EHR) but this is not a valid assumption. The reason is that the majority of healthcare organizations have to digitize patient records in order to comply with the federal mandate to adopt EHR (Adler-Milstein et al. 2015). As a result, individuals in real-world health settings may not have a choice to decline EHR opt-in requests. The context of our study is unique because individuals truly have the choice in allowing their personal data to be digitized, stored, and shared without any organizational pressure.

Finally, published privacy studies in the health domain have relied on disclosure intention measures (rather than disclosure behaviors or decisions) which have been shown as a critical limitation of the privacy literature (Smith et al. 2011). Our study addresses this limitation.

THEORETICAL BACKGROUND AND HYPOTHESES

In this section, we provide an overview of the privacy literature followed by a focused review of empirical privacy studies in the health domain given their relevance to our study. Across various contexts including health, several studies have observed a negative effect of privacy concerns on disclosure-related outcomes (e.g., willingness or intention to disclose, EHR opt-in intentions, self-report of past disclosure behaviors, or actual disclosure behaviors). However, we are not aware of any study that has tested the effect of privacy concerns on data donation, a disclosure-related behavioral outcome. Thus, our first hypothesis replicates previous findings in this novel context. That is, individuals who have higher privacy concerns are less likely to donate their data. Before developing our new hypotheses, we provide a theoretical discussion of the enhanced APCO model to describe how normative and non-normative factors affect privacy-related decisions.

Privacy Concerns and Disclosure of Personal Information

Information privacy reflects users' control over their personal information (Solove 2006; Westin 2003), and privacy concerns reflect the loss of information privacy (Smith et al. 1996). The construct of privacy concerns has been defined in different ways (Dinev and Hart 2006; Hong and Thong 2013; Malhotra et al. 2004; Smith et al. 1996). It has also been studied by scholars from different fields, such as Behavioral Economics, Communication, IS, and Marketing (e.g., Acquisti et al. 2016; Debatin et al. 2009; Smith et al. 2011; Tucker 2014). Privacy concerns refer to individuals' disposition to worry about how their personal information is collected, used, protected, and shared by organizations (Li et al. 2011; Smith et al. 1996).

Privacy concerns have been documented repeatedly in public polls and published research (Acquisti and Gross 2006; Choi et al. 2015; Rainie et al. 2013). These concerns have been shown to be affected by several antecedents (e.g., personality traits, privacy awareness, Internet experience, self-

efficacy, social norms, culture, and demographics) and to affect several attitudes and behavioral outcomes (e.g., risk and trust beliefs, privacy-protective responses, and disclosure intentions and behaviors) (for reviews, see Li 2011; Li 2012; Smith et al. 2011). The relationship between privacy concerns and outcomes is also contingent on affective, cognitive, heuristic, and contextual factors (Acquisti et al. 2016; Anderson and Agarwal 2011; Kehr et al. 2015; Mothersbaugh et al. 2012; Wakefield 2013).

Despite the wide-ranging nature of this literature and the various theories adopted, it can be reasonably inferred that privacy concerns have a negative effect on disclosure of personal information. For instance, Internet users tend to provide incomplete information, request removal of their information, and avoid registering for websites because of their privacy concerns (Sheehan and Hoy 1999). Users tend to refuse to provide personal information to online companies and are more willing to remove their personal information from online companies' databases because of privacy concerns (Son and Kim 2008). In online social environments, concerned users disclose less information to others and provide false personal information (Alashoor et al. 2017; Jiang et al. 2013). Several other studies have shown similar results (e.g., Breward et al. 2017; Dinev and Hart 2006; Miltgen and Peyrat-Guillard 2014).

Disclosure behaviors represent a very important organizational success factor. Data donation in our context reflects a disclosure behavior in which donors provide access to their personal data for medical research. Indeed, the medical community cannot realize the goals of data donation projects unless individuals are willing to provide access to their personal information. However, individuals' privacy concerns can be much more influential in this context because donating data involves highly sensitive personal information, such as health data (Bansal et al. 2016; Chhanabhai and Holt 2007).

Health Information Privacy Concerns

Although it is difficult to prove the potential harm to privacy, when personal information is compromised or inappropriately exploited, the probability of putting individuals at risk is quite high (Agarwal et al. 2010). For example, a privacy exposure incident of one's health data could increase the risk of raising their health insurance costs (Maddox 2015). The risk becomes more detrimental when exposures reach the hands of potential employers (Libert 2015). Because health data represents one of the most sensitive

types of personal information, individuals are likely to be highly concerned about how their health information is used, processed, and shared by healthcare and non-healthcare entities (Libert 2015; Westin 2005). These concerns will affect individuals' willingness to have their health data digitized and accessed by health entities.

A number of empirical studies have shown evidence of the negative effect of privacy concerns on health information disclosures (Bansal et al. 2016; Fox and Connolly 2018; Li et al. 2014). For instance, Bansal et al. (2016) argued for the contextual nature of privacy behaviors and tested a research model across three different contexts (i.e., e-commerce, financial, and health websites). Their findings showed that the context sensitivity and individuals' salient attributes (i.e., privacy concerns) are critical factors influencing the willingness to give access to personal information. As predicted, Bansal et al. (2016) found a negative relationship between privacy concerns and intention to disclose information across the three contexts; however, the effect size of this relationship is larger in the health context. Kuo et al. (2014) tested relationships between the sub-dimensions of privacy concerns, i.e. collection, unauthorized access, secondary use, and errors (Smith et al., 1996), and privacy-protective responses (e.g., requesting removal of personal information from EHR systems). Based on a random sample of patients drawn from a medical center in Taiwan, Kuo et al. (2015) found a positive relationship between collection, secondary use, and errors concerns and intentions to pursue privacy-protective responses. Li et al. (2014) provided additional evidence of the negative effect of privacy concerns on intentions to adopt standalone personal health record systems. Leveraging this literature to the context of data donation, we predict the following:

Hypothesis 1 (H1): *Individuals with high levels of privacy concerns will be less likely to donate data.*

Testing H1 will present empirical evidence of the main effect of privacy concerns on data donation decisions. However, as we discussed in the introduction, we are interested in testing conditions that may weaken this relationship. There is limited literature that investigated conditional factors in the health domain, from which we draw some theoretical implications. For instance, Angst and Agarwal (2009) used the ELM to examine attitude change and the likelihood of opting-in to an EHR system. Their

findings showed that a positive framing of the EHR program elicits positive attitudes toward digitizing personal health information (PHI) and contributes to minimizing the negative effect of privacy concerns. Li and Slee (2014) corroborated the significant effect of positive attitudes toward EHR and found a positive relationship between attitude toward EHR and EHR opt-in intentions. Anderson and Agarwal (2011) showed that privacy concerns are negatively associated with willingness to provide access to PHI. However, the effect of privacy concerns was contingent on factors like intended purpose (e.g., patient care, research, and marketing) and the entity requesting access to PHI (e.g., hospitals, governments, and pharmaceutical companies).

These findings contribute to identifying boundary conditions for the relationship between privacy concerns and health information disclosures. For example, to bypass individuals' negative privacy concerns, policymakers, governments, and healthcare providers could use positive frames and articulate the intended purpose when seeking consent to digitize individuals' health information. While these practical implications are worth implementing, the inferences made from this literature were all based on outcomes that reflect intentions rather than actual disclosure decisions. It may be that while participants of the above studies indicated less willingness to digitize or give access to PHI because of privacy concerns, their actual decisions could be inconsistent with their stated concerns or intentions. Evidence for this privacy paradox has been widely acknowledged in the literature (Acquisti et al. 2016; Smith et al. 2011). Moreover, this literature is built on an implicit assumption that individuals have a choice in opting-in to EHR or allowing their health data to be digitized. Yet, the reality is that the majority of healthcare providers are required to digitize individuals' PHI (Adler-Milstein et al. 2015) and hence, individuals have little to no influence on the collection and digitization of their health information. Additionally, the current literature provides little guidance on how non-normative factors (e.g., emotions and peripheral cues) can influence decisions to disclose health data. In the presence of such non-normative factors, it is also unclear how individuals assess normative factors (e.g., privacy controls) when deciding to provide health data. Next, we discuss the enhanced APCO model and present a research model that considers two normative and two non-normative factors and their individual and joint moderating effect on the

relationship between privacy concerns and data donation decisions. *Data donation* is a disclosure behavioral outcome in which individuals decide whether or not to provide their personal data for medical research.

The Enhanced Antecedents – Privacy Concerns – Outcomes (APCO) Model

The IS privacy literature is largely based on theories that assume individuals as rational agents (for review, see Smith et al.'s (2011) original APCO model).⁴⁶ However, recent publications showing discrepancies in privacy decisions have led scholars to reconsider this assumption (for reviews, see Barth and de Jong 2017; Kokolakis 2017). Grounded on the ELM (Petty and Briñol 2010; Petty and Cacioppo 1986) and principles from behavioral economics (Acquisti et al. 2016; Kahneman 2011), Dinev et al. (2015) synthesized the current knowledge on privacy and proposed enhancements to Smith et al.'s (2011) original APCO model. The enhanced APCO model offers a set of propositions that explain why individuals' behavioral reactions (e.g., information disclosure) might not be consistent with their privacy preferences. It suggests that privacy decisions are highly conditional on the amount of cognitive effort expended. For example, experiencing intense emotional states can induce lower effort processing, which in turn can lead individuals to make disclosure decisions that are inconsistent with their dispositional privacy concerns. This is consistent with the ELM which explains decision-making based on two routes of information processing: central and peripheral. The central route involves a thoughtful judgment of the available information during the decision-making process, whereas the peripheral route involves reliance on simple heuristics and little attention to the merits of the available information. Dinev et al. (2015) refer to the former as “high-effort” and the latter as “low-effort” cognitive processing.

In order to engage in a high-effort cognitive processing, individuals must have the ability and motivation to process relevant information (Petty and Briñol 2010). Relevant information represents normative factors that individuals use to make informed decisions. In privacy-related decisions, the level of privacy risk involved that can be assessed by the privacy assurances afforded (e.g., privacy controls) or the level of convenience afforded in a privacy-related context (e.g., ease of donation) are examples of

⁴⁶ Some exceptions include Adjerid et al. (2018), Bansal et al. (2015), and Lowry et al. (2012).

normative factors. Individuals are more likely to elaborate on the utility of such factors when they are able to perceive their merits. Thus, applying high-effort cognitive processes involves thoughtful information processing of relevant normative factors.

However, individuals can be easily influenced by irrelevant non-normative factors such as website quality and brand image (Lowry et al. 2012), or when their cognitive processing is disturbed by intense emotions or diverted by social nudges (Acquisti et al. 2017; Dinev et al. 2015). Such non-normative factors can significantly reduce the ability and/or motivation to scrutinize one’s own privacy preferences (Dinev et al. 2015). Therefore, to the extent that individuals are low on either ability or motivation, they will not engage in high-effort processing when making privacy decisions. Disclosure decisions may therefore be more strongly guided by low-effort processing in the presence of disruptive non-normative factors that should not theoretically influence the disclosure decision being made.

In each of the two experiments (to be described), we induce one normative and one non-normative factor and test their individual and joint effect on data donation decisions. Next, we develop hypotheses related to the moderating effect of each normative (i.e., privacy controls and ease of donation) and non-normative (i.e., empathic concern and social nudging) factor on the relationship between privacy concerns and data donation decisions (H1). We posit that these factors can moderate the negative effect of privacy concerns on data donation. Figure 1 depicts our research model.

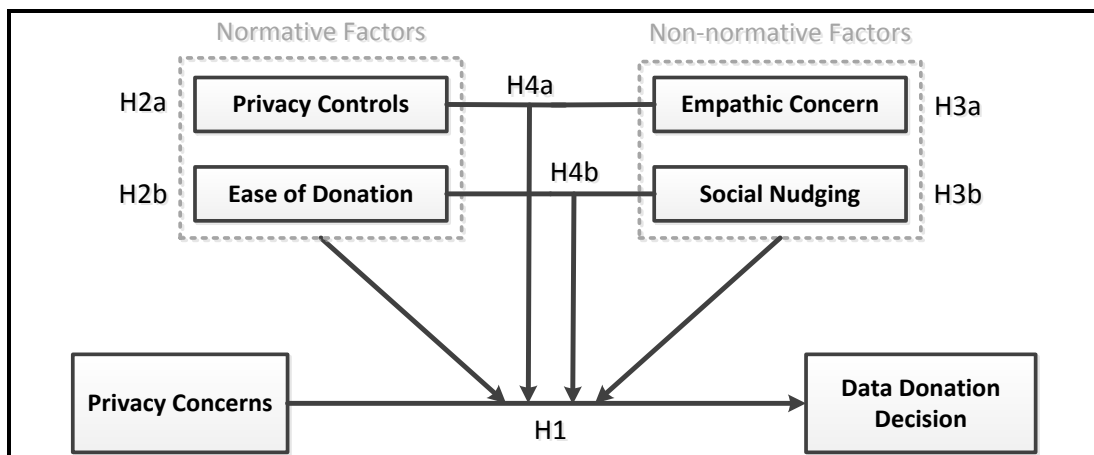


Figure 1. Research Model

Normative Factor 1: Empowering Donors through Privacy Controls

Empowering individuals is a significant predictor of various performance outcomes (Conger and Kanungo 1988; Deng et al. 2016). The IS literature emphasizes the importance of empowering consumers in order to achieve maximal benefits of information technologies (Lucas et al. 2013). For example, users of an e-commerce website are empowered when they are able to make orders, check the status of orders, send a claim, and resolve many service problems without the need to contact customer service. Lucas et al. (2013) also suggest that healthcare organizations could benefit from empowering patients by changing the locus of control from the doctor to the patient via social media.

In the context of data donation, we propose that empowerment can be achieved by providing individuals with privacy controls. The ability to control personal information is a key component of information privacy (Solove 2006; Westin 2003) and the majority of privacy research has used the control aspect to define privacy concerns (Hong and Thong 2013; Malhotra et al. 2004; Smith et al. 1996). The literature also shows consistent evidence for the significant effect of the control construct in contexts like e-commerce and social media (Alashoor et al. 2017; Brandimarte et al. 2013; Cavusoglu et al. 2016; Dinev and Hart 2006). Similarly, findings from privacy studies in the health domain and those from health informatics contend that individuals want to have control over their health data, and perceptions of low control aggravate perceptions of privacy risks (Li et al. 2014; Willison et al. 2009).

Thus, it is probable that the more control individuals have, the more likely they are to make data donations. However, this control needs to be tangible and easily accessible through technology (e.g., mobile apps). In particular, individuals need not only promises of control in a written or online document (e.g., privacy statement), but they also need to exercise this control and feel its power. Data donation organizations can achieve this goal by allowing individuals to opt-out from the donation program completely and to monitor and control who can have access to and share their donated data. Empowering donors via these privacy controls can be seen as a way of building trust with them before they make donation decisions. It is also a way to emphasize transparency in handling donors' data. Prior research found that privacy concerned individuals are more willing to opt-in to EHR when they perceive high

privacy control based on a privacy statement (Li and Slee 2014). Individuals also tend to perceive low privacy risks when they perceive high, although illusory, control over their data (Brandimarte et al. 2013). Thus, we predict that empowering donors through privacy controls will relax the negative effect of privacy concerns and hence individuals will be more likely to make data donations. In other words, the negative effect of privacy concerns on data donation (H1) will be attenuated when individuals have effective, transparent, and easily accessible privacy controls.

Hypothesis 2a (H2a): *The negative relationship between privacy concerns and data donation will be weaker (stronger) when privacy controls are provided (not provided) to donors.*

Non-Normative Factor 1: Motivating Donors' Altruism through Empathic Concern

Altruism is “a desire to benefit someone else for his or her sake rather than one’s own” (Batson 2011, p. 3). There are two main sources of altruistic motivation: altruistic personality and empathic concern (Batson 2011; Batson et al. 2009). The theory of altruistic motivation explains altruism through empathic concern. It posits that “feeling other-oriented emotion elicited by and congruent with the perceived welfare of another person in need (i.e. empathic concern) produces a motivational state with the ultimate goal of increasing that person’s welfare by having the empathy-inducing need removed (i.e. altruistic motivation)” (Batson 2011, p. 29). This is the empathy-altruism hypothesis in which a motivational state with the ultimate goal of increasing another’s welfare takes place if an individual imagines a desirable change in the other person’s world and experiences a force to make some change as an end in itself (Batson 2011). In a series of experiments, Batson and colleagues have shown strong support for the empathy-altruism hypothesis by ruling out alternative explanations, such as helping the other for egoistic motivation and reward seeking (for review, see Batson 2011). When empathic concern is induced, individuals tend to be motivated to help the person in need from a purely altruistic motivation. We adapt the empathy-altruism hypothesis to our context which involves helping more than one person, such as patients and research communities, by donating personal data. We propose that inducing people’s empathic concern for patients suffering from incurable diseases can help to increase data donations.

Cognitive psychology research suggests that aroused emotional states are associated with less effortful analysis of relevant information, consistent with the predictions of the enhanced APCO model (Dinev et al. 2015). When emotional states are aroused, individuals exhibit lower ability and motivation to make effortful analysis of the decision being made (Bless et al. 1990; Schwarz and Clore 2007; Wegener and Petty 1994). As a result, individuals' data donation decisions may become highly driven by non-normative factors, such as feelings of empathic concern. Both cognitive psychology research and the theory of altruistic motivation suggest that decision-making under aroused emotional states will be driven by a peripheral rather than a central route.

Empirical privacy research also provides evidence for the significant effect of emotions (e.g., Anderson and Agarwal 2011; John et al. 2011; Kehr et al. 2015). For instance, Anderson and Agarwal (2011) found that sad feelings about health status and altruistic personality are associated with higher willingness to provide access to health information. However, it is not clear whether or not altruism induced by empathic concern will increase data donations for research purposes. The donation literature further contends that emotional factors (e.g., empathic concern, perspective taking, and personal distress) are positive predictors of organ and blood donation decisions (Kim and Kou 2014; Piersma et al. 2017). While these studies present evidence for the positive effect of empathic concern on donation decisions, it is not clear how empathic concern affects privacy-related donation decisions. We predict a moderating effect of empathic concern on the negative relationship between privacy concerns and data donation. In particular, empathic concern will weaken this relationship because inducing empathic concern will motivate both altruism (Batson 2011) and low-effort cognitive processing (Dinev et al. 2015), making individuals less likely to act on their privacy concerns.

Hypothesis 3a (H3a): *The negative relationship between privacy concerns and data donation will be weaker (stronger) when donors' empathic concern is induced (not induced).*

Privacy Concerns, Privacy Controls, and Empathic Concern: A Three-Way Interaction

We also predict a three-way interaction between privacy concerns, privacy controls, and empathic concern. In particular, privacy concerns will be more predictive of data donation in the *absence* of both a

facilitating normative factor (i.e., privacy controls) and a disruptive non-normative factor (i.e., empathic concern). For instance, when privacy controls are not provided and empathic concern is not induced, individuals are likely to act on their dispositional privacy concerns. The rationale is that dispositional privacy concerns, absent other factors, become the reference point based on which individuals make their privacy decisions. As a result, and consistent with H1, those who have high privacy concerns are unlikely to donate data. However, when privacy controls and/or empathic concern are in effect, individuals are less likely to base their data donation decisions on dispositional privacy concerns because they will either perceive a high level of privacy control in a rational manner (i.e., central route) or be disturbed by feelings of empathic concern (i.e., peripheral route).

Hypothesis 4a (H4a): *There will be a three-way interaction between privacy concerns, privacy controls, and empathic concern, such that privacy concerns will be more (less) predictive of data donation in the absence of both (presence of either) privacy controls and (or) empathic concern.*

Normative Factor 2: Facilitating Donors through Ease of Donation

Drawing upon the donation literature, we consider ease of donation as another normative factor that could be leveraged to facilitate data donors. Ease of donation is a key determinant for blood and organ donation intentions and behaviors (for review, see Beurel et al. 2017; Feeley and Moon 2009; Masser et al. 2008; Piersma et al. 2017). It reflects perceptions of convenience associated with the donation process (Schreiber et al. 2006). When individuals find the donation process to be convenient, they are more willing to make blood, organ, and tumor tissue donations (Godin et al. 2007; Hyde and White 2009; Schreiber et al. 2006; Suárez et al. 2004). However, in the presence of physical and time constraints (e.g., distance to donation site, time commitment, and the length of and effort involved in the donation process), individuals find it difficult to donate. The theoretical rationale that ease of donation is a significant factor affecting intentions and behaviors stems from its effect on increasing perceived behavioral control and self-efficacy (Giles et al. 2004; Masser et al. 2008). In other words, if individuals find the donation process easy and convenient, they are more likely to believe they have the ability and confidence to donate. As such, ease of donation is a normative factor that individuals consider rationally when deciding to make blood and organ donations (Godin et al. 2007; Suárez et al. 2004). The donation literature

suggests a number of interventions (e.g., mobile collections and extra hours of operations) to help make it easier for individuals to donate (Godin et al. 2007; Masser et al. 2008; Schreiber et al. 2006; Van Dongen 2015).

In the context of data donation, effective and efficient interventions can be simply achieved through information technologies. Donating data often requires individuals to manually enter their personal information. Yet, individuals might be reluctant to expend effort and time, as observed in blood donations (Sojka and Sojka 2003). The amount of cognitive effort and time required to recall and enter the data manually would be an inhibiting factor for individuals who are willing to donate their personal data. We propose that ease of donation can be achieved by providing donors with technology features that are able to capture personal data automatically. Mobile apps are well suited for such an intervention. In particular, the mobile context can make it easy for individuals to donate by allowing the donation app to automatically capture data from other apps, such as default health apps, Fitbit, Facebook, Twitter, etc. Automatic capturing of data from other apps will obviate the need to manually enter the data, thereby saving time and making the donation process effortless.

We predict that such a feature will increase data donations in general. However, it is important to consider dispositions of potential donors before applying donation interventions, as suggested by Feeley and Moon (2009). In our context, imposing automatic capturing of personal data could have a positive effect, even in the presence of privacy concerns, as individuals are willing to give up privacy for convenience (Acquisti and Grossklags 2005). However, automatic capturing could also backfire because individuals could perceive this feature in a different way (e.g., automatic capturing will reduce control over the donation method⁴⁷ and hence aggravate potential privacy risks). This situation is akin to that of the personalization privacy paradox where individuals value the convenience associated with online services (e.g., personalized ads), but they also value the transparency associated with organizational privacy practices (Awad and Krishnan 2006). Thus, while an automatic donation method provides

⁴⁷ Control over the donation method is different from control over the donated data (which is afforded via privacy controls). The former refers to individuals' control over the method with which their data can be donated (e.g., manual or automatic method) while the latter refers to individuals' control over the donated data (e.g., who can access and share the donated data).

convenience and hence individuals are more likely to relax their privacy concerns in a rational manner before making a donation decision, it is also possible that individuals, especially privacy fundamentalists⁴⁸, would perceive a low level of control over the donation method as the app could have access to data beyond the intended donation purpose. In order to account for this possibility, we consider donors' perceived control over the donation method and partial its effect out from the construct of ease of donation.⁴⁹

Overall, we predict that an automatic donation method (where donors simply select the data they would like to donate, which takes just a few seconds, and the donation app captures the selected data from other apps) will weaken H1 as the majority of individuals are privacy pragmatists⁵⁰ who are likely to weigh convenience over potential privacy risks (Quint and Rogers 2015). In a manual donation method, however, donors are more likely to base their donation decisions on dispositional privacy concerns due to the inconvenient method afforded as they will have to enter the data manually, an effortful and time-consuming process. Thus, we argue that in the presence of privacy concerns, data donation outcomes can be improved by applying an automatic donation method.

Hypothesis 2b (H2b): *The negative relationship between privacy concerns and data donation will be weaker (stronger) when the donation method is automatic (manual).*

Non-Normative Factor 2: Herding Donors through Social Nudging

Nudging is another non-normative factor that can be used to increase data donations. Nudging is a behavioral economic concept introduced by Thaler and Sunstein (2008). A nudge refers to any aspect of the choice architecture aimed at influencing individuals in a predictable way through easy and cheap-to-run interventions without limiting individuals' choices or significantly changing their economic incentives (Thaler and Sunstein 2008). Nudging has been shown to influence individuals' decisions in various contexts. For example, simple and nonintrusive nudges (e.g., a small sign that encourages restaurant buffet customers to help themselves more than once) were found to reduce food waste by 20%

⁴⁸ Privacy fundamentalists are those who express extreme concerns for privacy and are generally unwilling to provide personal information even in the existence of privacy-protective measures (Ackerman et al. 1999).

⁴⁹ We do not state a hypothesis for the effect of perceived control over the donation method, but we account for it in the statistical model.

⁵⁰ Privacy pragmatists are those who express concerns for privacy but are willing to provide personal information in the presence of privacy protective measures (Ackerman et al. 1999).

(Kallbekken and Sælen 2013). Making salad rather than chips as the default side order in restaurant menus is another nudge to encourage a healthy diet (Marteau et al. 2011). Nudging smokers to stand a few meters away from buildings reduced smoking rates significantly (Eyal 2014). In the donation literature, studies have examined the effect of nudges, and findings indicate that nudges can enhance donation outcomes (Lee et al. 2017; Goswami and Urminsky 2016). In the current study, we apply social nudging which refers to positive reinforcement aimed at influencing individuals' donation decisions based on the group they belong to.

Acquisti et al. (2017) discuss how social nudges can influence privacy decisions (p. 17). The enhanced APCO model also suggests that privacy decisions are likely to be influenced by the herding effect, a nudging-related concept, which refers to individuals following established social norms that “everyone is doing it too” (Cialdini 2009; Dinev et al. 2015). The ELM theoretical explanation for this phenomenon is that simple cues will significantly influence individuals' information processing. More specifically, individuals are less likely to employ an effortful analysis because their cognitive ability and/or motivation to assess the privacy risks involved are distracted by the presence of the social nudge. As a result, the decision-making process is guided through a peripheral rather than a central route.

We predict that the presence of a social nudge can moderate the relationship between privacy concerns and data donation because individuals are more likely to employ low-effort cognitive processing as they are influenced by others' donation decisions. We propose two modes of social nudging: high and low. A high (low) social nudge reflects that a large majority (only a minority) of in-group people have made data donations. The high social nudge, according to the herding effect, will likely lead individuals to follow the herd and donate. In contrast, the low social nudge could lead to reduced donations, “not everyone is doing it; therefore, I should not do it.” We expect the high (low) social nudge to attenuate (strengthen) the negative effect of privacy concerns on data donation decisions because individuals' decisions can be driven by this peripheral cue rather than processing their own privacy preferences.

Hypothesis 2b (H2b): *The negative relationship between privacy concerns and data donation will be weaker (stronger) in the presence of a high (low) social nudge.*

Privacy Concerns, Ease of Donation, and Social Nudging: A Three-Way Interaction

Last, we predict a three-way interaction between privacy concerns, ease of donation, and social nudging. In particular, when manual entry of the donation is required especially in the presence of a low nudge, individuals' mindset can be easily directed toward their dispositional privacy beliefs. In such a condition (i.e., manual donation method and low social nudge), privacy concerns will be more predictive of donation decisions. In other words, the donation decision process is driven by the notion that donating data is an effortful and time-consuming process and only a limited number of people are doing it. As a result, donors with high privacy concerns are less likely to donate their data. The rationale is that dispositional privacy concerns, absent a facilitating factor (i.e., automatic donation method) or a peripheral encouraging cue (i.e., high social nudge), become the reference point based on which individuals make their donation decisions.

In contrast, when donors find convenience in the donation process, even with a discouraging social nudge, there is less likelihood that they will engage in processing their privacy preferences. In this condition (i.e., automatic donation method and low social nudge), the donation decision process is driven by the notion that while not everyone is doing it, prosocial behaviors are needed especially given the donation process is easy with the automatic donation method. As a result, privacy concerns will be less predictive of donation decisions. Similarly, in the presence of an encouraging social nudge, even with an effortful and time-consuming donation process, there is less likelihood that donors will engage with their privacy preferences and instead they will be directed by the encouraging peripheral cue. Therefore, in this condition (i.e., manual donation method and high social nudge), privacy concerns will be less predictive of donation decisions because donors' processing of privacy beliefs is distracted by the encouraging social nudge. Finally, in the presence of an easy donation method coupled with an encouraging social nudge, we predict donors to be even less likely to engage in an effortful analysis of their privacy concerns. The rationale is that donors will process their donation decision based on the convenience associated with the donation process while being diverted by the high social nudge which signifies that

the majority of people are donating their data. Thus, in this condition (i.e., automatic donation method and high social nudge), privacy concerns will be even less predictive of donation decisions.

Hypothesis 4b (H4b): *There will be a three-way interaction between privacy concerns, ease of donation, and social nudging, such that privacy concerns will be more (less) predictive of data donation in the absence of both (presence of either) an automatic donation method and (or) a high social nudge.*

METHOD

Mandl et al. (2015) and Topol (2015) call for innovative health apps that allow healthcare personnel easy access to personal health and non-health data. They suggest that mobile-based apps are needed to enhance the utilization of available medical research data. In line with this emphasis, we designed an experimental data donation app. Our app is named after a real donation project (i.e., datadonors). Using the experimental app, we manipulated one normative and one non-normative factor in each of the two experiments. In both experiments, we measured privacy concerns, data donation, and a number of control variables (i.e., trust, mood, altruistic personality, media exposure of health data misuse, privacy invasion experience, frequency of doctor visits, health status, age, gender, and ethnicity) as research showed their significant effect on disclosure-related outcomes (Anderson and Agarwal 2011; Dinev and Hart 2006; Malhotra et al. 2004; Yun et al. 2014).

In experiment 1, we examined privacy controls (normative factor 1) and empathic concern (non-normative factor 1). Experiment 1's design was a 2 (privacy controls: provided vs. not provided) X 2 (empathic concern: induced vs. not induced) between-subjects full factorial design. Thus, experiment 1 provides a test for H1, H2a, H3a, and H4a. In experiment 2, we held privacy controls and empathic concern constant, such that privacy controls were provided and empathic concern was induced for all participants. In experiment 2, we tested ease of donation (normative factor 2) and social nudging (non-normative factor 2) using a 2 (ease of donation: automatic vs. manual) X 2 (social nudging: high vs. low) between-subjects full factorial design. Thus, experiment 2 replicates H1 and tests H2b, H3b, and H4b.

This experimental approach is cumulative, such that experiment 2 builds on experiment 1 in a way to maximize donation outcomes. For both experiments, we collected data using Amazon Mechanical Turk.⁵¹

EXPERIMENT 1

Sample and Procedure

The sample included 139 participants: mean age = 33.7 years; female = 49.3%; White = 66.9%. The experiment involved screen mockups of the experimental *datadonors* app through which participants viewed several screenshots of the app. After being introduced to the app and its features (in which we manipulated privacy controls and empathic concern), participants were then asked to select the data they would like to donate (23 items, adapted from the original *datadonors* project, constituted our measure for data donation). Participants were asked to select the data they wanted to donate: 1) Demographic Data [*gender, birthdate, ethnicity, education, work experience, and sexual orientation*], 2) Basic Health Data [*height, weight, blood type, vaccination, and sleep*], 3) Medical History Data [*benign chronic diseases, risky chronic diseases, family health history, drug use, surgeries, and allergies*], and 4) Lifestyle Data [*drinking, smoking, exercise, social media use, diet, and emotions*]. Next, participants were asked to provide qualitative feedback about their donation decisions followed by scales for dispositional privacy concerns (Dinev and Hart 2006), trust (Moody et al. 2017), mood (Dickert et al. 2011), altruistic personality, media exposure of health data misuse, privacy invasion experience, frequency of doctor visits, and health status (Anderson and Agarwal 2011). Participants were asked for feedback about the study after they were debriefed at the end.

Because our goal was not to actually collect data donations, participants were led to believe that they would be asked to provide the data after they made their data donation selections. This procedure was used to provide a suitable proxy for actual behaviors and to avoid simply measuring intentions to donate. The feedback we received from the vast majority of the participants confirms the validity of this

⁵¹ In both experiments, the title of the study was “Mobile Design and Decision Making.” In the consent form, participants were told that they will be asked to evaluate a mobile app designed for a data donation organization. They were also informed that they will be asked to make a data donation decision. The study was approved by the Institutional Review Board (IRB). Participants received \$1.50 (experiment 1) and \$2.00 (experiment 2) for participation. Participants who failed the two attention checks, spent extremely little time, or appeared to be bots (according to the qualitative feedback they provided for three open-ended questions) were excluded from the final analysis. A total of 8% (experiment 1) and 10% (experiment 2) of subjects were excluded for failing at least one of the exclusion criteria.

proxy as most participants took the scenario seriously and went through the kind of thought processes that one would only go through if they were providing an actual data donation. Below are a few examples reflecting that participants acted as if they were making actual donation decisions:

- *“I didn't want to go through the processing.”*
- *“I didn't donate my blood type because I do not know it.”*
- *“I am a private person and don't like to give out too much information.”*
- *“I chose to donate most of the data wanted, except for the few that I cannot prove because I simply do not know.”*
- *“I think that it will be beneficial and besides I have control over the privacy settings anyway.”*

Manipulations and Measurements

We manipulated privacy controls, such that participants were randomly assigned to view a version of the app in which granular privacy settings were provided (treatment group) or not provided (control group) (Figure 2, Panel A).⁵² We manipulated empathic concern by using different images in the home screen of the app. The empathy literature provides various methods for inducing empathic concern (see Eisenberg and Miller 1987). We chose to induce empathic concern via images because this method is the most realistic one that can be easily adopted in actual donation apps. Other methods (e.g., story, misattribution, and videos) could be difficult or even impossible to implement in an actual app. Participants were randomly assigned to view the app with the home screen depicting images of cancer and Alzheimer's patients (treatment group) or images of oceans (control group) (Figure 2, Panel B).⁵³

⁵² In the privacy controls treatment condition (Panel A), the app shows that users can 1) select/unselect who can access their data, 2) select/unselect who can share their data, 3) request approval before any organization can use their data, and 4) retract their donations. The five screens in Panel A were presented one by one using a much larger size and clarity than they appear in Figure 2.

⁵³ The reason for using two images in the home screen is to make sure that we induce empathic concern successfully as one image might not result in sufficient empathic concern. Participants, in both the treatment and control groups, were told that the actual app displays each image for 5 seconds in a dynamic fashion and therefore they were asked to view each image for 5 seconds, after which they were asked to respond to the empathy concern scale (Batson 2011) to provide their opinion about these screens. However, the main purpose of this scale was to serve as a manipulation check.

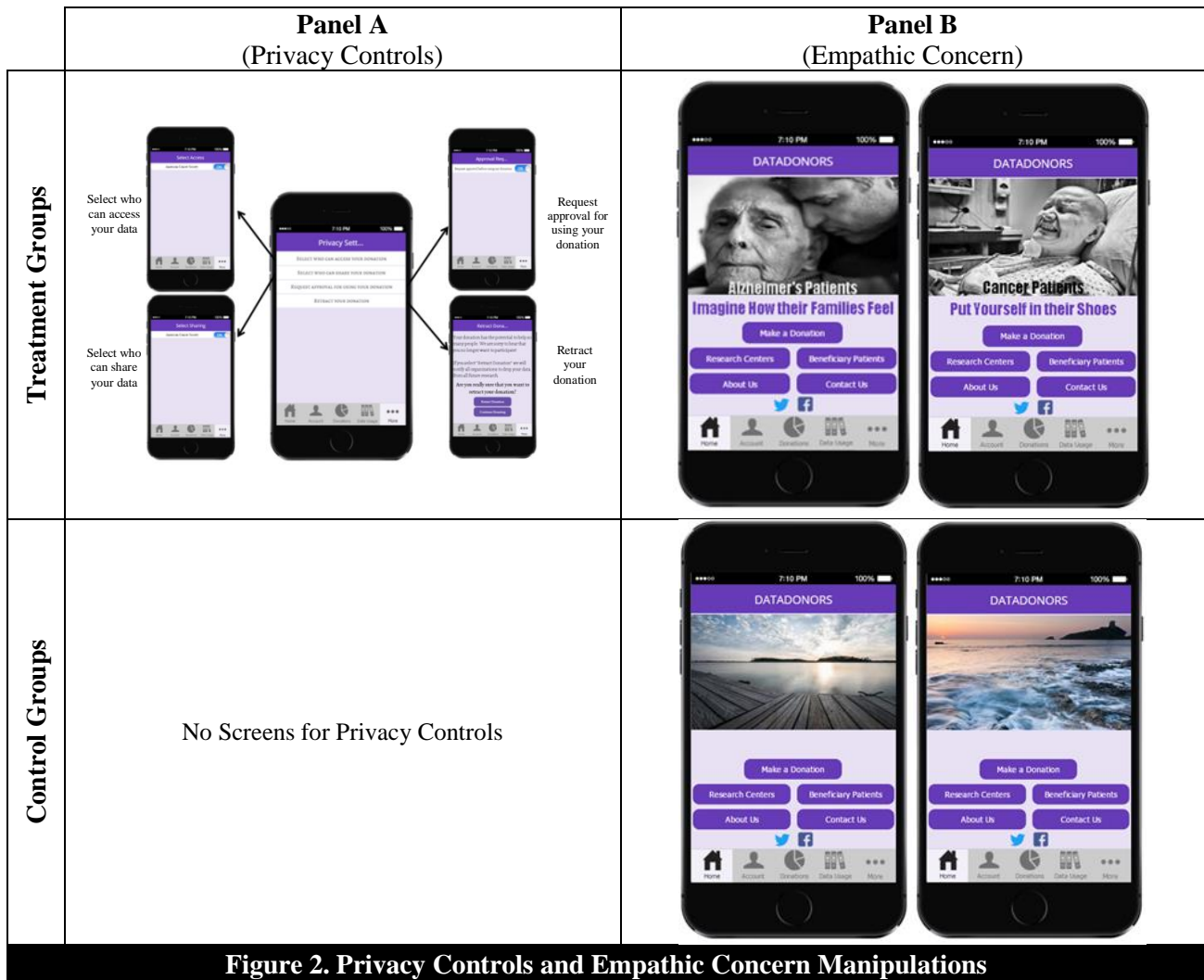


Figure 2. Privacy Controls and Empathic Concern Manipulations

Five items [e.g., “I will have control over who can access my donated data; I will be able to retract my donation” (7-point Likert scale)] (Cronbach’s $\alpha = .93$) were used as a manipulation check for privacy controls (Li et al. 2014). Eleven items [e.g., “moved; softhearted; sorrowed; touched; empathic...” (1 Not at all ... 9 Very much)] (Cronbach’s $\alpha = .97$) were used as a manipulation check for empathic concern (Batson 2011). To test whether the manipulations were successful, we used *t*-tests. The results indicated that both manipulations were successful. With regard to privacy controls, the *t*-test indicated a significant mean difference ($t(137) = -7.97; p < .001$) between the treatment group ($n = 68$; $mean = 5.49$; $s.e. = .15$) and the control group ($n = 71$; $mean = 3.52$; $s.e. = .18$). This indicates that those who viewed the app version that included privacy controls perceived a higher level of control than those

who viewed the app without the privacy controls. With regard to empathy, the *t*-test indicated a significant mean difference ($t(137) = -4.60; p < .001$) between the treatment group ($n = 68; mean = 5.77; s.e. = .29$) and the control group ($n = 71; mean = 4.09; s.e. = .22$). This indicates that those who viewed the app version in which the home screen included images of cancer and Alzheimer’s patients had higher empathic concern than those who viewed the app version in which the home screen included images of oceans.

Privacy controls and empathic concern were dummy coded (privacy controls: provided = 1, not provided = 0; empathy: induced = 1, not induced = 0). The privacy concerns construct was measured using four items [e.g., “*I am concerned that the data I donate to datadonors could be misused*” (7-point Likert scale)] (Cronbach’s $\alpha = .96$). A mean score was computed for privacy concerns ($mean = 5.03; s.d. = 1.70; min = 1; max = 7$).⁵⁴ The dependent variable (i.e., amount of data donation) is the sum of the items participants decided to donate ($mean = 12.32; s.d. = 9.32; min = 0; max = 23$). Appendix A.1 shows the study instrument and the measurement scales used.

Statistical Analyses

We applied Ordinary Least Square (OLS) multiple regression to test the hypotheses. Appendix A.3 shows additional analyses that were conducted before and after including the control variables. In the final model, we dropped a number of control variables because they did not improve the model fit. The final model was specified as follows:

$$\begin{aligned} AmountofDataDonation_i &= \beta_0 + \beta_1 Empathy_i + \beta_2 PrivacyControls_i + \beta_3 PrivacyConcerns_i \\ &+ \beta_4 EmpathyXPrivacyControls_i + \beta_5 PrivacyControlsXPrivacyConcerns_i \\ &+ \beta_6 EmpathyXPrivacyConcerns_i + \beta_7 EmpathyXPrivacyControlsXPrivacyConcerns_i + \beta_8 Trust_i \\ &+ \beta_9 Mood_i + u_i \end{aligned}$$

The β_7 coefficient for the 3-way interaction provides an appropriate (omnibus) test for H4a. The inclusion of this 3-way interaction, however, leads us to rely on marginal effect (*ME*) estimations instead of the β coefficient to test the two 2-way interaction hypotheses (H2a and H3b) and the main effect

⁵⁴ Exploratory factor analysis and reliability tests were conducted before computing a mean score for privacy concerns and the multi-item control variables (i.e., trust, mood, and altruistic personality). The factor analysis results (Appendix A.2) showed convergent and discriminant validity and the reliability results for each construct were well above the .7 threshold.

hypothesis (H1) (for more information on the appropriateness of the *ME* approach as compared to a hierarchical regression approach for testing main effect or 2-way interaction effect hypotheses in the existence of a 3-way interaction, see Brambor et al. 2006; Dawson 2014; Kingsley et al. 2017; Williams 2012). In short, this approach enables testing the 2-way interaction and main effects using the assumed correct specification of the model (i.e., full model) and hence unbiased estimates. However, the hierarchical approach leads to testing these effects using a misspecified model (e.g., testing the 2-way interaction and main effects without including the significant 3-way interaction term), and hence biased estimates of the 2-way interaction and main effects. Table 1 shows the correlation matrix for the variables tested based on experiment 1.

Table 1. Correlation matrix

| | <i>mean</i> | <i>s.d.</i> | <i>min</i> | <i>max</i> | 1 | 2 | 3 | 4 |
|----------------------------|-------------|-------------|------------|------------|------|------|-----|---|
| 1. Amount of Data Donation | 12.32 | 9.45 | 0.00 | 23.00 | 1 | | | |
| 2. Privacy Concerns | 5.03 | 1.70 | 1.00 | 7.00 | -.49 | 1 | | |
| 3. Trust | 4.74 | 1.15 | 1.45 | 7.00 | .64 | -.49 | 1 | |
| 4. Mood [†] | -.73 | 1.88 | -6.00 | 6.00 | .50 | -.33 | .38 | 1 |

[†] Mood was calculated by subtracting post-donation mood from baseline mood (see Appendix A.1). Therefore, it reflects the change in participants' mood after making the donation decision.

Note: A higher score on trust and mood reflects a trusting belief in the data donation app and a positive or enhanced mood state after making the donation decision.

Results

Table 2 presents the regression results. Based on both the β coefficient and *ME* estimation, the results show support for H1 as higher levels of privacy concerns are associated with lower data donations ($\beta_{PrivacyConcerns} = -1.670$; *s.e.* = .87; $p < .01$; $\beta_{PrivacyConcerns_ME} = -1.332$; *s.e.* = .40; $p < .01$).

Regarding the 2-way interaction effects (H2a and H3a), the β coefficients show that the negative effect of privacy concerns is weaker when privacy controls are provided ($\beta_{PrivacyControlsXPrivacyConcerns} = 2.003$; *s.e.* = .95; $p < .05$) or when empathic concern is induced ($\beta_{EmpathyXPrivacyConcerns} = 2.628$; *s.e.* = .90; $p < .01$). Probing the *ME* estimations for each privacy controls condition indicates that the negative effect of privacy concerns is weaker, but still significant, when privacy controls are provided ($\beta_{PrivacyConcerns_under_PrivacyControls[provided]_ME} = -1.124$; *s.e.* = .48; $p < .05$) compared to when privacy controls are not provided ($\beta_{PrivacyConcerns_under_PrivacyControls[not\ provided]_ME} = -1.530$; *s.e.* = .56; $p < .01$) (Figure 3, Panel A). Probing the *ME* estimations for each empathy condition indicates that the negative effect of privacy

concerns is not significant when empathic concern is induced ($\beta_{PrivacyConcerns_under_Empathy[induced]_{ME}} = -.805$; $s.e. = .52$; $p > .05$) but is significant when empathic concern is not induced ($\beta_{PrivacyConcerns_under_Empathy[not\ induced]_{ME}} = -1.836$; $s.e. = .51$; $p < .01$) (Figure 3, Panel B). Thus, H2a and H3a are supported.

Last, the β coefficient for the 3-way interaction term (H4a), is significant ($\beta_{EmpathyXPrivacyControlsXPrivacyConcerns} = -3.264$; $s.e. = 1.29$; $p < .05$) providing general support for H4a. To further probe this 3-way interaction effect, we test the significance of the four possible slopes. The results indicate that the negative effect of privacy concerns is significant only under one condition, where privacy controls are not provided and empathic concern is not induced ($\beta_{PrivacyConcerns_under_PrivacyControls[not\ provided]\&Empathy[not\ induced]_{ME}} = -2.816$; $s.e. = .87$; $p < .01$). However, the negative effect of privacy concerns is insignificant in the presence of privacy controls and/or empathic concern. These results provide full support for the predictions of H4a.⁵⁵ Figure 3 (Panel C) depicts the four slopes along with their statistics.

Table 2. Experiment 1's Regression Results

| Dependent Variable: Amount of Data Donation | Model |
|---|-----------------------|
| | β (robust s.e.) |
| Constant | -5.064 (2.86) |
| Empathy (induced) | 1.289 (1.67) |
| PrivacyControls (provided) | -1.670 (1.72) |
| PrivacyConcerns | -2.816** (.87) |
| EmpathyXPrivacyControls | .839 (2.33) |
| PrivacyControlsXPrivacyConcerns | 2.003* (.95) |
| EmpathyXPrivacyConcerns | 2.628** (.90) |
| EmpathyXPrivacyControlsXPrivacyConcerns | -3.264* (1.29) |
| Control Variables | |
| Trust | 3.895*** (.54) |
| Mood | 1.411*** (.29) |
| F value | (9, 129) 30.12*** |
| R ² (Adjusted R ²) | 54.63% (51.46%) |
| N | 139 |

* $p < .05$; ** $p < .01$; *** $p < .001$

Notes:

- PrivacyConcerns was mean centered before creating the interaction terms.

- A higher score on trust and mood reflects a trusting belief in the data donation app and a positive mood state after making the donation decision.

⁵⁵ We conducted further analyses using different proxies for amount of data donation (i.e., low sensitivity items [gender, ethnicity, education, height, and sleep], moderate sensitivity items [work experience, sexual orientation, weight, blood type, vaccination, allergies, drinking, smoking, exercise, social media, and diet], and high sensitivity items [birthdate, benign diseases, risky diseases, family history, drug use, surgeries, and emotions]). This categorization was based on the participants' ratings of the sensitivity of each item (1 Not at all sensitive... 7 Extremely sensitive). The average ratings for the low, moderate, and high sensitivity items were 2.65 ($s.d. = 1.82$), 3.36 ($s.d. = 1.79$), and 4.34 ($s.d. = 1.82$), respectively. The conclusions are very consistent when using low or moderate sensitivity items as a proxy for amount of data donation. When using high sensitivity items, the conclusions also remain consistent with one exception. The effect of privacy concerns when privacy controls are provided but without empathic concern inducement (Figure 3, Panel C, red slope right side) becomes significant ($\beta_{PrivacyConcerns_under_PrivacyControls[provided]\&Empathy[not\ induced]_{ME}} = -.363$; $s.e. = .17$; $p < .05$; amount of data donation $mean = 3.30$, $s.d. = 3.05$, $min = 0$, $max = 7$). Given that this proxy reflects high sensitivity items, this finding is not surprising and it actually indicates the significance of the joint effect of privacy controls and empathic concerns. For brevity and because this finding does not change our conclusions, we do not report the results.

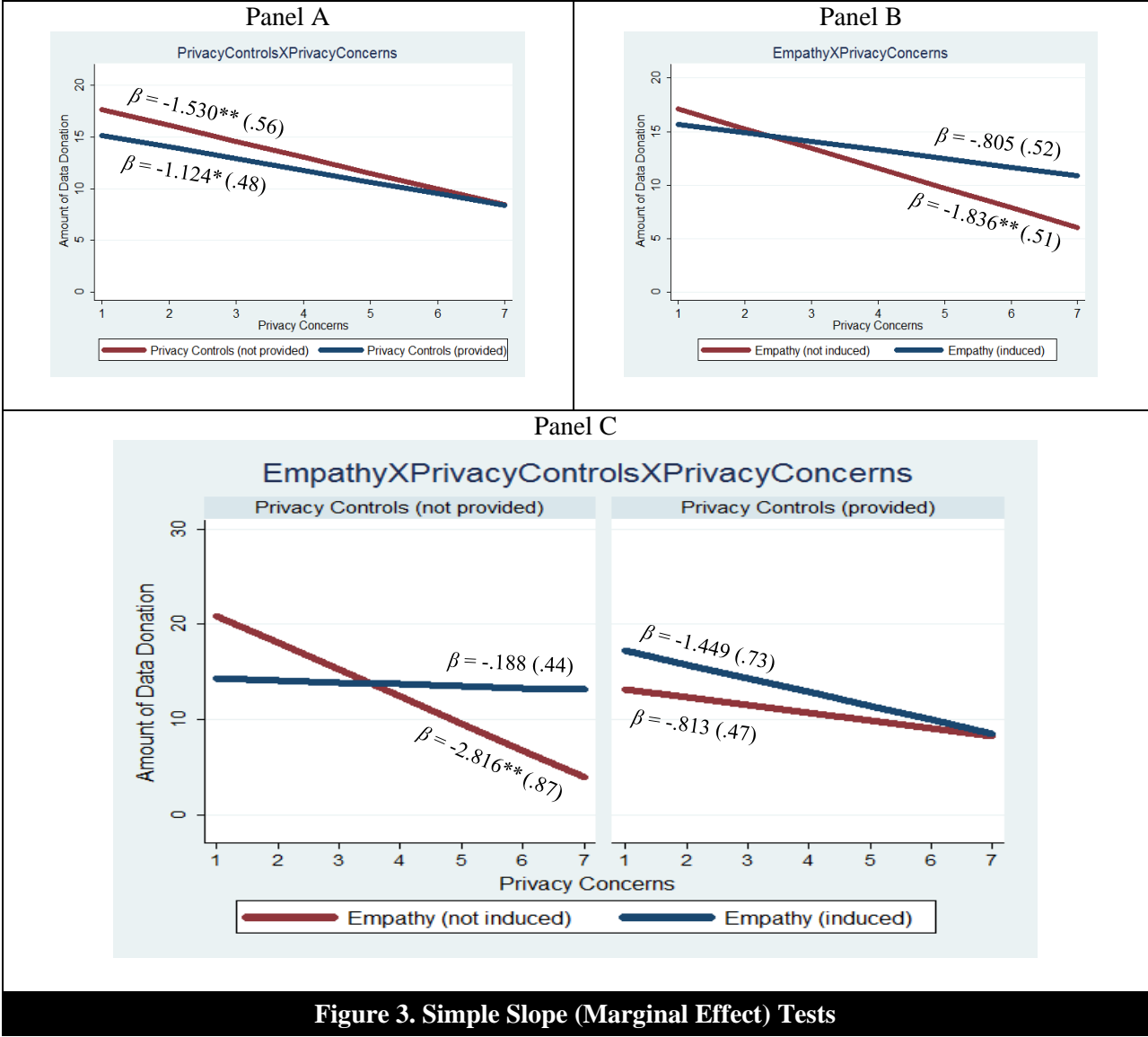


Figure 3. Simple Slope (Marginal Effect) Tests

EXPERIMENT 2

Sample and Procedure

The sample included 177 participants: mean age = 37.5 years; female = 69.5%; White = 72.9%. The procedure was the same as the one used in experiment 1 with some exceptions. Specifically, all participants viewed the app version in which the home screen included images of cancer and Alzheimer’s patients (i.e., empathy induced). In addition, all participants viewed the app version in which the privacy controls were provided. Thus, both empathic concern and privacy controls were constant. Similar to experiment 1, after being introduced to the app and its features (in which we manipulated ease of donation

and social nudging), participants were then asked to select the data they would like to donate. In addition to the scales used in experiment 1, we also measured perceived control over the donation method and other manipulation checks for the manipulated variables (see Appendix B.1). Again, we observed that the participants acted as if they were making actual donation decisions. Below are a few examples from experiment 2:

- *"I'm not sure that I would donate my data - I don't think that anyone would need my information about certain things just for donation processes."*
- *"I didn't donate any data because it would be very time consuming."*
- *"I decided to donate some data because it is what I am confident of knowing about myself."*
- *"I am not comfortable with providing donation history about my medical matters but I understand the importance of data being received. I will allow the site to use some of my data, but not all. I appreciate being able to choose which data to share and which to keep private."*
- *"I'm just not comfortable sharing much of my data because I do not know what type of risk is posed that this company's information could be compromised therefore compromising my data as well."*
- *"I decided to donate all of my data since it could help with research and possibly help other people."*

Manipulations and Measurements

We manipulated ease of donation and social nudging. Participants were randomly assigned to either an automatic donation method condition or a manual donation method condition (Figure 4, Panel A). Social nudging was also manipulated, such that participants were randomly assigned to view a version of the app in which they were informed that based on the data we have collected from Amazon Mechanical Turk workers, 89% (high nudge) or 11% (low nudge) of the participants decided to donate their data (Figure 4, Panel B).⁵⁶

We developed six items [e.g., *"it is easy to donate data through the datadonors app; donating data through the datadonors app takes a few seconds"* (7-point Likert scale)] (*Cronbach's* $\alpha = .93$) and used them as a manipulation check for ease of donation. We developed two items [*"it seems that many people have decided to donate their data; it seems that many people are in favor of this data donation initiative"* (7-point Likert scale)] (*Cronbach's* $\alpha = .95$) and used them as a manipulation check for social nudging.

⁵⁶ The screen shots for the social nudging conditions were presented using a much larger size than they appear in Panel B.



| Panel A (Ease of Donation) | Panel B (Social Nudging) |
|--|---|
| <p style="text-align: center;">Automatic Donation Method</p> <p>Donating data through datadonors takes a <u>few seconds with no effort</u> because the donation process is <u>automatic</u>. You <u>just</u> have to choose the data you would like to donate. Then, <u>the datadonors app will do the heavy work by searching and capturing the data from other apps</u>. This <u>automatic</u> donation method requires you to put <u>no</u> effort in entering the data and it takes <u>a few seconds only</u>.</p> | <p style="text-align: center;">High Social Nudge</p> <p>So far, based on the data we have collected from Amazon Mechanical Turk (MTurk) workers, <u>89%</u> of the participants decided to donate their data. If you decide to donate, you will help datadonors reach its goal.</p>  |
| <p style="text-align: center;">Manual Donation Method</p> <p>Donating data through datadonors takes <u>some time and effort</u> because the donation process is <u>manual</u>. You have to choose the data you would like to donate. Then, <u>you have to enter the data manually for each category</u>. This <u>manual</u> donation method requires you to put <u>some</u> effort in entering the data and it takes <u>about 45 minutes</u>.</p> | <p style="text-align: center;">Low Social Nudge</p> <p>So far, based on the data we have collected from Amazon Mechanical Turk (MTurk) workers, <u>11%</u> of the participants decided to donate their data. If you decide to donate, you will help datadonors reach its goal.</p>  |

Figure 4. Ease of Donation and Social Nudging Manipulations

The *t*-tests results indicated that both manipulations were successful. With regard to ease of donation, the *t*-test indicated a significant mean difference ($t(175) = -5.76; p < .001$) between the automatic condition ($n = 88; mean = 5.74; s.e. = .10$) and the manual condition ($n = 89; mean = 4.61; s.e. = .16$). This indicates that those who viewed the app version in which the donation method was automatic perceived more ease of donation than those who viewed the app version in which the donation method was manual. With regard to social nudging, the *t*-test indicated a significant mean difference ($t(175) = -9.78; p < .001$) between the high social nudging condition ($n = 84; mean = 5.77; s.e. = .12$) and the low social nudging condition ($n = 93; mean = 3.58; s.e. = .18$). This indicates that the social nudge conditions were perceived as intended.

Ease of donation and social nudging were dummy coded (ease of donation: automatic = 1, manual = 0; social nudging: high = 1, low = 0). The privacy concerns construct was measured using the same four items as in experiment 1 (*Cronbach's* $\alpha = .97$) and a mean score was computed for privacy concerns (*mean* = 4.92; *s.d.* = 1.89; *min* = 1; *max* = 7).⁵⁷ Amount of data donation was computed using the sum of items selected for donation as was done in experiment 1 (*mean* = 13.57; *s.d.* = 9.15; *min* = 0; *max* = 23). Last, perceived control over the donation method was measured using three items [*"I will have control over the method through which I enter my data; I will have control in terms of how I donate my data; I will have control over how the data is entered"* (7-point Likert scale)] (*Cronbach's* $\alpha = .89$). A mean score was computed for perceived control (*mean* = 5.82; *s.d.* = 1.12; *min* = 1; *max* = 7).

Statistical Analyses

We applied OLS multiple regression to test the hypotheses using the same approach that was applied to analyze the data for experiment 1. Appendix B.3 shows the additional analyses that were conducted before and after including the control variables. Table 3 shows the correlation matrix for the variables tested based on experiment 2. The final model was specified as follows:

$$\begin{aligned}
 \text{AmountofDataDonation}_i &= \beta_0 + \beta_1 \text{EaseOfDonation}_i + \beta_2 \text{SocialNudge}_i + \beta_3 \text{PrivacyConcerns}_i \\
 &+ \beta_4 \text{EaseOfDonationXSocialNudge}_i + \beta_5 \text{EaseOfDonationXPrivacyConcerns}_i \\
 &+ \beta_6 \text{SocialNudgeXPrivacyConcerns}_i + \beta_7 \text{EaseOfDonationXSocialNudgeXPrivacyConcerns}_i \\
 &+ \beta_8 \text{PerceivedControl}_i + \beta_9 \text{Trust}_i + \beta_{10} \text{Mood}_i + u_i
 \end{aligned}$$

Table 3. Correlation matrix

| | <i>mean</i> | <i>s.d.</i> | <i>min</i> | <i>max</i> | 1 | 2 | 3 | 4 | 5 |
|----------------------------|-------------|-------------|------------|------------|------|------|-----|-----|---|
| 1. Amount of Data Donation | 13.57 | 9.15 | 0.00 | 23.00 | 1 | | | | |
| 2. Privacy Concerns | 4.92 | 1.89 | 1.00 | 7.00 | -.49 | 1 | | | |
| 3. Perceived Control | 5.82 | 1.12 | 2.00 | 7.00 | .33 | -.23 | 1 | | |
| 4. Trust | 4.94 | 1.17 | 1.00 | 7.00 | .57 | -.63 | .39 | 1 | |
| 5. Mood [†] | -.25 | 1.77 | -6.00 | 5.00 | .42 | -.35 | .31 | .46 | 1 |

[†]Mood was calculated by subtracting post-donation mood from baseline mood. Therefore, it reflects the change in participants' mood after making the donation decision.

Note: A higher score on trust and mood reflects a trusting belief in the data donation app and a positive or enhanced mood state after making the donation decision.

Results

Table 4 presents the regression results. Based on both the β coefficient and *ME* estimation, the results show that higher levels of privacy concerns are associated with lower data donations ($\beta_{\text{PrivacyConcerns}} = -$

⁵⁷ Exploratory factor analysis and reliability tests were conducted before computing a mean score for privacy concerns, perceived control over the donation method and the multi-item control variables (i.e., trust, mood, and altruistic personality). The factor analysis results (Appendix B.2) showed convergent and discriminant validity and the reliability results for each construct were well above the .7 threshold.

1.699; *s.e.* = .47; *p* < .001; $\beta_{PrivacyConcerns_ME} = -1.198$; *s.e.* = .35; *p* < .01). This effect size is consistent with experiment 1's finding and thus provides further support for H1.

Regarding the 2-way interaction effects (H2b and H3b), the β coefficients show that the negative effect of privacy concerns is weaker when ease of donation is automatic ($\beta_{EaseOfDonation \times PrivacyConcerns} = 1.063$; *s.e.* = .53; *p* < .05) or when a high social nudge is induced ($\beta_{SocialNudge \times PrivacyConcerns} = 1.109$; *s.e.* = .72; *p* > .05). Probing the *ME* estimations for each ease of donation condition indicates that the negative effect of privacy concerns is almost identical for both the automatic and manual condition ($\beta_{PrivacyConcerns_under_EaseOfDonation[automatic]_ME} = -1.124$; *s.e.* = .40; *p* < .01; $\beta_{PrivacyConcerns_under_EaseOfDonation[manual]_ME} = -1.181$; *s.e.* = .45; *p* < .05). However, as Figure 5 (Panel A) shows, the effect of privacy concerns is weaker for the automatic condition in terms of the slope baseline. Specifically, the baseline for the negative privacy concerns slope for the automatic condition is significantly above that for the manual condition. This finding provides support for H2b as it indicates that the amount of data donation is higher when applying an automatic donation method even in the presence of privacy concerns. Probing the *ME* estimations for each social nudging condition indicates that the negative effect of privacy concerns is almost identical and significant under both the high and low social nudge conditions ($\beta_{PrivacyConcerns_under_SocialNudge[high]_ME} = -1.228$; *s.e.* = .50; *p* < .05; $\beta_{PrivacyConcerns_under_SocialNudge[low]_ME} = -1.170$; *s.e.* = .35; *p* < .01) (Figure 5, Panel B). Given no significant difference between these two slopes, H3b is not supported.

Last, the results indicate a significant 3-way interaction ($\beta_{EaseOfDonation \times SocialNudge \times PrivacyConcerns} = -2.309$; *s.e.* = .98; *p* < .05) providing general support for H4b. To further probe this 3-way interaction effect, we test the significance of the four possible slopes (Figure 5, Panel C). The results support three predictions proposed in H4b. Consistent with the findings from experiment 1, the negative effect of privacy concerns is significant in the absence of a facilitating normative factor or a distracting non-normative factor (i.e., manual donation method and low nudge) ($\beta_{PrivacyConcerns_under_EaseOfDonation[manual] \& SocialNudge[low]_ME} = -1.699$; *s.e.* = .47; *p* < .001). However, in the presence of either a facilitating normative factor (i.e., automatic donation method) or a distracting non-

normative factor (i.e., high social nudge), the negative effect of privacy concerns is not significant ($\beta_{PrivacyConcerns_under_EaseOfDonation[automatic]\&SocialNudge[low]_{ME}} = -.635; s.e. = .41; p > .05; \beta_{PrivacyConcerns_under_EaseOfDonation[manual]\&SocialNudge[high]_{ME}} = -.609; s.e. = .68; p > .05$). Unexpectedly, the negative effect of privacy concerns is significant under the condition of automatic donation method coupled with a high social nudge ($\beta_{PrivacyConcerns_under_EaseOfDonation[automatic]\&SocialNudge[high]_{ME}} = -1.855; s.e. = .61; p > .01$). Figure 5 (Panel C) depicts the four slopes along with their statistics.⁵⁸

Table 4. Experiment 2's Regression Results

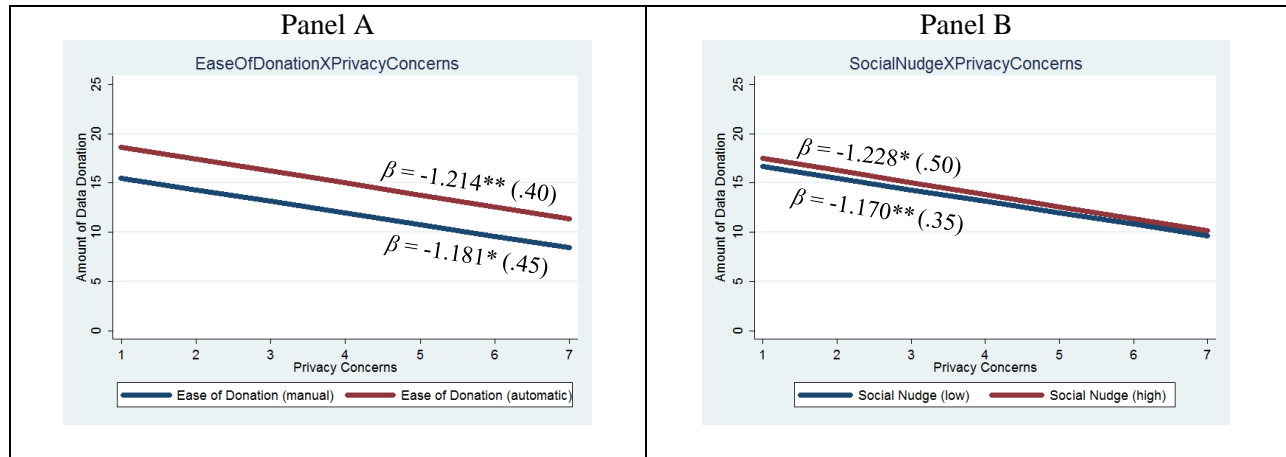
| Dependent Variable: Amount of Data Donation | Model |
|---|-----------------------|
| | β (robust s.e.) |
| Constant | -8.217 (4.22) |
| EaseOfDonation (automatic) | 4.047** (1.41) |
| Social Nudge (high) | 1.726 (1.70) |
| PrivacyConcerns | -1.699*** (.47) |
| EaseOfDonationXSocialNudge | -2.019 (2.16) |
| EaseOfDonationXPrivacyConcerns | 1.063* (.53) |
| SocialNudgeXPrivacyConcerns | 1.090 (.72) |
| EaseOfDonationXSocialNudgeXPrivacyConcerns | -2.309* (.98) |
| PerceivedControl | 1.437* (.65) |
| Control Variables | |
| Trust | 2.247** (.69) |
| Mood | 1.005** (.37) |
| F value | (10, 166) 27.61*** |
| R ² (Adjusted R ²) | 43.12% (39.69%) |
| N | 177 |

* $p < .05$; ** $p < .01$; *** $p < .001$

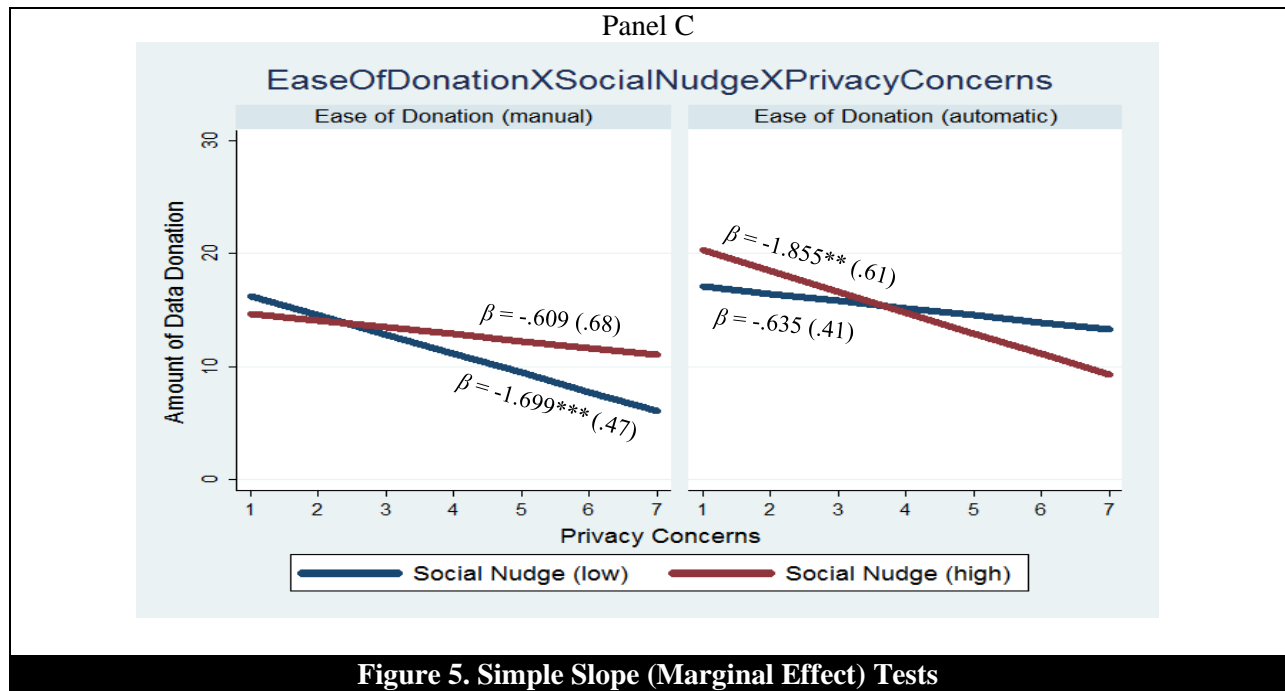
Notes:

- PrivacyConcerns was mean centered before creating the interaction terms.

- A higher score on trust and mood reflects a trusting belief in the data donation app and a positive mood state after making the donation decision.



⁵⁸ We conducted further analyses using different proxies for amount of donation (i.e., low sensitivity items, moderate sensitivity items, and high sensitivity items). Participants' ratings of the sensitivity of each item in experiment 2 were consistent with those observed in experiment 1. The average ratings for the low, moderate, and high sensitivity items were 2.70 ($s.d. = 1.71$), 3.55 ($s.d. = 1.75$), and 4.45 ($s.d. = 1.95$), respectively. The conclusions are very consistent when using different proxies for amount of data donation. Therefore, we do not report these results.



GENERAL DISCUSSION

The purpose of this study was to explore privacy concerns in the context of data donation in order to present practical implications for data donation organizations while providing theoretical implications for the privacy literature. The concept of data donation is recent and it is only in the past few years that physicians and medical researchers have recognized the promises of data donation initiatives. The medical community predicts that data donations will contribute to preventing chronic illness, which is “the biggest unfulfilled dream in health care” (Topol 2015, p. 238). The main challenge in this regard is the absence of rich health data, which makes prevention of chronic diseases difficult or even impossible. Data donation projects have the potential to address this challenge (Shaw et al. 2015, 2016; Taylor and Mandl 2015; Topol 2015). However, advocates for data donation also contend that individuals’ privacy concerns represent a strong barrier for the development and sustainability of data donation projects (Mandl et al. 2015; Shaw et al. 2016; Taylor and Mandl 2015; Topol 2015).

We designed a data donation app and conducted two experiments to examine whether privacy concerns impact data donation decisions. Our results show that individuals who have high privacy concerns are less likely to donate their data for medical research. This finding is based on the quantitative

data reported and the qualitative feedback reported by the participants. Many participants voiced their privacy concerns in this context:

- *“There is a limit to the amount of personal data I would donate. I feel there are too many data breaches these days and the last thing I would want to donate is "personal-private-identifiable" information. While I do not see an issue with the very basic information being shared I do feel too much basic information can fill in the missing pieces for a hacker to use against me in financial fraud etc.”*
- *“I am very cautious about sharing any of my personal data online. I generally do not do this if at all possible. Even though the app has a lot of safeguards in place, I believe that the only way to ensure safety from data misuse (leaks, hacks, etc.) is not to provide it in the first place.”*

Such a finding supports the anecdotal argument raised by the medical community regarding the critical role of privacy concerns. It also supports findings from the vast majority of privacy studies (i.e., privacy concerns are associated negatively with disclosure-related outcomes) (Li 2011; Smith et al. 2011; Yun et al. 2014). Because this finding was anticipated, we aimed to extend the literature by exploring factors that have the potential to attenuate this negative effect in order to enhance data donation outcomes. This was the main motivation of our study as privacy concerns represent one of the strongest determinants of data donation decisions. Accordingly, we leveraged relevant research and theories and we focused on two normative technology-based factors (i.e., privacy controls and ease of donation) and two non-normative peripheral factors (i.e., empathic concern and social nudging). The findings provided empirical evidence on the utility of these factors to enhance data donations. In addition, they provided empirical evidence supporting the enhanced APCO model, recently proposed by Dinev et al. (2015).

In experiment 1, we found a significant moderation effect of privacy controls, such that the negative effect of privacy concerns on data donation decisions is weaker when donors are provided with privacy controls through the donation app. From a normative and practical perspective, potential donors would appreciate the power of control over their donated data. The ability to allow or disallow certain organizations to access or share the donated data and the ability to retract donated data through easily accessible privacy controls can alleviate donors' perceptions of privacy risks, even in the presence of significant privacy concerns. When potential donors are empowered through privacy controls, they are more likely to relax their privacy concerns, if any, and hence they are more likely to donate. Therefore, we recommend implementing granular privacy controls in data donation projects. We also found a

significant moderation effect of empathic concern, such that the negative effect of privacy concerns is weaker when donors' empathic concern is induced through emotion-arousing images. Therefore, data donations could be further increased by inducing potential donors' empathic concern through emotional images or other feasible techniques (Batson 2011). When we accounted for the combined moderation effect (Figure 3, Panel C), the significant negative effect of privacy concerns disappeared in the presence of privacy controls and/or empathic concern. This finding suggests that the negative effect of privacy concerns on data donation decisions can be mitigated by providing donors with granular privacy controls and/or inducing their empathic concern.

In experiment 2, we provided donors with privacy controls and induced their empathic concern and we were still able to observe additional moderation effect by applying an automatic donation method or herding donors via a simple social nudge (Figure 5, Panel C). With respect to the normative factor, potential donors are likely to assess the amount of effort and time it would take to make a data donation. If it is easy and quick, potential donors, even if they have privacy concerns, would be willing to donate more data as compared to an effortful and time-consuming manual donation method. These findings corroborate those from the donation literature (Beurel et al. 2017; Feeley and Moon 2009; Lee et al. 2017; Masser et al. 2008; Piersma et al. 2017) and suggest that providing donors with an easy donation method can improve data donation outcomes. With respect to the non-normative factor, potential donors' cognitive processing of their privacy preferences can be easily influenced by the decision of their in-group members. We found that – in the manual donation condition – when a majority (only a minority) of in-group members decided to donate their data, our participants were less (more) likely to act on their privacy concerns and hence they were more (less) likely to donate. However, according to our results, such a strong positive nudge (i.e., high social nudge) when combined with an automatic donation method can backfire and lead potential donors to reflect more on their privacy concerns. This finding was unexpected especially since granular privacy controls were provided to these participants and hence they

should have perceived lower privacy risks.⁵⁹ A post-hoc plausible theoretical explanation is that our participants followed the notion of “I should give it more time and thought first.” A number of participants who were assigned to the automatic donation method coupled with a high social nudge provided this view when they were asked to tell us why they decided not to donate some or any of their data:

- *“I chose not to at this time, maybe if I think about it some more.”*
- *“I decided to donate nothing at the moment. Not any reason just my preference.”*
- *“I’m not sure what it is, but my instinct is telling me it is a bad idea.”*
- *“I have a lot of data, a lot of info. I’m not comfortable doing that in a few minutes.”*
- *“I would want to do extensive research before agreeing to provide any personal information”*
- *“I don’t want my data being shared to be used against me until we’ve stricter data protection laws”*
- *“I think that it’s a good idea and I like the app, however I won’t be interested in participating.”*

Said differently, privacy concerned donors might perceive this as “too much of a thing is a bad thing,” i.e., privacy controls, easy donation method, empathic concern, and social influence. Accordingly, data donation organizations should be careful about incorporating various interventions that theoretically seem useful or complementary because they can have unexpected results.

Our study makes theoretical contributions by shedding light on boundary conditions for the relationship between privacy concerns and disclosure decisions. While at the average level there is a significant effect of privacy concerns, this effect is conditional on normative factors through which individuals are able to manage their personal information or relax their concerns in a rational manner. This effect is also conditional on non-normative factors that could reduce individuals’ ability and/or motivation to act on their dispositional privacy concerns. Recent research provided support for the significant main effect of other normative and non-normative factors on disclosure decisions (Adjerid et al. 2016, 2018). We further show that normative and non-normative factors interact together to affect

⁵⁹ We also tested a model in which we specified perceived control over the donation method as a moderator while ease of donation is not. More specifically, we swapped automatic with perceived control in this model. The results of this model simply mimicked those reported above. The negative effect of privacy concerns was the largest in two conditions: 1) low perceived control & low nudge (a condition analogous to manual donation method & low nudge) and 2) high perceived control & high nudge (a condition analogous to automatic donation method & high nudge): ($\beta_{PrivacyConcerns_under_PerceivedControl[low]\&SocialNudge[low]}_{ME} = -2.562$; $s.e. = .83$; $p < .01$); ($\beta_{PrivacyConcerns_under_PerceivedControl[high]\&SocialNudge[high]}_{ME} = -1.244$; $s.e. = .65$; $p < .10$). Hence, this adds robustness to our conclusion that: 1) a manual donation method (which leads to higher perceived control but effortful and time-consuming donation process) coupled with a low social nudge results in the strongest effect of privacy concerns while 2) an automatic donation method (which leads to lower perceived control but effortless and efficient donation process) coupled with a high social nudge might also result in a negative effect of privacy concerns. Therefore, it is better to leverage only one of these factors (ease of donation or social nudge) in order to improve data donation outcomes because leveraging both factors together can backfire by leading potential donors to think suspiciously about the privacy implications of data donations.

disclosure decisions. Interestingly, experiment 1 shows that the non-normative factor (i.e., empathic concern), compared to the normative factor (i.e., privacy controls), has a stronger effect in terms of weakening the relationship between privacy concerns and disclosure decisions. In contrast, experiment 2 shows that the interaction between the normative (i.e., ease of donation) and the non-normative factor (social nudge) could either weaken or strengthen the relationship between privacy concerns and disclosure decisions. A direct theoretical implication, which supports the enhanced APCO model (Dinev et al., 2015), is that the effect of privacy concerns is indeed conditional on a number of non-normative factors, and we show that this effect is also conditional on normative factors. In summary, our study presents a number of boundary conditions for the link between privacy concerns and disclosure decision, and hence advances our understanding of the situations under which privacy beliefs might not be consistent with disclosure decisions (i.e., the privacy paradox).

Ethical Implications

It is important to note that the aim of our study is to advance our understanding of privacy decisions in the presence of significant privacy concerns while contributing to enhancing data donation outcomes. Yet, some ethical implications need to be considered carefully before applying some manipulations in practice, especially the non-normative factors that normally affect individuals' decisions in a subconscious way. While inducing normative factors (e.g., privacy controls and ease of donation) could facilitate donors to make informed decisions with appropriate justifications, manipulating non-normative factors that have the potential to reduce the level of effort in cognitive evaluation (e.g., emotions and social nudging) present an ethical dilemma to organizations. Specifically, individuals could be manipulated in a way that leads them to unjustifiably overlook their dispositional privacy concerns and this could lead them to make decisions that are inconsistent with their normal privacy preferences. Although this ethical consideration is beyond the scope of our study, we believe that data donation organizations should be cognizant of this ethical issue. Even if the ultimate goal is prosocial (i.e., data donation to help the medical community), putting manipulations such as ours into practice could raise ethical concerns. Therefore, if data donation organizations decide to employ such techniques they should do so with caution and they should assess

techniques that could be used to address this issue (e.g., informing potential donors about the role of emotions and nudging in influencing data donation decisions).

Limitations and Future Research

First, our experiments involved screen mockups of a data donation app. While the manipulations were successful and the participants acted as if they were making actual donations, future research is needed to replicate our findings in a simulated environment in which participants can decide to make data donations via their own electronic devices. Second, in each experiment, we focused on only three main constructs (i.e., privacy concern, normative factor, and non-normative factor) while controlling for a number of control variables. The findings showed a significant effect of perceived control over the donation method, trust, and mood. The higher perceived control and trusting beliefs participants had in data donors, the more likely they were to donate. Participants who believed that donating their data would enhance their mood state were more likely to donate. Although we were able to explain a large amount of the variance in data donation ($R^2_{\text{experiment1}} = 54.36\%$; $R^2_{\text{experiment2}} = 43.12\%$), future research may consider other constructs. Third, our sample is based on Amazon Mechanical Turk which has been shown to have acceptable statistical generalizability compared to traditional samples (Lowry et al. 2016). Future research may replicate our findings in other populations, such as chronic disease patients. Fourth, the images of patients we used to induce empathic concern were accompanied by a text that motivates perspective taking “put yourself in their shoes” and “imagine how their families feel.” Perspective taking is a widely used method to induce empathic concern (Batson 2011). However, our design cannot distinguish whether the empathic concern was induced because participants read the text and in turn took the perspective of the patients and their families (i.e., empathic concern induced by perspective taking) or due to viewing of the patients in the images only (i.e., empathic concern induced by an aroused emotional state) or both perspective taking and the viewing of the images. Future research is needed to tease apart the extent to which our results may have been influenced by perspective taking. Given that our objective was to increase data donations through empathic concern, however, the exact mechanism through which this was achieved is not a

critical limitation. Last, future research can further explore ethical research questions that may arise from this novel healthcare practice.

CONCLUSION

The promise of data donation projects has yet to be realized. Data donations have the potential for advancing medical research and preventing chronic diseases. However, individuals' privacy concerns might inhibit the development and sustainability of data donation projects. While individuals are interested in protecting the privacy of their personal data, medical researchers are interested in collecting data donations. Privacy scholars are well-equipped to reconcile these opposing interests by leveraging recent theoretical advances in the privacy literature in order to contribute to the public health.

REFERENCES

- Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," in *Proceedings of the 1st ACM Conference on Electronic Commerce*, pp. 1-8.
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., and Wilson, S. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys* (50:3), Article 44.
- Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technology*, G. Danezis and P. Golle (eds.), Cambridge, UK: 6th International Workshop, pp. 36-58.
- Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26-33.
- Acquisti, A., Taylor, C. R., and Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (52:2), pp. 1-64.
- Adjerid, I., Peer, E., and Acquisti, A. 2018. "Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making," *MIS Quarterly* (42:2), pp. 465-488.
- Adjerid, I., Samat, S., and Acquisti, A. 2016. "A Query-Theory Perspective of Privacy Decision Making," *The Journal of Legal Studies* (45:S2), pp. S97-S121.
- Adler-Milstein, J., DesRoches, C. M., Kralovec, P., Foster, G., Worzala, C., Charles, D., Searcy, T., and Jha, A. K. 2015. "Electronic Health Record Adoption in US Hospitals: Progress Continues, But Challenges Persist," *Health Affairs* (34:12), pp. 2174-2180.
- Agarwal, R., Gao, G., DesRoches, C., and Jha, A. K. 2010. "Research Commentary-The Digital Transformation of Healthcare: Current Status and the Road Ahead," *Information Systems Research* (21:4), pp. 796-809.
- Alashoor, T., Han, S., and Joseph, R. C. 2017. "Familiarity with Big Data, Privacy Concerns, and Self-Disclosure Accuracy in Social Networking Websites: An APCO Model," *Communications of the Association for Information Systems* (41), pp. 62-96.
- Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469-490.
- Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.
- Ashford, W. 2016. "Google Company's Access to NHS Records Raises Privacy Concerns," *Computer Weekly*. Retrieved (March 25, 2018) from <http://www.computerweekly.com/news/450295503/Google-companys-access-to-NHS-records-raises-privacy-concerns>
- Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.
- Bansal, G., Zahedi, F., and Gefen, D. 2016. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online," *Information & Management* (53:1), pp. 1-21.
- Bansal, G., Zahedi, M., and Gefen, D. 2015. "The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern," *European Journal of Information Systems* (24:6), pp. 624-644.
- Barth, S., and de Jong, M. 2017. "The Privacy paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review," *Telematics and Informatics* (34), pp. 1038-1058.

- Batson, C. D. 2011. *Altruism in Humans*. Oxford University Press, USA.
- Batson, C. D., Ahmad, N., and Lishner, D. A. 2009. "Empathy and Altruism," in *The Oxford Handbook of Positive Psychology*, C. R. Snyder and S. J. Lopez (eds.), New York, U.S.: Oxford University Press Inc., pp. 417-426.
- Beurel, A., Terrade, F., Lebaudy, J. P., and Danic, B. 2017. "Determinants of Plasma Donation: A Review of the Literature," *Transfusion Clinique et Biologique* (24:3), pp. 106-109.
- Bless, H., Bohner, G., Schwarz, N., and Strack, F. 1990. "Mood and Persuasion: A Cognitive Response Analysis," *Personality and Social Psychology Bulletin* (16:2), pp. 331-345.
- Brambor, T., Clark, W. R., and Golder, M. 2006. "Understanding Interaction Models: Improving Empirical Analyses," *Political Analysis* (14:1), pp. 63-82.
- Brandimarte, L., Acquisti, A., and Loewenstein, G. 2013. "Misplaced Confidences: Privacy and the Control Paradox," *Social Psychological and Personality Science* (4:3), pp. 340-347.
- Breward, M., Hassanein, K., and Head, M. 2017. "Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach," *Information Systems Research* (28:4), pp. 760-774.
- Cavusoglu, H., Phan, T. Q., Cavusoglu, H., and Airoidi, E. M. 2016. "Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook," *Information Systems Research* (27:4), pp. 848-879.
- Chhanabhai, P., and Holt, A. 2007. "Consumers are ready to Accept the Transition to Online and Electronic Records If They Can be Assured of the Security Measures," *Medscape General Medicine* (9:1), pp. 8.
- Choi, B. C., Jiang, Z., Xiao, B., and Kim, S. S. 2015. "Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding," *Information Systems Research* (26:4), pp. 675-694.
- Cialdini, R. B. 2009. *Influence: Science and Practice*, Boston: Pearson Education.
- Conger, J. A., and Kanungo, R. N. 1988. "The Empowerment Process: Integrating Theory and Practice," *Academy of Management Review* (13:3), pp. 471-482.
- Dawson, J. F. 2014. "Moderation in Management Research: What, Why, When, And How," *Journal of Business and Psychology* (29:1), pp. 1-19.
- Debatin, B., Lovejoy, J. P., Horn, A. K., and Hughes, B. N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* (15:1), pp. 83-108.
- Deng, X., Joshi, K. D., and Galliers, R. D. 2016. "The Duality of Empowerment and Marginalization in Microtask Crowdsourcing: Giving Voice to the less Powerful through Value Sensitive Design," *MIS Quarterly* (40:2), pp. 279-302.
- Dickert, S., Sagara, N., and Slovic, P. 2011. "Affective Motivations to Help Others: A Two-Stage Model of Donation Decisions," *Journal of Behavioral Decision Making* (24:4), pp. 361-376.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80,100.
- 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.
- Eisenberg, N., and Miller, P. A. 1987. "The Relation of Empathy to Prosocial and Related Behaviors," *Psychological Bulletin* (101:1), pp. 91-119.
- Eyal, N. 2014. "Nudging by Shaming, Shaming by Nudging," *International Journal of Health Policy and Management* (3:2), pp. 53-56.
- Feeley, T. H., and Moon, S. I. 2009. "A Meta-Analytic Review of Communication Campaigns to Promote Organ Donation," *Communication Reports* (22:2), pp. 63-73.
- Fox, G., and Connolly, R. 2018. "Mobile Health Technology Adoption across Generations: Narrowing the Digital Divide," *Information Systems Journal* (28:6), pp. 995-1019.

- Garber, C. 2015. "Donate Your Health Data to Medical Science," *Scientific American*. Retrieved (March 25, 2018) from <http://www.scientificamerican.com/podcast/episode/donate-your-health-data-to-medical-science/>
- Giles, M., Mcclenahan, C., Cairns, E., and Mallet, J. 2004. "An Application of the Theory of Planned Behaviour to Blood Donation: The Importance of Self-Efficacy," *Health Education Research* (19:4), pp. 380-391.
- Godin, G., Conner, M., Sheeran, P., Bélanger-Gravel, A., and Germain, M. 2007. "Determinants of Repeated Blood Donation among New and Experienced Blood Donors," *Transfusion* (47:9), pp. 1607-1615.
- Goswami, I., & Urminsky, O. 2016. "When Should the Ask be a Nudge? The Effect of Default Amounts on Charitable Donations," *Journal of Marketing Research* (53:5), pp. 829-846.
- Hong, W., and Thong, J. Y. L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.
- Hyde, M. K., and White, K. M. 2009. "To Be a Donor or Not to Be? Applying an Extended Theory of Planned Behavior to Predict Posthumous Organ Donation Intentions," *Journal of Applied Social Psychology* (39:4), pp. 880-900.
- Jiang, Z., Heng, C. S., and Choi, B. C. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579-595.
- John, L., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a Plane: Context Dependent Willingness to Divulge Personal Information," *Journal of Consumer Research* (37:5), pp. 858-873.
- Kahneman, D. 2011. *Thinking, Fast and Slow*, New York: Farrar, Straus and Giroux.
- Kallbekken, S., and Sælen, H. 2013. "'Nudging' Hotel Guests to Reduce Food Waste as a Win-Win Environmental Measure," *Economics Letters* (119:3), pp. 325-327.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.
- Kim, S. J., and Kou, X. 2014. "Not All Empathy Is Equal: How Dispositional Empathy Affects Charitable Giving," *Journal of Nonprofit & Public Sector Marketing* (26:4), pp. 312-334.
- Kingsley, A. F., Noordewier, T. G., and Bergh, R. G. V. 2017. "Overstating and Understating Interaction Results in International Business Research," *Journal of World Business* (52:2), pp. 286-295.
- Knapton, S. 2016. "How the NHS Got It So Wrong with Care.data," *The Telegraph*. Retrieved (March 25, 2018) from <http://www.telegraph.co.uk/science/2016/07/07/how-the-nhs-got-it-so-wrong-with-caredata/>
- Kohli, R., and Tan, S. S. L. 2016. "Electronic Health Records: How Can IS Researchers Contribute to Transforming Healthcare?," *MIS Quarterly*, (40:3), pp. 553-573.
- Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), pp. 122-134.
- Kuo, K. M., Ma, C. C., and Alexander, J. W. 2014. "How Do Patients Respond to Violation of Their Information Privacy?," *Health Information Management Journal* (43:2), 23-33.
- Lee, B., Fraser, I., and Fillis, I. 2017. "Nudging Art Lovers to Donate," *Nonprofit and Voluntary Sector Quarterly* (46:4), pp. 837-858.
- Li, H., Gupta, A., Zhang, J., and Sarathy, R. 2014. "Examining the Decision to Use Standalone Personal Health Record Systems as a Trust-Enabled Fair Social Contract," *Decision Support Systems* (57), pp. 376-386.
- Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), pp. 434-445.
- Li, T., and Slee, T. 2014. "The Effects of Information Privacy Concerns on Digitizing Personal Health Records," *Journal of the Association for Information Science and Technology* (65:8), pp. 1541-1554.

- Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28:28), pp. 453-496.
- Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp. 471-481.
- Libert, T. 2015. "Privacy Implications of Health Information Seeking on the Web," *Communications of the ACM* (58:3), pp. 68-77.
- Lipset, C. H. 2015. "What If You Could Donate Your Data for Research?," *Get Healthy Stay Healthy*. Retrieved (March 25, 2018) from <http://www.gethealthystayhealthy.com/articles/electronic-health-records>
- Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. 2016. "'Cargo Cult' Science in Traditional Organization and Information Systems Survey Research: A Case for Using Nontraditional Methods of Data Collection, Including Mechanical Turk and Online Panels," *The Journal of Strategic Information Systems* (25:3), pp. 232-240.
- Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers," *Journal of the Association for Information Science and Technology* (63:4), pp. 755-776.
- Lucas Jr, H. C., Agarwal, R., Clemons, E. K., El Sawy, O. A., and Weber, B. W. 2013. "Impactful Research on Transformational Information Technology: An Opportunity to Inform New Audiences," *MIS Quarterly* (37:2), pp. 371-382.
- Maddox, T. 2015. "The Dark Side of Wearables: How They're Secretly Jeopardizing Your Security and Privacy," *Tech Republic*. Retrieved (March 25, 2018) from <http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/>
- 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.
- Mandl, K. D., Mandel, J. C., and Kohane, I. S. 2015. "Driving Innovation in Health Systems through an Apps-Based Information Economy," *Cell Systems*, (1:1), pp. 8-13.
- Marteau, T. M., Ogilvie, D., Roland, M., Suhrcke, M., and Kelly, M. P. 2011. "Judging Nudging: Can Nudging Improve Population Health?," *British Medical Journal* (342), pp. 1-5.
- Masser, B. M., White, K. M., Hyde, M. K., and Terry, D. J. 2008. "The Psychology of Blood Donation: Current Research and Future Directions," *Transfusion Medicine Reviews* (22:3), pp. 215-233.
- Mies, G. 2013. "Big Data, Philanthropy, and Health at SOCAP13," *TechSoup Global*. Retrieved (March 25, 2018) from <http://forums.techsoup.org/cs/community/b/tsblog/archive/2013/09/10/big-data-philanthropy-health-socap13.aspx>
- 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.
- Moody, G. D., Lowry, P. B., and Galletta, D. F. 2017. "It's Complicated: Explaining the Relationship between Trust, Distrust, and Ambivalence in Online Transaction Relationships Using Polynomial Regression Analysis and Response Surface Analysis," *European Journal of Information Systems* (26:4), pp. 379-413.
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76-98.
- Payne, K. 2017. "Organ Donors? Lawmaker Wants Data Donors," *WLRN*. Retrieved (March 25, 2018) from <http://wlrn.org/post/organ-donors-lawmaker-wants-data-donors>

- Petty, R. E., and Briñol P. 2010. "Attitude Change," in *Advanced Social Psychology: The State of the Science*, R. F. Baumeister and E. J. Finkel (eds.), Oxford, UK: Oxford University Press, pp. 217-259.
- Petty, R. E., and Cacioppo, J. T. 1986. *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*, New York: Springer-Verlag.
- Piersma, T. W., Bekkers, R., Klinkenberg, E. F., De Kort, W. L., and Merz, E. M. 2017. "Individual, Contextual and Network Characteristics of Blood Donors and Non-Donors: A Systematic Review of Recent Literature," *Blood Transfusion* (15:5), pp. 382-397.
- Quint, M., and Rogers, D. 2015. "What is the Future of Data Sharing: Consumer Mindsets and the Power of Brands," *Center on Global Brand Leadership Columbia Business School*. Retrieved (March 20, 2018) from <https://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing>
- Rainie, L., Kiesler, S., Kang, R., and Madden, M. 2013. "Anonymity, Privacy, and Security Online," *The Pew Research Center*. Retrieved (February 14, 2018) from <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
- Romanow, D., Cho, S., and Straub, D. 2012. "Editor's Comments: Riding the Wave: Past Trends and Future Directions for Health IT Research," *MIS Quarterly* (36:3), pp. III-A18.
- Schreiber, G. B., Schlumpf, K. S., Glynn, S. A., Wright, D. J., Tu, Y., King, M. R., Higgins, M. J., Kessler, D., Gilcher, R., Nass, C. C., Guiltinan, A. M., 2006. "Convenience, the Bane of Our Existence, and Other Barriers to Donating," *Transfusion* (46:4), pp. 545-553.
- Schwarz, N., and Clore, G. L. 2007. "Feelings and Phenomenal Experiences," in *Social Psychology: Handbook of Basic Principles*, A. Kruglanski, and E. T. Higgins (eds.), New York, U.S.: Guilford Press, pp. 385-407.
- Shaw, D. M., Gross, J. V., and Erren, T. C. 2015. "Data Donation after Death," *The Lancet* (386: 9991), pp. 340.
- Shaw, D. M., Gross, J. V., and Erren, T. C. 2016. "Data Donation after Death," *EMBO Reports: Science & Society* (17:1), pp. 14-17.
- Sheehan, K. B., and Hoy, M.G. 1999. "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns," *Journal of Advertising* (28:3), pp. 37-52.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.
- 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.
- Sojka, B. N., and Sojka, P. 2003. "The Blood-Donation Experience: Perceived Physical, Psychological and Social Impact of Blood Donation on the Donor," *Vox Sanguinis* (84:2), pp. 120-128.
- Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477-560.
- 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.
- Suárez, I. M. B., Fernández-Montoya, A., Fernández, A. R., López-Berrio, A., and Cillero-Peñuela, M. 2004. "How Regular Blood Donors Explain Their Behavior," *Transfusion* (44:10), pp. 1441-1446.
- Taylor, P. L., and Mandl, K. D. 2015. "Leaping the Data Chasm: Structuring Donation of Clinical Data for Healthcare Innovation and Modeling," *Harvard Health Policy Review* (14:2), pp. 18-21.
- Thaler, R., and Sunstein, C., 2008. *Nudge: Improving Decisions about Health, Wealth and Happiness*, New Haven: Yale University Press.
- Topol, E. 2015. *The Patient Will See You Now: The Future of Medicine is in Your Hands*, New York, NY: Basic Books.
- Tucker, C. E. 2014. "Social Networks, Personalized Advertising, and Privacy Controls," *Journal of Marketing Research* (51:5), pp. 546-562.
- Van Dongen, A. 2015. "Easy Come, Easy Go. Retention of Blood Donors," *Transfusion Medicine* (25:4), pp. 227-233.

- Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157-174.
- Wegener, D. T., and Petty, R. E. 1994. "Mood Management across Affective States: The Hedonic Contingency Hypothesis," *Journal of Personality and Social Psychology* (66:6), pp. 1034-1048.
- Weintraub, A. 2015. "This Website Invites You to Donate Your Body to Science without Having to Die," *Forbes*. Retrieved (March 25, 2018) from <https://www.forbes.com/sites/arleneweintraub/2015/03/27/open-humans-network-invites-everyone-to-share-their-personal-health-data/#36fda5cc4441>
- Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431-453.
- Westin, A. F. 2005. "American Attitudes on Health Care and Privacy," *I-WAYS, Digest of Electronic Commerce Policy and Regulation* (28:2), pp. 79-84.
- Williams, R. 2012. "Using the Margins Command to Estimate and Interpret Adjusted Predictions and Marginal Effects," *The Stata Journal* (12:2), pp. 308-331.
- Willison, D. J., Steeves, V., Charles, C., Schwartz, L., Ranford, J., Agarwal, G., Cheng, J., and Thabane, L. 2009. "Consent for Use of Personal Information for Health Research: Do People with Potentially Stigmatizing Health Conditions and the General Public Differ in Their Opinions?," *BMC Medical Ethics* (10:10), pp. 1-12.
- Yun, H., Lee, G., and Kim, D. 2014. "A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.

APPENDIX A: EXPERIMENT 1

Appendix A.1 Experiment 1's Instrument

Baseline Mood (Dickert et al. 2011)

How do you feel at this moment?

| | | |
|---------------|-------|--------------|
| 1 Terrible | | 7 Delightful |
| 1 Unhappy | | 7 Happy |
| 1 Not content | | 7 Content |
| 1 Bad | | 7 Good |

Introduction to Datadonors

Datadonors provides a database that can be used by researchers, scientists, and physicians around the world to advance scientific research that can improve health and well-being.

We have developed a mobile app "datadonors" to enable individuals donate their health data in a simple way.

We would like you to view several screenshots of the app and tell us your opinion about it by answering a number of questions.

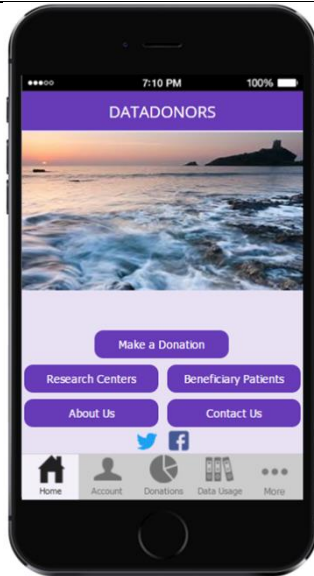
Screen Mockups of Datadonors

This is the "Home" screen of the "datadonors" app.

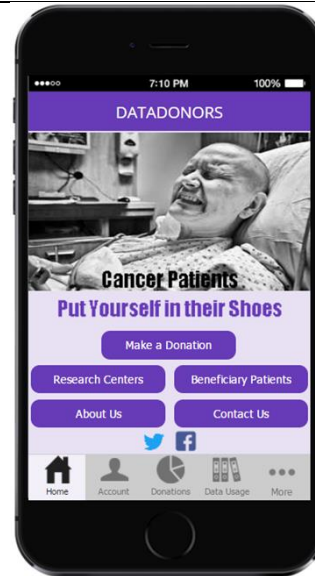
The "Home" screen has five buttons including a button for making a donation.

The bottom tab enables you to view your account information, total amount of donations, information about the use of donated data, and the "More" tab includes other functions.

Empathic Concern (Control Group)



Empathic Concern (Treatment Group)



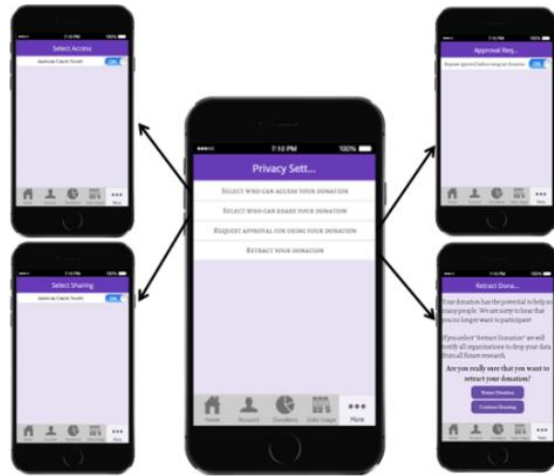
Next, all participants were asked to view several screens of the datadonors app (e.g., profile, account, and donation screens), among which we manipulated privacy controls and empathic concern.

Privacy Controls Manipulation

Privacy Controls (Control Group)

Privacy Controls (Treatment Group)

No Screens for Privacy Controls



Participants in this group viewed a total of five screens: 1) privacy settings main menu screen, and a screen for each feature provided in the privacy settings main menu: 2) select/unselect who can access donated data, 3) select/unselect who can share donated data, 4) request approval before any organization can use donated data, and 5) retract data donations. The five screens were presented one by one using a much larger size and clarity than they appear here.

Empathic Concern Manipulation

Next, we would like you to give us your opinion on some features we added to the "Home" screen.

Mainly, we added two images to the "Home" screen.

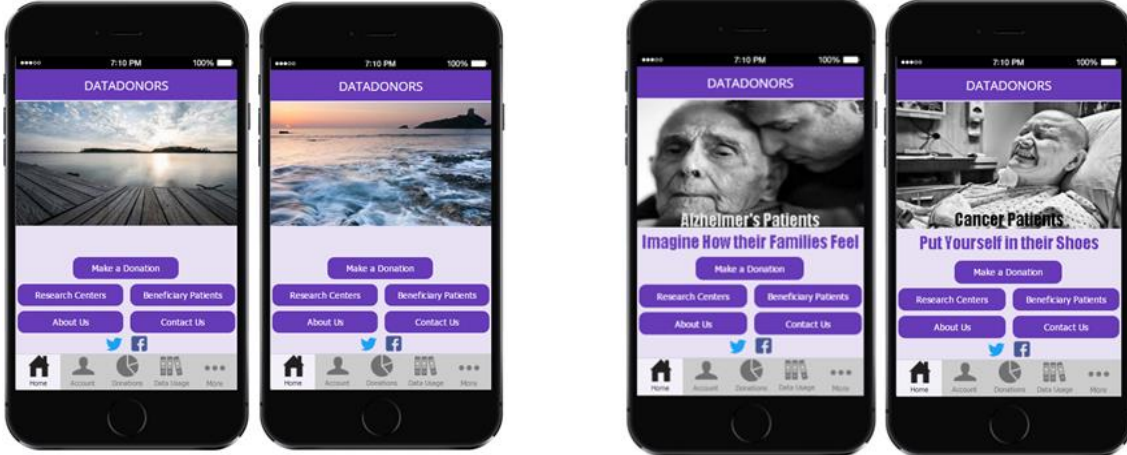
In a real mobile medium, each image is displayed for 5 seconds in a dynamic fashion. In order to simulate the real mobile medium, we will have you view each image for 5 seconds.

We are interested in how you view these images and the overall look of the "Home" screen.

Take at least 5 seconds viewing the "Home" screen and then you will be asked a number of questions.

Empathic Concern (Control Group)

Empathic Concern (Treatment Group)



Empathic Concern Manipulation Checks (Batson 2011)

Please indicate how much you have experienced each of the emotional adjectives while viewing the "Home" screen. (1 Not at all ... 9 Very much)

- Moved
- Softhearted
- Sorrowed
- Touched
- Empathic
- Warm
- Concerned
- Compassionate
- Sympathetic
- Tender
- Kind

Data Donation Decision

It is very hard or even impossible to help patients directly. For those wishing to help, they can volunteer by donating their personal health data. With more data, medical researchers will be better able to discover the real causes and effects of many diseases/disorders. However, data about different facets of people's lives are needed because such data are necessary input to find effective cures. If you wish to help, you can volunteer by donating your personal health data.

We would like to let you know that the data you donate will be completely anonymous and made available only to licensed health researchers at participating institutions. Your personal data will never be shared with or sold to third parties.

Below is a list of data categories that you can donate. These categories are exactly the same as those listed in the app. See the screenshots below.



In the next page, for each category, select “Yes” if you would like to donate and select “No” if you would not like to donate.

After you make selections, at the end of this survey, you will be given some guidelines about completing your donation.

I would like to donate data about my demographics:

- | | | |
|--------------------|-----|----|
| Gender | Yes | No |
| Birthdate | Yes | No |
| Ethnicity | Yes | No |
| Education | Yes | No |
| Work experience | Yes | No |
| Sexual orientation | Yes | No |

I would like to donate data about my basic health:

- | | | |
|-------------|-----|----|
| Height | Yes | No |
| Weight | Yes | No |
| Blood type | Yes | No |
| Vaccination | Yes | No |
| Sleep | Yes | No |

I would like to donate data about my medical history:

- | | | |
|-------------------------|-----|----|
| Benign chronic diseases | Yes | No |
| Risky chronic diseases | Yes | No |
| Family health history | Yes | No |
| Drug use | Yes | No |

| | | |
|--|-----|----|
| Surgeries | Yes | No |
| Allergies | Yes | No |
| I would like to donate data about my lifestyle: | | |
| Drinking | Yes | No |
| Smoking | Yes | No |
| Exercise | Yes | No |
| Social media use | Yes | No |
| Diet | Yes | No |
| Emotions | Yes | No |

Qualitative Feedback

If you decided to donate only some data or decided to donate nothing, please tell us why:

Answer: _____

Privacy Controls Manipulation Checks (Li et al. 2014)

Based on the screens you viewed, indicate whether you agree or disagree with the following statements. (7-point Likert Scale)

- I will have control over who can access my donated data.
- I will have control over who can share my donated data with other parties.
- I will have control over how my donated data are used by organizations.
- I will have full control over my donated data provided to datadonors.
- I will be able to retract my donation.

Post-Donation Mood (Dickert et al. 2011)

How do you feel at this moment?

- | | | |
|---------------|-------|--------------|
| 1 Terrible | | 7 Delightful |
| 1 Unhappy | | 7 Happy |
| 1 Not content | | 7 Content |
| 1 Bad | | 7 Good |

Perceived Sensitivity of Donation Items

Below is the same list of data we asked you to donate.

Please rate the sensitivity of donating each of these items. (1 Not sensitive at all ... 7 Extremely sensitive)

Donating demographics data:

- Gender
- Birthdate
- Ethnicity
- Education
- Work experience
- Sexual orientation

Donating basic health data:

- Height
- Weight
- Blood type
- Vaccination
- Sleep

Donating medical history data:

- Benign chronic diseases
- Risky chronic diseases
- Family health history
- Drug use

Surgeries
Allergies

Donating lifestyle data:

Drinking
Smoking
Exercise
Social media use
Diet
Emotions

Privacy Concerns (Dinev and Hart 2006)

For each of the following, please indicate how much you agree or disagree with the statement. (7-point Likert Scale)

I am concerned that the data I donate to datadonors could be misused.
I am concerned that others can find private information about me from datadonors.
I am concerned about donating my data to datadonors, because of what others might do with it.
I am concerned about donating my data to datadonors, because it could be used in a way I did not foresee.

Trust (Moody et al. 2017)

For each of the following, please indicate how much you agree or disagree with the statement. (7-point Likert Scale)

I believe that datadonors would act in my best interest.
If I required help, datadonors would do its best to help me.
Datadonors is interested in my well-being, not just its own.
Datadonors would be competent and effective in utilizing donated data.
Datadonors would perform its role of providing opportunities for donated data very well.
Overall, datadonors would be a capable and proficient donation organization.
In general, datadonors would be very knowledgeable about handling donations.
Datadonors would be truthful in its dealings with my data.
I would characterize datadonors as honest.
Datadonors would keep its commitments.
Datadonors would be sincere and genuine.

Altruism (Anderson and Agarwal 2011)

Please indicate how much you agree or disagree with the following statements. (5-point Likert Scale)

Helping others is one of the most important aspects of life.
I enjoy working for the welfare of others.
My family tends to do what we can to help those less fortunate than ourselves.
I agree with the old saying, "It is better to give than to receive".

Privacy invasion Experience (Anderson and Agarwal 2011)

How frequently have you personally been the victim of what you felt was an improper invasion of privacy?

(1 Very infrequently ... 7 Very frequently)

Media Exposure of Health Data Misuse (Anderson and Agarwal 2011)

How much have you heard or read during the last year about the use and potential misuse of health information collected electronically?

(1 Not at all ... 7 Very much)

Doctor Visits (Anderson and Agarwal 2011)

How frequently do you schedule doctor appointments for yourself?

More than once a month

Every 1 to 2 months

Every 3 to 6 months

Every 7 to 12 months

Less than once a year

Health Status (Anderson and Agarwal 2011)

How would you rate your health status?

(Poor, fair, good, very good, excellent)

Appendix A.2 Experiment 1's Measurement Validation

Exploratory Factor Analysis

Extraction method: maximum likelihood with varimax rotation

| | $\alpha = .968$ | $\alpha = .968$ | $\alpha = .975$ | $\alpha = .949$ | $\alpha = .888$ |
|--------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Trust 1 | .769 | -.217 | .210 | .144 | .248 |
| Trust 2 | .717 | -.117 | .147 | .162 | .222 |
| Trust 3 | .695 | -.078 | .149 | .125 | .283 |
| Trust 4 | .792 | -.199 | .255 | .007 | .115 |
| Trust 5 | .802 | -.185 | .245 | -.003 | .220 |
| Trust 6 | .844 | -.154 | .246 | .053 | .191 |
| Trust 7 | .772 | -.209 | .277 | .026 | .233 |
| Trust 8 | .844 | -.195 | .220 | .141 | .089 |
| Trust 9 | .794 | -.251 | .226 | .124 | .122 |
| Trust 10 | .881 | -.233 | .158 | .078 | .049 |
| Trust 11 | .858 | -.203 | .195 | .160 | .082 |
| Privacy Concerns 1 | -.290 | .852 | -.217 | -.069 | .008 |
| Privacy Concerns 2 | -.269 | .884 | -.202 | -.085 | -.034 |
| Privacy Concerns 3 | -.258 | .916 | -.175 | -.067 | .001 |
| Privacy Concerns 4 | -.305 | .880 | -.152 | -.052 | -.081 |
| Post-Donation Mood 1 | .391 | -.198 | .836 | .039 | .117 |
| Post-Donation Mood 2 | .372 | -.218 | .871 | .073 | .111 |
| Post-Donation Mood 3 | .383 | -.240 | .828 | .027 | .037 |
| Post-Donation Mood 4 | .356 | -.194 | .855 | .008 | .092 |
| Baseline Mood 1 | .167 | -.051 | .069 | .863 | .207 |
| Baseline Mood 2 | .135 | -.021 | .015 | .901 | .236 |
| Baseline Mood 3 | .092 | -.075 | -.009 | .890 | .106 |
| Baseline Mood 4 | .067 | -.083 | .043 | .895 | .108 |
| Altruistic Personality 1 | .268 | .064 | .062 | .102 | .810 |
| Altruistic Personality 2 | .205 | -.080 | .084 | .176 | .828 |
| Altruistic Personality 3 | .153 | -.073 | .043 | .196 | .682 |
| Altruistic Personality 4 | .198 | .008 | .081 | .158 | .798 |

Appendix A.3 Experiment 1's Additional Statistical Analyses

| Dependent Variable: Amount of Data Donation | Model 1 | Model 2 | Model 3 |
|---|------------------------|------------------------|------------------------|
| | β (robust s. e.) | β (robust s. e.) | β (robust s. e.) |
| Constant | 11.591*** (1.47) | -4.686 (5.64) | -5.064 (2.86) |
| Empathy (induced) | .797 (2.03) | 1.018 (1.89) | 1.289 (1.67) |
| PrivacyControls (provided) | 1.205 (1.96) | -1.101 (1.80) | -1.670 (1.72) |
| PrivacyConcerns | -4.845*** (.75) | -3.286** (.98) | -2.816** (.87) |
| EmpathyXPrivacyControls | -.784 (2.78) | .711 (2.44) | .839 (2.33) |
| PrivacyControlsXPrivacyConcerns | 2.974** (.95) | 2.222* (1.06) | 2.003* (.95) |
| EmpathyXPrivacyConcerns | 2.549* (.98) | 2.625** (.96) | 2.628** (.90) |
| EmpathyXPrivacyControlsXPrivacyConcerns | -4.569** (1.37) | -3.26* (1.35) | -3.264* (1.29) |
| Control Variables | | | |
| Trust | - | 3.515*** (.68) | 3.895*** (.54) |
| Mood | - | 1.476*** (.31) | 1.411*** (.29) |
| AltruisticPersonality | - | .302 (.73) | - |
| HealthDataMisuseMediaExposure | - | .222 (.34) | - |
| PrivacyInvasionExperience | - | .592 (.42) | - |
| DoctorVisits | - | -.621 (.53) | - |
| HealthStatus | - | .534 (.67) | - |
| Age | - | -.039 (.05) | - |
| Female | - | -.478 (1.32) | - |
| White | - | -.459 (1.36) | - |
| F value | (7, 131) 13.76*** | (17, 114) 14.80*** | (9, 129) 30.12*** |
| R ² (Adjusted R ²) | 27.74% (23.87%) | 56.57% (50.09%) | 54.63% (51.46%) |
| N | 139 | 132 | 139 |

* $p < .05$; ** $p < .01$; *** $p < .001$

- PrivacyConcerns was mean centered before creating the interaction terms.

- A higher score on trust and mood reflects a trusting belief in the data donation app and a positive mood state after making a donation.

- F test shows that the control variables in Model 2 (altruistic personality, health data misuse media exposure, privacy invasion experience, doctor visits, health status, age, female, and white) are jointly insignificant $F(8, 114) = .83, p > .05$. Therefore, we remove them and use Model 3 for the final analysis as it has a significantly better fit compared with Model 2.

APPENDIX B: EXPERIMENT 2

Appendix B.1 Experiment 2's Instrument

The instrument for experiment 2 was exactly similar to that used for experiment 1 with some exceptions. First, all participants viewed the app version in which the home screen included images of cancer and Alzheimer's patients (i.e., empathy induced) (see Appendix A.1). Second, all participants viewed the app version in which the privacy controls were provided (see Appendix A.1). Third, we manipulated ease of donation and social nudging (as shown below) and included a number of manipulation check items for these new manipulations. Fourth, we measured perceived control over the donation method.

| Ease of Donation Manipulation | |
|--|---|
| Manual Donation Method | Automatic Donation Method |
| <p>Donating data through datadonors takes <u>some time and effort</u> because the donation process is <u>manual</u>.</p> <p>You have to choose the data you would like to donate.</p> <p>Then, <u>you have to enter the data manually for each category</u>.</p> <p>This <u>manual</u> donation method requires you to put <u>some</u> effort in entering the data and it takes <u>about 45 minutes</u>.</p> | <p>Donating data through datadonors takes a <u>few seconds with no effort</u> because the donation process is <u>automatic</u>.</p> <p>You <u>just</u> have to choose the data you would like to donate.</p> <p>Then, <u>the datadonors app will do the heavy work by searching and capturing the data from other apps</u>.</p> <p>This <u>automatic</u> donation method requires you to put <u>no</u> effort in entering the data and it takes <u>a few seconds only</u>.</p> |

Ease of Donation Manipulation Checks

Indicate whether you agree or disagree with the following statements. (7-point Likert Scale)

- It is easy to donate data through the datadonors app.
- It is convenient to make a data donation through the datadonors app.
- Donating data through the datadonors app requires minimal effort.
- Donating data through the datadonors app is quick.
- Donating data through the datadonors app takes a few seconds.
- Donating data through the datadonors app is not time consuming.

Perceived Control over the Donation Method

Indicate whether you agree or disagree with the following statements. (7-point Likert Scale)

- I will have control over the method through which I enter my data.
- I will have control in terms of how I donate my data.
- I will have control over how the data is entered.

Social Nudging Manipulation

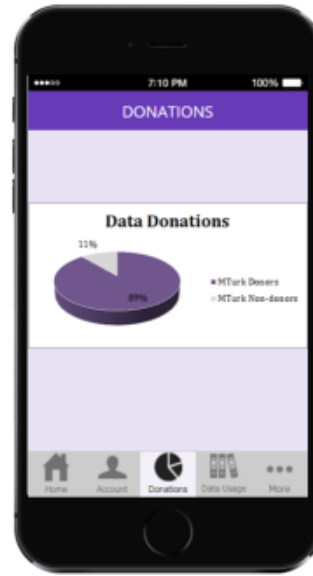
Low Social Nudge

So far, based on the data we have collected from Amazon Mechanical Turk (MTurk) workers, **11%** of the participants decided to donate their data. If you decide to donate, you will help datadonors reach its goal.



High Social Nudge

So far, based on the data we have collected from Amazon Mechanical Turk (MTurk) workers, **89%** of the participants decided to donate their data. If you decide to donate, you will help datadonors reach its goal.



Social Nudging Manipulation Checks

Indicate whether you agree or disagree with the following statements. (7-point Likert Scale)

It seems that many people have decided to donate their data.

It seems that many people are in favor of this data donation initiative.

Appendix B.2 Experiment 2's Measurement Validation

Exploratory Factor Analysis

Extraction method: maximum likelihood with varimax rotation

| | $\alpha = .968$ | $\alpha = .973$ | $\alpha = .953$ | $\alpha = .885$ | $\alpha = .822$ | $\alpha = .967$ |
|--------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Trust 1 | .737 | .243 | .029 | .113 | .064 | .255 |
| Trust 2 | .668 | .230 | .135 | .113 | .061 | .214 |
| Trust 3 | .663 | .210 | .223 | .160 | .046 | .198 |
| Trust 4 | .808 | .170 | .084 | .206 | .099 | .166 |
| Trust 5 | .806 | .159 | .058 | .190 | .067 | .202 |
| Trust 6 | .794 | .186 | .077 | .238 | .082 | .148 |
| Trust 7 | .791 | .169 | .055 | .171 | .008 | .140 |
| Trust 8 | .864 | .187 | .164 | .086 | -.070 | .101 |
| Trust 9 | .884 | .224 | .103 | .113 | .050 | .092 |
| Trust 10 | .899 | .199 | .090 | .151 | .072 | .073 |
| Trust 11 | .854 | .212 | .007 | .100 | .051 | .100 |
| Privacy Concerns 1 | -.404 | .831 | -.052 | -.012 | -.002 | -.180 |
| Privacy Concerns 2 | -.375 | .843 | -.097 | -.059 | -.006 | -.090 |
| Privacy Concerns 3 | -.361 | .882 | -.043 | -.055 | -.036 | -.156 |
| Privacy Concerns 4 | -.332 | .889 | -.053 | .009 | .000 | -.110 |
| Baseline Mood 1 | .122 | .055 | .885 | -.052 | .172 | .054 |
| Baseline Mood 2 | .152 | .074 | .931 | .016 | .135 | -.007 |
| Baseline Mood 3 | .082 | .052 | .873 | .070 | .132 | .097 |
| Baseline Mood 4 | .139 | .027 | .886 | .061 | .134 | .095 |
| Perceived Control 1 | .169 | .020 | .040 | .722 | .298 | .129 |
| Perceived Control 2 | .265 | -.009 | .038 | .846 | .133 | .063 |
| Perceived Control 3 | .213 | .111 | .089 | .815 | .233 | .113 |
| Altruistic Personality 1 | .064 | .045 | .091 | .164 | .741 | .041 |
| Altruistic Personality 2 | .044 | .045 | .061 | .149 | .806 | .104 |
| Altruistic Personality 3 | .034 | .004 | .191 | .121 | .678 | .067 |
| Altruistic Personality 4 | .037 | -.048 | .146 | .155 | .617 | .024 |
| Post-Donation Mood 1 | .531 | .213 | .156 | .226 | .160 | .674 |
| Post-Donation Mood 2 | .518 | .251 | .138 | .233 | .138 | .699 |
| Post-Donation Mood 3 | .522 | .253 | .154 | .229 | .144 | .658 |
| Post-Donation Mood 4 | .515 | .204 | .059 | .238 | .128 | .701 |

Appendix B.3 Experiment 2's Additional Statistical Analyses

| Dependent Variable: Amount of Data Donation | Model 1 | Model 2 | Model 3 |
|---|------------------------|------------------------|------------------------|
| | β (robust s. e.) | β (robust s. e.) | β (robust s. e.) |
| <i>Constant</i> | -5.000 (3.707) | -12.069* (5.68) | -8.217 (4.22) |
| <i>EaseOfDonation (automatic)</i> | 3.741* (1.43) | 4.430** (1.47) | 4.047** (1.41) |
| <i>Social Nudge (high)</i> | 1.386 (1.75) | 1.500 (1.77) | 1.726 (1.70) |
| <i>PrivacyConcerns</i> | -2.562*** (.35) | -1.630** (.47) | -1.699*** (.47) |
| <i>EaseOfDonationXSocialNudge</i> | -1.610 (2.32) | -2.361 (2.22) | -2.019 (2.16) |
| <i>EaseOfDonationXPrivacyConcerns</i> | .936* (.46) | 1.208* (.56) | 1.063* (.53) |
| <i>SocialNudgeXPrivacyConcerns</i> | .825 (.71) | 1.134 (.71) | 1.090 (.72) |
| <i>EaseOfDonationXSocialNudgeXPrivacyConcerns</i> | -2.307* (1.01) | -2.454* (.96) | -2.309* (.98) |
| <i>PerceivedControl</i> | 2.769*** (.58) | 1.067 (.71) | 1.437* (.65) |
| Control Variables | | | |
| <i>Trust</i> | - | 2.072** (.71) | 2.247** (.69) |
| <i>Mood</i> | - | 1.133** (.40) | 1.005** (.37) |
| <i>AltruisticPersonality</i> | - | 2.015* (.87) | - |
| <i>HealthDataMisuseMediaExposure</i> | - | -.122 (.35) | - |
| <i>PrivacyInvasionExperience</i> | - | -.142 (.40) | - |
| <i>DoctorVisits</i> | - | .001 (.55) | - |
| <i>HealthStatus</i> | - | -.154 (.68) | - |
| <i>Age</i> | - | .023 (.05) | - |
| <i>Female</i> | - | -1.451 (1.24) | - |
| <i>White</i> | - | .463 (1.41) | - |
| <i>F value</i> | (8, 168) 28.67*** | (18, 157) 17.50*** | (10, 166) 27.61*** |
| <i>R² (Adjusted R²)</i> | 34.08% (30.95%) | 45.07% (38.77%) | 43.12% (39.69%) |
| <i>N</i> | 177 | 176 | 177 |

* $p < .05$; ** $p < .01$; *** $p < .001$

- *PrivacyConcerns* was mean centered before creating the interaction terms.

- A higher score on trust and mood reflects a trusting belief in the data donation app and a positive mood state after making a donation.

- *F* test shows that the control variables in Model 2 (altruistic personality, health data misuse media exposure, privacy invasion experience, doctor visits, health status, age, female, and white) are jointly insignificant $F(8, 157) = .87, p > .05$. Therefore, we remove them and use Model 3 for the final analysis as it has a significantly better fit compared with Model 2.

APPENDIX: REFERENCES

- Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469-490.
- Batson, C. D. 2011. *Altruism in Humans*. Oxford University Press, USA.
- Dickert, S., Sagara, N., and Slovic, P. 2011. "Affective Motivations to Help Others: A Two-Stage Model of Donation Decisions," *Journal of Behavioral Decision Making* (24:4), pp. 361-376.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80,100.
- Li, H., Gupta, A., Zhang, J., and Sarathy, R. 2014. "Examining the Decision to Use Standalone Personal Health Record Systems as a Trust-Enabled Fair Social Contract," *Decision Support Systems* (57), pp. 376-386.
- Moody, G. D., Lowry, P. B., and Galletta, D. F. 2017. "It's Complicated: Explaining the Relationship between Trust, Distrust, and Ambivalence in Online Transaction Relationships Using Polynomial Regression Analysis and Response Surface Analysis," *European Journal of Information Systems* (26:4), pp. 379-413.

CHAPTER 5

Conclusion

The main objective of this dissertation was to explain the privacy paradox in order to present a deeper understanding of the causal link between privacy concerns and disclosure behaviors. This objective was motivated by the lack of knowledge about the conditions under which the privacy paradox might be observed. The novelty of the dissertation lies in its systematic approach to test and explain the privacy paradox along with its presentation of empirical evidence based on both qualitative and quantitative research methods.

It is noteworthy that evidence for the privacy paradox was supported across a multitude of different contexts. The contexts used are not only different but they represent areas in which people today have to be especially concerned about their personal information. The fact that the privacy paradox emerged in these contexts by manipulating a simple cue in the participants' minds presents important theoretical and practical implications. The existing literature suggests that the privacy paradox is more prevalent in the social media context. This dissertation suggests that it may not be the context that drives privacy paradoxical decisions. Rather, it is more likely the conditions that individuals experience before they make disclosure decisions. Therefore, the privacy paradox may not be caused by the nature of the context in which privacy decisions are made, but rather by the situational or conditional factors experienced at the individual level.

Individuals should be cognizant of such conditional factors, particularly those that act in the subconscious mind (e.g., positive mood and empathic concern), as they could lead to making uninformed privacy decisions. For example, when individuals browse Facebook, they tend to view positive contents posted by their friends. In most cases, however, individuals are unaware that such behavior, while it boosts their mood state, it would also lead them to make unintended revelations of personal preferences (e.g., reacting to a sensitive funny post). Similarly, while reading an engaging and uplifting news article on a news website, individuals experience cognitive absorption and as a result they might be more likely to participate in a random survey that pops up on the news website. By participating in such a survey, individuals would be more likely to reveal personal information which they would rather withhold if they were not cognitively absorbed. These two examples demonstrate that it is probably not the context

(Facebook vs. a news website) that may lead to privacy paradoxical behaviors, but rather it is the conditions experienced by individuals. In the next sections, I provide a summary of the conditions examined in this dissertation and I conclude with general policy implications and I introduce the concept of privacy intelligence as a new research program for future research.

SUMMARY OF BOUNDARY CONDITIONS AND GUIDELINES FOR FUTURE RESEARCH

Reflecting back on the overarching research question (*under what conditions do dispositional privacy concerns exhibit weak influence on disclosure behaviors?*), this dissertation presents a total of seven conditions under which dispositional privacy concerns have weak or insignificant effects on disclosure behaviors. The first research essay indicates that under the condition of high cognitive absorption, individuals tend to overlook their privacy concerns when disclosing personal information in the context of social media. As a result, the privacy paradox can be explained through cognitive absorption.

Boundary Condition #1: *The privacy paradox is likely to be observed when individuals are cognitively absorbed.*

The second research essay shows that under the condition of a depleted cognitive resource or a positive mood state, both of which can trigger low-effort cognitive processing, individuals are also unable to act on their privacy concerns when they encounter requests for personal information. Therefore, the privacy paradox can be explained through cognitive resource depletion or positive mood state.

Boundary Condition #2: *The privacy paradox is likely to be observed when individuals are cognitively depleted.*

Boundary Condition #3: *The privacy paradox is likely to be observed when individuals are experiencing a positive mood state.*

Using the context of data donation, the third research essay suggests that individuals, when asked to disclose their personal information, relax their privacy concerns when they are able to control their private information via privacy controls, when they find convenience in the disclosure decision, or when they exhibit feelings of empathic concern. Thus, the privacy paradox can be explained through privacy controls, convenience, or empathic concern.

Boundary Condition #4: *The privacy paradox is likely to be observed when individuals are able to control their private information via privacy controls.*

Boundary Condition #5: *The privacy paradox is likely to be observed when individuals find convenience in the disclosure decision.*

Boundary Condition #6: *The privacy paradox is likely to be observed when individuals exhibit feelings of empathic concern.*

The third research essay also shows that social influence (manipulated by a simple social nudge which shows that the majority of people disclose their personal information) can lead individuals to overlook their privacy concerns particularly in the absence of a convenient disclosure context. However, such social influence can backfire in the presence of a convenient disclosure context leading individuals to act on their privacy concerns when asked to disclose their personal information. Therefore, the privacy paradox manifests in the former condition but disappears in the latter condition.

Boundary Condition #7: *The privacy paradox is likely to be observed when individuals are influenced by an encouraging social nudge, particularly in the absence of a convenient disclosure context.*

These explanations advance the privacy literature and provide explicit illustration of the causes of the privacy paradox phenomenon. The systematic approach followed in this work will hopefully guide future research toward a deeper understanding of privacy decisions while contributing to enhancing privacy policies, organizational privacy practices, and individuals' privacy decisions.

CONCLUDING REMARKS ABOUT POLICY IMPLICATIONS: TOWARD A PRIVACY INTELLIGENCE PERSPECTIVE

An intriguing question arises after learning about individuals' intentions and behaviors in privacy decisions: Is it even possible for individuals to make privacy decisions that are consistent with their privacy concerns, given that today's digital environment is designed in a way to limit cognitive processing (e.g., positive images and videos, immersive websites, and an endless number of nudges)? My answer is that in the present environment it is very unlikely that individuals will be able to completely align their privacy concerns with their privacy decisions. Nevertheless, let's assume that it is possible to reverse the privacy paradox such that individuals' privacy concerns become consistent with their privacy

decisions. In this case, online companies are very likely to find such endeavor undesirable as they seek to collect as much personal data as possible to improve their business. Data is the new oil, at least as of today. Given online companies' increasing desire to utilize personal data and individuals' increasing need for online services, it is very unlikely that online companies will start initiatives to make privacy concerned individuals limit their disclosure behaviors. In fact, it is likely that online companies might do just the opposite (e.g., apply more interventions to increase disclosure behaviors). Thus, even if behavioral research presents novel techniques and interventions that will enable individuals to be consistent in their privacy decisions, online companies will not be interested in implementing them. Involving governmental regulators (e.g., the federal trade commission, FTC) might seem to be the right path to go; however, history suggests otherwise as the industry groups participating in developing privacy policies undertaken by governmental agencies are very powerful in driving such policies. As a result, industry and governmental initiatives are not likely to be effective. This leaves us with individuals. In other words, individuals will have to train themselves to make informed privacy decisions (i.e., making privacy decisions that are consistent with their level of privacy concern). Yet, we know that individuals can be easily manipulated by the context in which they make privacy decisions. My proposal is that it is time to pay less attention to privacy concerns and to start focusing on enhancing individuals' privacy intelligence.

To a large extent, the privacy literature in the past twenty years has focused on studying privacy concerns and how such concerns influence privacy decisions. However, this scholarly work has come at the expense of deeper understanding of privacy-related decision-making. I believe that the construct of privacy concerns misses the full context of individuals' privacy-related decision-making processes and that it should be replaced by a *privacy intelligence quotient* (PQ)—that is, mental and behavioral capabilities that guide individuals' privacy decisions. In particular, rather than simply examining privacy decisions from a privacy concerns perspective, it is more important and useful to study why some people function more effectively than others as they make privacy decisions. It is time to consider a broader but

more nuanced view of the processes involved in privacy decisions and the concept of PQ, in my view, is the way to proceed.

To make informed privacy decisions, individuals need to have sufficient knowledge about privacy practices, to be motivated to protect their privacy, and to regularly employ privacy-protective behaviors. I argue that these cognitive and behavioral capabilities (i.e., PQ) represent the main mechanism through which users make privacy decisions. This new construct should enable us to understand what individuals do at the action level (e.g., when they make a disclosure decision) rather than what they think (e.g., whether or not they are privacy concerned). Privacy intelligence reflects cognitive and behavioral capabilities pertaining to privacy decisions and not privacy concerns, *per se*. Privacy intelligence is not specific to a particular context and it evolves over time as individuals' cognitive and behavioral capabilities develop. Privacy intelligence is a dynamic construct that continues developing as individuals acquire experience with privacy-related issues in different contexts. Privacy intelligent individuals are adept at employing privacy protective strategies and therefore they can still enjoy disclosing a high amount of personal information as long as the disclosure behavior is an informed one or protected. In other words, their disclosure behaviors are appropriate in the sense that minimal to no potential risks are expected after sharing private information. In addition, individuals with a high level of privacy intelligence are aware of the contextual cues and nudges that may shape their privacy decisions and are capable of making informed privacy decisions even in the existence of such contextual factors.

I believe that future privacy research should invest in studying the construct of PQ because it has a potential to help us understand privacy decisions from a broad, nuanced, and novel perspective. It has a potential not only to explain and predict but also to enhance individuals' privacy decisions. Notably, future generations will be much more attached to technological revolutions (e.g., Internet-of-Things, Artificial Intelligence, and robots). The PQ concept can contribute to developing and evaluating novel privacy educational programs whose mission is to enhance individuals' privacy awareness and behaviors. Such a research program will potentially have a significant impact on individuals, societies, and public policies.