UNIVERSITY OF CALIFORNIA

Santa Barbara

Privacy decisions on SNSs:
An exploration of cognitive heuristics

A dissertation submitted in partial satisfaction of the

requirements for the degree Doctor of Philosophy

in Communication

by

Ji Young Suh

Committee in charge:

Professor Miriam J. Metzger, Chair

Professor Ronald E. Rice

Professor Joseph B. Walther

June 2020

The dissertation of Ji Young Suh is approved.

_____

Ronald E. Rice

_____

Joseph B. Walther

_____

Miriam J. Metzger, Committee Chair

May 2020

Privacy decisions on SNSs:

An exploration of cognitive heuristics

ACKNOWLEDGEMENTS

I am eternally grateful for my advisor Miriam Metzger's mentorship, guidance, and endless support, which helped me grow as a researcher and complete a dissertation during a pandemic. I am also thankful for invaluable and thoughtful feedback from my committee members, Ron Rice and Joe Walther. I feel very fortunate to have had continuous emotional and social support from friends, family, and beautiful Californian nature throughout my time at UCSB.

JI YOUNG SUH

Department of Communication, University of California, Santa Barbara
3311 Social Sciences & Media Studies (SSMS), Santa Barbara, CA 93106
jennsuh.net|suh@ucsb.edu

EDUCATION

University of California, Santa Barbara, Ph.D. Communication, anticipated 2020
Research areas: privacy, information sharing, human-computer interaction (HCI)

University of California, Santa Barbara, M.A. Communication, 2016
Master's Thesis: *Comparative Optimism About Privacy Risks on SNSs*

Northwestern University, B.S. Communication Studies, 2014
Honors Thesis: *What They Think vs. What They Do: Online Privacy Management via Different Devices in Different Locations*
Departmental honors, Magna Cum Laude
Study abroad program at Sciences Po. (L'Institut d'études politiques de Paris), Fall 2012

PUBLICATIONS

1. Metzger, M. J., & Suh, J. J. (2017). Comparative optimism about privacy risks on Facebook. *Journal of Communication, 67*(2). http://doi.org/10.1111/jcom.12290
2. Suh, J. J., & Hargittai, E. (2015). Privacy management on Facebook: Do device type and location of posting matter? *Social Media + Society*, *1*(2), 1-11. http://doi.org/10.1177/2056305115612783

REFEREED CONFERENCE PROCEEDING

1. Suh, J. J., Metzger, M. J., Reid, S., & El Abbadi, A. (2018). Distinguishing group privacy from personal privacy: The effect of group inference technologies on privacy perceptions and behaviors. The 21st ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW), Jersey City, NJ.

BOOK CHAPTER

1. Metzger, M. J., Suh, J.J., Reid, S., & El Abbadi, A. (in press). What can fitness apps teach us about group privacy? In. S. Devjani, & R. Ahmed (Eds.), *Privacy concerns surrounding personal information sharing on health and fitness mobile applications*. IGI Global.

CONFERENCE PAPERS

1. Suh, J. J., & Metzger, M. J. (2019). Privacy decision-making on social network sites: The role of heuristics. International Communication Association (ICA), Washington, D.C.
2. Suh, J. J., & Metzger, M. J. (2017). Comparative optimism about privacy risks on social network sites. International Communication Association (ICA), San Diego, CA.

RESEARCH WORKSHOP PAPERS

1. Suh, J. J., & Metzger, M. J. (2018). Privacy heuristics on social network sites. CSCW Workshop on Privacy in Context, Jersey City, NJ.
2. Suh, J. J. (2017). Maximizing the quality of social support and minimizing the networked privacy risk. CSCW Workshop on Privacy Ethics, Portland, OR.
3. Metzger, M. J., & Suh, J. J. (2015). Public perceptions of networked privacy: Past, present, and future. CSCW Workshop on the Future of Networked Privacy, Vancouver, Canada.

AWARDS & HONORS

Regent's Special International Fellowship, University of California, Santa Barbara, 2014 - 2019
Communication Studies Departmental Excellence Award, Northwestern University, 2014
Communication Century Scholar, Northwestern University, 2013
George M. Sargent Award for Academic Excellence, Northwestern University, 2011 & 2013
Delta Epsilon Iota Academic Honor Society, 2012
Lambda Pi Eta Communication Studies Honor Society, 2011

RESEARCH EXPERIENCE

LogMeIn, Inc., *User Experience Researcher (contract)*, Summers 2018 and 2019

- Proposed a new categorical system for webinars on GoToStage (video hosting website) to improve alignment between users' mental models and machine learning models.
- Developed new categories for GoToStage webinars by conducting multi-stage content analyses of textual and visual information in existing webinars.
- Interviewed users of competing online meeting software (e.g., GoToMeeting) and LogMeIn employees to understand how users develop trust to continue using the product.

NSF EAGER: Towards a Better Understanding of Group Privacy in Social Media Community Detection (PIs: Drs. Amr El Abbadi, Miriam Metzger, and Scott Reid),
Graduate Student Researcher, 2017 – present

- Designed and conducted a set of experiments to understand threats to privacy posed by technology that enables extended trending topics analysis and its implications for people's use of social media.
- Provided human-centered insights in a cross-functional team of computer scientists and HCI researchers to develop a tool that protects social media users from hashtag-related inference algorithms.
- Made design recommendations based on findings from experiments that aimed to understand privacy threats by a technology that enables extended trending topics analysis (e.g., predicting users' personal characteristics based on hashtags they use).

FlowNet at University of California, Santa Barbara (PIs: Drs. Elizabeth Belding, Miriam Metzger, Lisa Parks, and Ben Zhao), *Graduate Student Researcher*, 2016 – 2017

- Coordinated usability testing of an Android app SecurePost before and after its launch on Google Play Store by managing survey responses.

- Assisted in data synthesis and report writing on a cross-cultural research in Zambia, Turkey, and Mongolia that identified users' need for SecurePost.

Collaborative Technology Laboratory at Northwestern University (PI: Dr. Darren Gergle), *Research Assistant*, 2013

- Assisted with data collection for a lab study that assessed when people would use search engines (Google and Bing) and/or social network sites (Facebook and Twitter) for their information needs.
- Coded open-ended responses from a survey about online information seeking.

Web Use Project at Northwestern University (PI: Dr. Eszter Hargittai), *Research Assistant*, 2011-2012

- Transcribed interviews for a project that examined people's web search processes to find answers to specific health questions.
- Summarized and coded data compiled from participant interviews.

RESEARCH GRANTS

Graduate Research Grant, Department of Communication, University of California, Santa Barbara, 2018, $500.
Undergraduate Research Grant (URG), Office of Undergraduate Research, Northwestern University, 2013, $3,000.

TRAVEL GRANT

NSF CNS:SaTC: Student Travel Grants to Attend CSCW, 2017, $1,700.

TEACHING EXPERIENCE

Diffusion of Innovations (COMM 163), *Teaching Assistant*, Winter 2020
Small Group Communication (COMM 106), *Teaching Assistant*, Fall 2019
Social Media Controversies: The Good, the Bad, and the Ugly (COMM 184), *Teaching Assistant*, Spring 2019
Theories of Communication (COMM 89), *Teaching Assistant*, Winter 2019
Family Communication (COMM 124), *Teaching Assistant*, Winter 2017
Statistical Analysis for Communication (COMM 87), *Teaching Assistant*, Spring 2016 & Fall 2018
Communication Research Methods (COMM 88), *Teaching Assistant*, Fall 2016, Winter 2016, Spring 2017, & Spring 2020
Introduction to Communication (COMM 1), *Teaching Assistant*, Fall 2015

PROFESSIONAL SERVICE

DEPARTMENT OF COMMUNICATION, UNIVERSITY OF CALIFORNIA, SANTA BARBARA

Graduate Student Advisory Committee to Chair (GSACC)

PhD Candidate Representative, 2018 - 2019
PhD Student Representative, 2017 - 2018
First-Year Graduate Student Representative, 2014-2015

REVIEWING & REFEREEING

ACM CHI Conference on Human Factors in Computing Systems (CHI)
ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)
International Communication Association (ICA)
Journal of the Association for Information Science and Technology (JASIST)
Social Media + Society

LANGUAGES

English & Korean (Bilingual), French & Japanese (Advanced)

ABSTRACT

Privacy decisions on SNSs:

An exploration of cognitive heuristics

by

Ji Young Suh

By taking a mixed-methods approach, this dissertation presents results from three studies that offer both qualitative and quantitative insights into how cognitive heuristics influence users' risk perceptions and decisions about disclosure and privacy in the context of social network sites (SNSs). Findings from focus group interviews in Study 1 include numerous personal anecdotes about the effects of nine cognitive heuristics, which serve as proof-of-concept that illustrates how SNS users perceive these heuristics in relation to their disclosure and privacy decisions on SNSs. To complement the findings from the first study, Study 2A used a survey and "direct" measurement approach to examine the heuristics' effects on privacy and disclosure via SNS users' self-reported agreement with the effect of cognitive heuristics on their own decision-making processes. The findings from Study 2A help quantify and generalize the findings from Study 1 to a larger and more representative sample of SNS users. Due to the invisible and elusive nature of heuristic processes that largely occur subconsciously, Study 2B employs another survey-based study, but one that uses an "indirect" approach to measure the heuristics' effects on four different SNSs (Facebook, Instagram, Snapchat, and Twitter) to examine potential correlational relationships

between the cognitive heuristics and SNS users' decisions about disclosure and privacy and to help improve the understanding of heuristic effects and their implications for SNS users' privacy. The findings from Study 2B show that relying on cognitive heuristics (e.g., homophily heuristic, hyperbolic discounting, ephemerality heuristic, etc.) can result in negative consequences for SNS users' privacy and that the underlying mechanism for these heuristic processes cannot be easily explained in terms of fully rational cost-benefit decision models, which so far have been popular in the literature (e.g., the privacy calculus model). The findings across the three studies in this dissertation not only help gain a deeper and more nuanced understanding of heuristic effects in the context of managing privacy on SNSs, but also demonstrate the importance of expanding scholars' assumptions about human rationality when investigating privacy-related decision-making processes on SNSs. Overall, this dissertation provides results that contribute to the growing discussion about people's bounded rationality and their reliance on cognitive heuristics when making decisions about privacy in the context of SNSs and offer future directions for research that could help SNS users make more informed decisions.

TABLE OF CONTENTS

Chapter 1: Introduction to the Project

Social network sites (SNS) have become a pivotal part of human communication. Nearly 70% of U.S. adults use Facebook, and almost three quarters of them visit the site daily (Perrin & Anderson, 2019). A typical American uses three of following social platforms—Twitter, Instagram, Facebook, Snapchat, YouTube, WhatsApp, Pinterest, and LinkedIn—and as 88% of young adults who are between the ages of 18-29 report to use at least one SNS, people's adoption of SNSs will most likely continue to rise (A. Smith & Anderson, 2018). In addition to joining more SNSs, people are also generating increasing amounts of information. Every minute, Snapchat users send more than two million snaps while Twitter users share about 473,400 tweets (Cohen, 2018). This pattern in the amount of information users share on SNSs seems to suggest that users of social platforms do not care about their privacy. Since SNSs are important for engaging in many social interactions, participating in civic and political activities, and sometimes even performing job-related activities (Rainie, 2018), a recent *New York Times* op-ed pointed out that privacy is "something a lot of people are happy to trade away at a moment's notice, for the slightest reward" (Manjoo, 2019).

In contrast to how the public may discuss privacy, or how the media may portray people's online privacy concerns (Harding, 2018; Menand, 2018), the widespread use of SNSs should not be taken to indicate that people do not care about privacy. A survey conducted after Edward Snowden's revelations about government surveillance programs showed that 80% of SNS users are concerned about third parties, such as advertisers and businesses, accessing the information they share on these sites (Madden, Rainie, Zickuhr, Duggan, & Smith, 2014). Moreover, 70% of SNS users are at least somewhat concerned that the government is accessing the information they share on SNSs without their knowledge

(Madden et al., 2014). A more recent survey shows that about half (51%) of adult Facebook users in the U.S. are not comfortable with Facebook creating a list of categories about them based on information they share with the platform, and this number may actually be an underestimation since 74% of U.S. Facebook users reported that they did not know that Facebook maintained lists of their interests and traits (Hitlin & Rainie, 2019). Overall, more than 80% of U.S. adults report that they do not feel comfortable about using SNSs to share private information with another trusted person or organization (Madden et al., 2014). This sense of discomfort likely stems from the complexity of information flow on SNSs that can blur public and private. The survey results show that users are concerned about having their information accessed by unauthorized parties with selfish or adverse purposes (e.g., government surveillance programs, targeted advertising, data collection by businesses that own or contract with SNSs, etc.).

Perhaps due to concerns about online privacy, 61% of online adults say that they would like to do more to protect the privacy of their personal information (Madden et al., 2014). More recently, in a survey conducted after the Cambridge Analytica scandal, the Pew Research Center found that 54% of Facebook users reported they adjusted their privacy settings "in the last 12 months" and that 26% said they deleted the Facebook app from their phones (Perrin, 2018). Researchers have also found that teenagers are using more creative means to manage their privacy on SNSs. Despite the myth that teenagers do not care about privacy, a large-scale ethnographic study of teenagers in the U.S. found that they engage in creative tactics to control others' access to the meaning of information they share as a means to protect their privacy (Marwick & boyd, 2014). For example, teens often use "social steganography" on SNSs, which refers to encoding their messages to ensure that they are functionally accessible, yet meaningless for those who are not part of their intended audience

(e.g., subtweeting on Twitter) (boyd, 2014; Marwick & boyd, 2011, 2014). These findings indicate that teens use cultural or linguistic tools (e.g., in-jokes, song lyrics, culturally-specific references, etc.) to prevent outsiders from understanding their context-specific conversations and thus protect their privacy from outgroups (boyd, 2014). In other words, although teens may appear rather cavalier in their privacy attitudes and behavior, this should not be taken as evidence that they do not care about their privacy when interacting online.

Because these recent studies clearly show that people care about their privacy on SNSs despite their extensive disclosure activities on social media platforms, this dissertation aims to better understand the discrepancy between people's privacy concerns and their SNS activities. In this chapter, I will clarify the relationship between people's needs for privacy and disclosure to help explain how people weigh the expected costs and benefits to make decisions to share information on SNSs. In addition, while a popular theoretical approach to understanding people's disclosure decisions (i.e., the privacy calculus model) views people's decision-making processes as highly rational, I will explain why this approach may not be suitable for understanding SNS users' privacy-related behavior due to the unique dynamics of information flow on SNSs (boyd, 2010) that force users to manage higher uncertainty and complexity – such as the unpredictable range of information flow to not only visible, but also invisible audiences (e.g. marketers, advertisers, government organizations, and unknown third parties through retweeting, forwarding, etc.). Because disclosing information on SNSs is associated with distinct privacy risks compared to other forms of communication, broadening the prevailing perspective that assumes complete rationality in people's decision-making processes concerning privacy on SNSs would offer a better understanding about SNS users' decision-making processes about disclosure and partially explain SNS users' continued experience of privacy breaches and violations on SNSs.

Understanding Privacy

Definition of Privacy

Given the way that information is transmitted, stored, mined, and sold in the digital age, commentators (e.g., Warzel, 2019) point out that privacy is not simply about secrets, but instead is about autonomy. For example, sharing seemingly innocuous information, such as clicking "likes" on pages that users enjoy, can enable third parties to infer personality traits about these users, resulting in these users losing control over their own information (Kosinski, Stillwell, & Graepel, 2013). The idea that, at its core, privacy is about control has been around a long time. Key privacy scholars have defined privacy as individuals' ability to control their information. For example, Westin (1967) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 5), and Altman (1975) defined privacy as "selective control of access to the self or to one's group" (p. 18). Using this definition, a survey by the Pew Research Center demonstrates how much people value privacy. Ninety-three percent of U.S. adults say that being in control of who can get information about them is important, and 90% of the same population says that controlling what information is collected about them is important (Madden & Rainie, 2015). While a large majority of U.S. adults continue to use SNSs and post a lot of information in these platforms, maintaining their privacy in the form of information control remains an important issue for them.

At the same time, while they place a high value on privacy, most people feel powerless about navigating privacy management on SNSs. A large majority of adults (69%) are not confident that the records of their activity maintained by the SNS they use will remain private and secure (Madden & Rainie, 2015). And SNS providers' efforts to become more

transparent about their data collection processes might not be enough to solve this issue. After reviewing a list of advertisers that collected information about her to run targeted advertisements on Facebook, investigative reporter Katie Notopoulos (2019) described this experience by saying: “Facebook showed me my data is everywhere, and I have absolutely no control over it.” The asymmetries in information between people and companies is one of many traits that describe “surveillance capitalism,” which is defined as “a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales” (Zuboff, 2019). Surveillance capitalism helps explain the lack of control users have over the flow of their information and their sense of helplessness.

Privacy vs. Disclosure

Despite privacy settings, the level of control people have over a good deal of their information is difficult to measure because their information flow is largely unpredictable and invisible in SNSs. Given this limitation, another way to examine people’s sense of privacy is to analyze their disclosure behavior. The fraught relationship between people’s need to maintain their privacy and the need to disclose information is illustrated in Petronio’s (2002) Communication Privacy Management (CPM) theory. Adopting the control-based definition of privacy, Petronio (2002) posits that people feel they own their information and that they can protect their information from others’ access through control. Based on this definition, CPM describes how people decide to reveal or conceal their information using their perceived control over the ownership of their information. This decision-making process illustrates that Petronio (2002) views privacy and disclosure in dialectical tension because they are opposites that function in incompatible ways.

Petronio’s idea echoes arguments made by other key privacy scholars. For example, Altman (1975) describes privacy as a dialectic process that involves “an interplay of

opposing forces—that is, different balances of opening and closing the self to others" (p. 11). Since privacy and disclosure have a dialectic relationship, Petronio (2002) argues that disclosure means giving up a certain amount of privacy, and thus disclosure is "meaningful only in relationship to privacy" (p. 14). Using the relative tension of these opposing forces, she explains that the degree of privacy individuals hold can be measured by looking at how public people are with others—i.e., their disclosure behavior. Based on this relationship between disclosure and privacy, SNS users' decision to disclose information may be taken to indicate their intent to share, or possibly surrender, their control over their information, and thus implicates privacy.

Making Privacy-Related Decisions

There are two schools of thought when it comes to making decisions about privacy online. Some scholars presume that people make decisions concerning how to protect their privacy in a highly rational manner (e.g., the *privacy calculus* model). This approach assumes unbounded rationality and says people decide whether to disclose information through a process of weighing all of the benefits and risks associated with the disclosure (e.g., Culnan & Bies, 2003). Others, however, argue that people cannot always make completely rational decisions due to *bounded rationality*, which refers to the fact that decision makers are inevitably constrained by having limited information, limited human capacity to process information, and limited time (Simon, 1997). Comparing these two approaches will illustrate why the second approach is more appropriate for understanding how users make decisions concerning privacy when using SNSs.

CPM Theory and the Privacy Calculus Model

As a rule-based theory, CPM proposes that disclosure is regulated by rule management processes. These rules are developed by five decision criteria: cultural,

gendered, motivational, contextual, and risk-benefit ratio. This dissertation will focus on how the last criterion affects people's rules about disclosure. According to Petronio (2002), thinking about the risk-benefit ratio helps people take into account both the felt vulnerability and expected advantages of disclosure to decide whether they want to share information. Because people balance the need for disclosure and privacy, they aim to make decisions in a way that minimizes risk and maximizes their control over private information (Petronio, 1991, 2002). This is consistent with social exchange theory (Homans, 1961), which posits that people will engage in interpersonal interactions if they see more rewards than costs (Cook & Rice, 2003).

The process of using the risk-benefit ratio criterion to develop rules about disclosure is called the "privacy calculus" (Culnan & Armstrong, 1999). This concept stems from Laufer and Wolfe's (1977) work, in which they described "calculus of behavior" as a process of deciding whether to disclose information by rationally evaluating the potentially positive and negative outcomes of doing so (p. 35). This concept was later applied to internet use to examine disclosures related to targeted advertising (Culnan & Armstrong, 1999) and online shopping (Dinev & Hart, 2006). Culnan and Armstrong (1999) found that people were more willing to share information for targeted advertisements when they could observe that their information would be managed based on fair information practices. They used this study result to argue that customers will continue to share information as long as their perceived benefits exceed the risks. Dinev and Hart (2006) used the privacy calculus model in the context of providing personal information for online transactions and found that people's willingness to share personal information to online retailers was indeed negatively affected by perceived privacy risk while it was positively affected by personal interests in internet content that overrides their privacy concerns (i.e., benefits).

Beyond its application to understand online disclosures to companies conducting business online, the privacy calculus model has also been applied to the SNS context (Dienlin & Metzger, 2016; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Min & Kim, 2015; Shibchurn & Yan, 2015; Sun, Wang, Shen, & Zhang, 2015). Research applying the privacy calculus model to SNS contexts argues that users weigh the perceived costs and benefits of disclosure to decide whether to disclose information on these platforms. The benefits of disclosure may include social gratifications, such as improved connectedness and maintaining existing relationships, self-presentation, social support, and social capital (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011; Krasnova et al., 2010; Krasnova, Veltri, & Günther, 2012; Trepte et al., 2017). The risks of disclosure are usually described as concerns users have about their privacy on SNSs, such as losing control over their information (e.g., identity theft), having others misuse their information (e.g., stalking), consenting to data collection by third-parties (e.g., advertisers, law enforcement, etc.), and having their information accessed by unintended audiences (e.g., a post that was meant for a specific group of friends may be circulated among other users) (Krasnova et al., 2010, 2012; Trepte et al., 2017; Vitak, 2012). The privacy calculus model predicts that users will disclose information on SNSs when they think that the net benefit would be positive as a result of comparing the anticipated benefits and costs of disclosure.

Another Approach to Understanding Privacy-Related Decisions: Bounded Rationality and Cognitive Heuristics

While the privacy calculus model is a popular approach to understanding how people make decisions about sharing information on SNSs, this model has been criticized for being unrealistic and neglecting bounded rationality (Acquisti, 2004; Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Wilson, 2015). Because of these issues, Soros (2010) claims that "rational

expectations theory is no longer taken seriously outside academic circles" (p. 6). Because the privacy calculus model is consistent with traditional economic theory that describes people to have "rationality and unbounded 'computational' power" (Acquisti, 2004), it assumes that SNS users take the time and processing capacity to weigh all of the costs and benefits associated with each instance of disclosure. However, people cannot process and use all of the relevant information to make accurate conclusions (Simon, 1982). Especially in the context of disclosure on SNSs, the flow of information is difficult to predict, and thus the risk associated with disclosures is difficult to calculate (Acquisti, 2004).

Making decisions with bounded rationality does not mean people are making irrational decisions. Instead, this means people are making adaptive decisions that are rational enough in a given environment (Gigerenzer, Todd, & the ABC Research Group, 1999). Decision-making processes with bounded rationality can mean satisficing—making a choice from a set of available, but not complete, alternatives in a given situation, or can mean relying on cognitive heuristics—making a choice from simultaneously available objects without searching for all relevant objects for the decision, but instead, using "easily computable stopping rules" (i.e., cognitive heuristics) (Gigerenzer et al., 1999, p. 14). Overall, Gigerenzer and colleagues' (1999) research shows that making decisions with bounded rationality is not inherently inaccurate nor is it without rules and, most importantly, it is adaptive to real environments without applying unrealistic expectations of full rationality in people's decision-making processes.

Because using the privacy calculus approach is not realistic for SNS users, some recent research has shown that SNS users may go through decision-making processes that are not fully rational by relying on cognitive heuristics that help them make decisions quickly without experiencing cognitive overload (Acquisti, 2012; Acquisti, Brandimarte, &

Lowenstein, 2015; Acquisti & Grossklags, 2005; Carey & Burkell, 2009). In this stream of research, researchers have started to identify some heuristics that might influence people's decisions in various online contexts (e.g., online banking, mobile applications, online news, etc.) (Gambino, Kim, Sundar, Ge, & Rosson, 2016; Knobloch-Westerwick, Sharma, Hansen, & Alter, 2005; Sundar, 2008). For example, Gambino and colleagues (2016) identified "positive heuristics" that increase disclosure online (e.g., gatekeeping heuristic, safety net heuristic, bubble heuristic, and ephemerality heuristic) and "negative heuristics" that decrease disclosure (e.g., fuzzy-boundary heuristic, intrusiveness heuristic, uncertainty heuristic, and mobility heuristic) in online contexts.

Unique Dynamics of Information Flow on SNSs

The difficulty of estimating the costs and benefits of disclosure on SNSs may come from the unique dynamics of information flow on SNSs that distinguish this setting from other online and offline contexts. According to boyd (2010), social network sites are shaped by three central dynamics: (1) collapsed contexts, (2) invisible audiences, and (3) the blurring of public and private. These dynamics are unique to the context of SNSs, and thus are not applicable to contexts that involve other forms or formats of communication.

Collapsed Contexts

As each instance of disclosure on an SNS leads to potential information access by multiple types of audiences, users should think about the consequences associated with disclosing specific information. When considering other SNS users only, having people from different social circles (e.g., family, friends, colleagues, employers, etc.) become part of a single group of message recipients on social media platforms is called social "context collapse" (Vitak, 2012). Dealing with multiple audiences from different social contexts of one's life for every instance of disclosure is a unique feature of SNSs, compared to other

forms of interpersonal communication, that increases the cognitive load required to complete a risk-benefit analysis. Mismanagement of collapsed social contexts in SNSs can have negative repercussions. In 2018, when a nurse posted a picture (i.e., a photo of herself in a culturally insensitive and inappropriate Halloween costume) that was meant only for her close group of friends on Facebook, this post quickly circulated online and she lost her job as a result (Klausner, 2018). This incident is one example among several highly-publicized cases in which social context collapse led to job loss (Bracetti, 2012; Halper, 2015).

Invisible Audiences

SNS users also need to consider the potential privacy risk associated with disclosing their information to "invisible audiences" of unknown others, or who Stutzman and colleagues (2013) call "silent listeners." This may include, for example third-party apps, advertisers, the government, or Facebook itself, as well as other SNS platform operators and even other users such as if a friend reposts or relays the original information. A complete privacy calculus about disclosure on SNSs would require users to think about privacy risks associated with both visible and invisible audiences, but it is highly unlikely for users to consider all of these factors because research shows that they have difficulty estimating the size and the types of their audience(s) (Acquisti & Gross, 2006; Bernstein, Bakshy, Burke, & Karrer, 2013; Marwick & boyd, 2011), and in general cannot know all the types of potential invisible audiences.

The Blurring of Public and Private

As SNS users typically face multiple types of audiences during each instance of information disclosure, it becomes difficult to distinguish between private and public information. For example, even when SNS users decide to share information that they consider personal or even "private" with only close friends or relatives, this same decision

makes their information directly and indirectly accessible to other entities, such as public companies and government organizations. Because the information was shared on SNSs, it leaves discoverable digital traces that can be accessed by individuals or organizations other than the friends or relatives the person originally shared the information with. Since each instance of disclosure on SNSs spans across multiple contexts that are simultaneously private and public, once any information is disclosed on an SNS, this information cannot be easily categorized as private or public.

Consequences of the Unique Dynamics of Information Flow on SNSs

Due to the three unique dynamics of information flow on SNSs, users' disclosure involves considering multiple types of audiences that are both visible and invisible to them. As different groups of people ranging from close friends and acquaintances to corporations, marketers, and government officials can gain access to the information disclosed by SNS users, information moves more quickly and widely on SNSs, and the distinction between private and public disclosure becomes blurred. In this context, SNS users' decision-making processes cannot be fully rational due to lack of complete information, situational constraints (e.g., habits, emotions, dependency), and cognitive limitations (Acquisti, 2009; Acquisti et al., 2015; Kehr et al., 2015; Phelan, Arbor, & Resnick, 2016; Trepte et al., 2017). Consequently, users' decisions to share information may be affected by misperceptions of costs and benefits, as well as by social norms, emotions, and cognitive heuristics (Acquisti et al., 2015). For example, users might disclose information due to their need for immediate gratification (e.g., social gratifications), while discounting the distant or invisible future risks (e.g., identity theft) (Acquisti, 2004). The complexity of understanding privacy risks on SNSs has resulted in privacy scandals that demonstrate how disclosure on SNS is distinct from disclosures made through other forms of communication.

A recent example of such as scandal occurred in 2018, when it was revealed that up to 87 million Facebook users' information had been harvested without their knowledge by a voter-profiling company called Cambridge Analytica (Kang & Frenkel, 2018; Rosenberg, Confessore, & Cadwalladr, 2018). Cambridge Analytica asked 270,000 Facebook users to complete what they were told was an "academic study" in which they downloaded a personality quiz app called "This is Your Digital Life" (BBC News, 2018). The app required access to their Facebook accounts, and while those users consented to sharing their account information with the app (e.g., their name, age, "likes," etc.), the app also collected data from the profiles of their Facebook friends (Davies, 2015; Rosenberg et al., 2018). In this way, Cambridge Analytica accessed millions of raw profiles of Facebook users to build psychographic profiles of users without their consent that were later used to design powerful political messages intended to manipulate their voting decisions (Rosenberg et al., 2018).

The Cambridge Analytica scandal also demonstrated that while SNS users can consent to disclose their information to one entity and for one purpose (e.g., an academic survey), their data can end up in the hands of a completely different entity and used for a very different purpose. Although this type of situation is also possible in offline interpersonal communication settings—for example when personal disclosures or even secrets someone divulges to a trusted friend reach other people through word-of-mouth (Petronio, 2002)—the rate and scale of information flow on SNSs is different from any other settings. The Cambridge Analytica example again serves as a good case in point. As mentioned earlier, only a little more than a quarter million users agreed to share their information, and so the remaining 99.7% of the 87 million users affected by the scandal had information collected by an unknown party without their awareness or consent simply because they were connected to a single user who chose to participate in an online survey. In other words, one click to

download a Facebook "personality quiz" app by a few users who relied on an incorrect understanding of the privacy risk associated with their action ended up revealing information about tens of millions of people. This surpasses the scale and scope of information leakage in other interpersonal disclosure settings by several orders of magnitude.

The Cambridge Analytical scandal is the biggest information leakage and misuse case in Facebook's history, but it is not the only example. Later that same year, Facebook disclosed a bug that revealed 6.8 million users' private photos (e.g., photos uploaded on Facebook Stories or photos that users uploaded, but decided not to share at all) to third-party developers. These photos were visible to the developers of over 1,000 apps, and the photos' visibility could not be controlled by users' privacy settings (Barrett, 2018). These photos, which users had intentionally decided *not* to share publicly, may have given away private details of these users' personal lives without their consent, and could have helped the third-party developers create unwanted targeted advertising messages to gain revenue. Unlike information leakage in other communication settings, SNS users often have no way to estimate the nature or scope of privacy risk associated with their information leakage because they are not made aware that their information (e.g., photos) was leaked in the first place and do not know who could access their information as a result. While people are likely more familiar with understanding and dealing with privacy risk associated with information leakage to others within their social networks (information flowing from "friends only" on Facebook to "friends-of-friends," or texting a photo to one person but that person sharing it with others, etc.), they also need to navigate the risk associated with information leakage to complete strangers who are interested in their information (e.g., advertisers, developers, etc.). Yet this is extremely difficult or impossible to do.

In addition, it was recently revealed that Facebook allowed Microsoft's search engine Bing to access Facebook users' friend networks without their consent, and gave Netflix and Spotify access to users' private messages (Dance, La Forgia, & Confessore, 2018). This leakage of information to prominent third-party companies and corporations could help Facebook build advertising, marketing, and communication strategies to increase revenue. This case also demonstrates that the flow of users' information is often out of their control and that their information may have reached others who hold different interests in users' information. Because information moves faster and further on SNSs than in other information disclosure settings, the full range of possible consequences of such information leakage is unpredictable. Interestingly, due to the consequences that can result from multiple large-scale breaches of confidentiality online, the *New York Times'* has started a project that aims to begin a discussion about the evolving boundaries of privacy (i.e., "The Privacy Project" [https://www.nytimes.com/series/new-york-times-privacy-project]). As part of this initiative, opinion columnist Farhad Manjoo says that: "It is time to start caring about the mess of digital privacy. In fact, it's time to panic" (Manjoo, 2019).

Overview and Rationale for this Project

Given the unique dynamics of SNSs that make users' information flow especially complex and uncertain, disclosure decision-making theories (such as the privacy calculus model) that involve a rational decision-making process based on having complete information may not be useful or applicable in SNS settings. Indeed, as discussed earlier, the complexity of information flow in the SNS environment likely necessitates the use of heuristics. It is well known that in situations where there is too much information to process (e.g., risks associated with disclosing information to different types of known and unknown audiences) and too much uncertainty (e.g., predicting the range of information flow),

information processors experience cognitive overload when trying to make a rational decision, and thus often rely on cognitive heuristics to guide their decisions (Carey & Burkell, 2009; Chaiken, 1987; Kahneman, 2003; Payne, 1976; Sundar, Knoblock-Westerwick, & Hastall, 2007; Sweller, 1988; Sweller, Van Merrienboer, & Paas, 1998; Tversky & Kahneman, 1974). Therefore, this dissertation sought to investigate the possible heuristics that govern disclosure in SNS contexts involving possible risks to privacy via loss of control over information about the self. In the following chapter, I will define the concept of heuristics and provide an overview of relevant literature that discusses the effects of heuristics on people's decision-making processes. This literature review was used to develop hypotheses that are specific to the context of SNSs and to design studies aimed to provide a deeper understanding of how heuristics operate in people's decision-making processes about privacy and disclosure on SNSs.

To gain a thorough and nuanced understanding about the effects of heuristics, this dissertation consists of three studies that use different methods. First, focus group interviews were conducted to gauge "proof-of-concept" by collecting anecdotal evidence to see if SNS users report relying on cognitive heuristics and, if so, how these heuristics affect their disclosure and other privacy-related behaviors on SNSs. Second, the qualitative data based on these focus group interviews informed the development of two survey questionnaires that were used in Study 2A and Study 2B. Study 2A examined whether the qualitative results from the focus group interviews could be extended and generalized to a larger and more representative population of SNS users. Study 2B then tested specific hypotheses about theoretically-derived relationships between the cognitive heuristics observed in the focus groups and SNS users' privacy-related attitudes and behaviors. In sum, as the effect of cognitive heuristics is usually seen as a subconscious and invisible process, using both

qualitative and quantitative methods and employing different measurement approaches provided an opportunity to study cognitive heuristics through different lenses, thereby offering richer evidence and insight into the role of cognitive heuristics in SNS users' privacy attitudes and behaviors than what is currently available in the literature.

Chapter 2: Relying on Heuristics on SNSs

As explained in the previous chapter, the privacy calculus model has been adopted in a lot of research aimed to understand how people make disclosure or other privacy-related decisions online. However, some scholars have begun to recognize that making these decisions involves a high level of complexity and uncertainty, which makes it difficult for people to engage in a thorough rational calculus analysis about privacy (Acquisti, 2012; Acquisti et al., 2015; Acquisti & Grossklags, 2004, 2005; Carey & Burkell, 2009). Acquisti and Grossklags (2004, 2005) were perhaps the first to study how cognitive heuristics, such as hyperbolic discounting, might affect people's privacy-related decisions online. They hypothesized that people discount their future privacy risks in the context of online banking or web searching by making decisions that lead to immediate gratification instead of more long-term and privacy-protective decisions (e.g., paying for an anonymous browsing service, signing up for a credit alert, etc.). More recently, a few scholars have conducted both qualitative and quantitative studies to generate a more comprehensive list of cognitive heuristics that might influence people's privacy-related decisions in various online contexts (e.g., online banking services, mobile applications, online discussion boards, virtual assistants, cloud services, etc.) (Gambino et al., 2016; Sundar, Gambino, Kim, & Rosson, 2016; Sundar, Kim, & Rosson, 2019).

Similar to other web use contexts, SNS users are also unable to evaluate all of the benefits and risks associated with their disclosure on SNSs. As explained in Chapter 1, the dynamics of information flow on SNSs make them a uniquely complex environment in which to make fully rational decisions, and thus may necessitate SNS users' reliance on cognitive heuristics. But the role of cognitive heuristics has yet be explored thoroughly in the specific context of SNS use. In this chapter, I will explain the relationship between people's

bounded rationality and their reliance on cognitive heuristics, describe how these concepts are applicable to SNS users' privacy-related decision-making processes, and describe relevant prior research to propose nine cognitive heuristics that might influence disclosure and other privacy-related decisions in the context of SNS use.

Bounded Rationality and Cognitive Heuristics

People's innate bounded rationality—which refers to human limitations of both knowledge and cognitive computational capacity—prevents them from (1) creating a comprehensive list of benefits and costs, (2) generating all alternatives to a given decision, or (3) predicting the likelihood of associated consequences (Simon, 1955, 1979, 1997). Instead, people usually analyze risk in an "experiential" mode of thinking, which is intuitive and fast because it is based on making associational, rather than logical, connections (Slovic, Finucane, Peters, & MacGregor, 2004). Therefore, when people assess the probability of uncertain events with limited cognitive resources, they tend to rely on heuristics, rather than logic or statistics (Gigerenzer & Gaissmaier, 2011; Kahneman, 2003; Kahneman & Frederick, 2002; Shah & Oppenheimer, 2008; Simon, 1979; Slovic et al., 2004; Tversky & Kahneman, 1974).

In the behavioral economics literature, *heuristics* refer to cognitive shortcuts that serve as mental "rules of thumb" (Acquisti & Grossklags, 2005; Kahneman, 2003; Shah & Oppenheimer, 2008; Tversky & Kahneman, 1974). Since Newell and Simon's (1972) book, the term heuristics has received wide attention and became popular in psychology and behavioral economics, and several scholars have offered definitions of this term (Shah & Oppenheimer, 2008). Herbert Simon (1990) introduced the concept of bounded rationality and defined heuristics as "methods for arriving at satisfactory solutions with modest amounts of [mental] computation" (p. 11). Kahneman and Frederick (2002) describe heuristic-based

judgment as “attribute substitution” in which “an individual assesses a specified target attribute of a judgment object by substituting another property of that object—the heuristic attribute—that comes more readily to mind” (p. 707). More recently, Shah and Oppenheimer (2008) proposed an effort-reduction framework for studying heuristics that views relying on heuristics to make decisions as the exact opposite of using the weighted additive rule, which refers to a complex algorithm that helps people come to optimal decisions and accurate judgments by considering all of the alternatives to a particular decision. Shah and Oppenheimer’s framework views relying on heuristics as not completing at least one of five known tasks required to use the weighted additive rule. In other words, relying on heuristics involves: (a) examining fewer cues, (b) reducing the difficulty associated with retrieving and storing cue values, (c) simplifying the weighting principles for cues, (d) integrating less information, and/or (e) examining fewer alternatives.

After conducting a series of studies that examined the effect of heuristics, Tversky and Kahneman (1974) associated heuristics with cognitive biases. They compared making heuristic-based judgments to relying on blurry outlines of mountains to estimate distance, because relying on this cue could result in predictable errors (Kahneman, 2003). Consistent with what this analogy suggests, when people rely on cognitive heuristics, their decisions may not be consistent with rational decisions they would have made after completing a careful cost-benefit calculus analysis and may result in systematic biases, such as nonregressive prediction, neglect of base-rate information, overconfidence, etc. (Kahneman, 2003; Tversky & Kahneman, 1974). Moreover, these heuristic-induced biases could lead people to negative consequences, such as inaccurate evaluations (Slovic et al., 2004; Tversky & Kahneman, 1974). Tversky and Kahneman (1974) concluded that “heuristics are quite useful, but sometimes they lead to severe and systematic errors” (p. 1124). Some scholars

have opposing views toward associating biases with cognitive heuristics, as they view these heuristics as a useful "adaptive toolbox" that offers fast and frugal ways to make reasonable decisions (e.g., using a simple decision tree to classify heart attack patients as high-risk or low-risk) (Gigerenzer et al., 1999), but scholars on both sides seem to agree that people make decisions with bounded rationality and that no heuristic is failproof.

People are more likely to rely on heuristics when they are under time pressure and/or engage in concurrent but different cognitive tasks (Kahneman, 2003). Disclosures on SNSs involve multiple cognitive tasks at once because it is associated with complex information flow to multiple types of audiences and are usually done under some time pressure because it brings immediate gratification. Due to the unique nature of the environment, SNS users would be more likely to rely on cognitive heuristics that simplify their privacy-related decision-making processes to let them gain immediate gratification. Moreover, reliance on cognitive heuristics may be more consequential for SNS users due to the unique dynamics of information flow on SNSs that were discussed in the previous chapter. For example, a private disclosure to a close friend may become a public revelation of personal details and private information may become available to unknown entities (e.g., silent listeners) without having the chance to give consent to such a disclosure. Cognitive heuristics could partly explain why SNS users may still have negative privacy-related experiences on SNSs despite the increasing number of privacy management tools available to them.

A review of literature in communication, behavioral economics, and psychology shows that there are at least nine cognitive heuristics that might influence SNS users' disclosure and privacy-related decisions: affect heuristic, availability heuristic, optimistic bias, bubble heuristic, homophily heuristic, bandwagon heuristic, inequity aversion, hyperbolic discounting, and ephemerality heuristic. These are each explained in turn in the

following sections. The following literature review is intended to help develop the interview protocol for focus group interviews conducted for this dissertation, and thus specific hypotheses about each heuristic are proposed later in the dissertation after the focus group interview data are analyzed, such that the hypotheses may be based on both prior literature and the empirical findings of the focus group interviews.

Affect Heuristic

The affect heuristic refers to using emotions—both positive and negative—about an activity or object as mental shortcuts to make judgments or decisions (Slovic, Finucane, Peters, & MacGregor, 2007). Slovic and colleagues (2004) define "affect" as the "specific quality of 'goodness' or 'badness' (1) experienced as feeling state (with or without consciousness) and (2) demarcating a positive or negative quality of stimulus" (p. 312). In the 1970s, social psychologists began to recognize the importance of affect in decision making (Slovic et al., 2007). Early research illustrated that people rely on affect while engaging in the experiential mode of thinking, which as mentioned before, is a "quicker, easier, and more efficient" way to deal with complex or uncertain situations (Slovic et al., 2007, p. 1334). Research has shown that priming people with a smiling face can induce them to make favorable judgments about stimuli that appear after the prime (Winkielman, Zajonc, & Schwarz, 1997). Affective feelings can also influence people's judgments about risk perceptions (Peters & Slovic, 1996). For example, research finds that people's perceived risks and benefits associated with various activities are negatively related (Fischoff, Slovic, Lichtenstein, Read, & Combs, 1978), and thus if people feel favorably towards an activity, they tend to underestimate the risk and overestimate the benefit, regardless of the actual relationship between the risk and benefit associated with the activity (Alhakami & Slovic, 1994). This effect of affect on people's risk-benefit judgments has been supported in multiple

domains—people's judgments about technology, toxicology, and finance (see Slovic et al., 2007).

Research further shows that affective impressions influence people's privacy risk assessment and decision-making processes when sharing information online (see Kokolakis, 2015 for an overview). Wakefield (2013), for example, found that people's intention to disclose increases when they are on a website that induces positive affect (e.g., website for buying a pool table) compared to a neutral website (e.g., appliances website for buying a refrigerator). Similarly, when Kehr and colleagues (2015) studied how people feel about sharing information on a driving app, they found that risk perception of people in the control group was dependent on information sensitivity (i.e., a rational factor that affects risk assessment of sharing information), whereas people's risk perception was less affected by information sensitivity when they were in a condition that triggered positive affect.

This research suggests that the affect heuristic might influence people's decision-making processes on SNSs, similar to how it does in other contexts. For example, if people feel good when blogging or using a SNS, their positive affect might lead them to become less mindful about the privacy risks associated with those activities and, consequently, to share more information. Carey and Burkell first suggested this hypothesis in 2009, arguing that if self-expression activities within social media contexts provide users with strong positive feelings, they may "underestimate the harms arising from the disclosure of personal information" (p. 77). When Yu and colleagues (2015) tested the effect of affect on self-disclosure in SNSs, they found that affect positively influenced the motivators of self-disclosure, such as expression, self-presentation, social acceptance, and reciprocity, and suggested that people who feel positive affect overestimate the benefits of disclosure on SNSs. While Yu and colleagues' (2015) findings offer some insight into how the affect

heuristic can influence SNS users' disclosure decisions, the effect of affect on other privacy-related decisions (e.g., using privacy settings, etc.) has yet to be tested.

Availability Heuristic

According to Tversky and Kahneman (1974), the availability heuristic leads people to think certain events are more likely to occur if they can easily remember past occurrences of similar events. The availability heuristic refers to people's biased probability judgment about the likelihood of future occurrences of events that are more recent, familiar, or cognitively salient. For example, people may perceive a higher risk of heart attack among middle-aged people if it has occurred among their acquaintances (Fiandt, Pullen, & Walker, 1999). Similarly, because plane accidents receive more publicity than bike accidents, people think plane accidents occur more frequently than bike accidents regardless of their actual frequency (Baddeley, 2011). These examples illustrate that relying on this heuristic leads people to have systematic biases and become more or less attuned to particular risks (Tversky & Kahneman, 1973, 1974).

Having a biased probability judgment could have behavioral consequences. When people experience a negative outcome as a result of an activity, that experience becomes more salient in their memory and becomes more easily retrievable. As a result, people may think that the probability of negative outcome is higher than it actually is, which could increase the level of risk they associate with that activity. In turn, this may lead them to use more precaution when engaging in that activity again or become more likely to avoid that activity. Research shows that this type of reasoning affects people's behaviors in the context of assessing privacy risks during online disclosure. For example, people reconsider their behaviors and privacy expectations and/or apply a stricter boundary around their information after having a negative privacy experience (i.e., having a privacy expectation violated)

(Child, Haridakis, & Petronio, 2012; Child, Petronio, Agyeman-Budu, & Westermann, 2011).

A similar behavioral consequence that may relate back to the availability heuristic is also seen in the context of SNSs. Having a negative privacy experience may motivate SNS users to reevaluate their privacy rules and expectations and become more likely to use privacy-protecting tools, such as privacy settings (Debatin, Lovejoy, Horn, & Hughes, 2009; Litt & Hargittai, 2014). Indeed, people who have had a negative privacy experience in the past use more privacy tools that those who have not (Litt, 2013) or those who have heard of others' negative privacy experiences vicariously (Debatin et al., 2009), likely because such experiences are more salient and retrievable from memory (Carey & Burkell, 2009). Using the same logic, it can be hypothesized that a past negative privacy experience might trigger the availability heuristic to limit how much information users share on SNSs and/or make their privacy settings more restrictive. In contrast, the availability heuristic may not be triggered for SNS users who have not had any past negative experience, and thus they might feel more comfortable about sharing information on SNSs.

Optimistic Bias

Optimistic bias is a psychological phenomenon that refers to people's tendency to believe that they are less susceptible to risks than are others (Weinstein, 1980). Optimistic bias is a robust phenomenon with empirical evidence across several domains, including people's perceived likelihood of injury or disease (Dillard, McCaul, & Klein, 2006; Helweg-Larsen & Shepperd, 2001; Wei, Lo, & Lu, 2007), or natural disasters or crime (Shepperd, Helweg-Larsen, & Ortega, 2003; Weinstein, 1980). Ironically, optimistic bias can serve as a subconscious heuristic that fosters overconfidence, which leads to failure to take precautionary measures, thereby exposing people to a greater risk of experiencing negative

events (Radcliffe & Klein, 2002). For example, Radcliffe and Klein (2002) found that people who were unrealistically optimistic about their risk of heart attack knew less about the risk factors for having a heart attack and retained less information when they read an essay about those risk factors.

In addition to the evidence of optimistic bias in numerous offline contexts, prior research shows evidence of optimistic bias with regards to online privacy risk (Acquisti & Gross, 2006; Baek, Kim, & Bae, 2014; Campbell, Greenauer, Macaluso, & End, 2007; Cho, Lee, & Chung, 2010; Debatin et al., 2009). People think they are less likely to have a negative privacy experience than are others as a result of engaging in online activities. For example, Baek and colleagues (2014) found that people are optimistically biased about their privacy risk in comparison to younger internet users in their study that used a nationally representative sample of online users in South Korea. More recently, Metzger and Suh (2017) found evidence for optimistic bias among a nationally representative sample of U.S. adults in the specific context of SNSs. Both of these studies have also found that prior experience of privacy infringement increases optimistic bias by influencing people's perceived privacy risk for themselves, which might make them feel overconfident about making risky disclosure decisions. These findings illustrate that optimistic bias would influence SNS users' privacy-related decisions.

Bubble Heuristic

The bubble heuristic stems from the idea that humans (and animals) often feel more secure in enclosed spaces. The bubble heuristic was introduced by Gambino and colleagues (2016) as a cognitive heuristic that might affect people's judgments in the context of making privacy decisions online. People's sense of security in enclosed spaces appears to span across both offline and online contexts. Research from computer science shows that people feel

their data are more secure in an online "enclosure," such as personal Wi-Fi networks, incognito or private web-browser modes, etc. (e.g., Gao, Yang, Fu, Lindqvist, & Wang, 2014; Ion, Sachdeva, Kumaraguru, & Čapkun, 2011; Klasnja et al., 2009). Gambino and colleagues found evidence that the bubble heuristic influenced decisions concerning personal data disclosure to commercial services online (e.g., online banking services, mobile applications, and cloud services), as people reported that they felt better when they used their personal Wi-Fi networks at home because they thought others could not break into their networks, and they were more willing to share more personal information when using personal networks at home compared to unknown or public networks in other locations (e.g., hotels).

SNSs include features that could trigger the bubble heuristic; for example, most offer privacy settings that allow users to limit who can see their posts, send private messages, or untag themselves from photos—in other words, to curate who has access to one's information in the SNS. Analogous to Gambino and colleagues' (2016) reasoning, SNS users might feel more comfortable about sharing their information when they have adjusted their privacy settings, which could also provide a similar sense of security that comes from "enclosed" or protected spaces. Therefore, SNS users who have changed their privacy settings might share more personal information by relying on the bubble heuristic without carefully assessing the available and relevant risks associated with individual instances of disclosure. However, since limiting one's audience for particular posts does nothing to hide information that is culled by companies that own SNSs and sold to marketing agencies, relying on the bubble heuristic may lead SNS users to overlook privacy risks associated with having their information accessed by third party "silent listeners" (Stutzman et al., 2013). SNS users who have adjusted their privacy settings may feel that they are in an online

enclosure on SNSs, which could have implications for users' disclosure and privacy-related decisions.

Homophily Heuristic

The homophily principle is summarized by the idiom "birds of a feather flock together," and refers to people's tendency to associate more with people who are similar than with people who are dissimilar to them (Lazarsfeld & Merton, 1964; McPherson, Smith-Lovin, & Cook, 2001; Rogers, 2003). Research has found evidence of homophily in terms both status-based (e.g., race, sex, age, religion, education, social class, etc.) and value-based (e.g., attitudes, abilities, beliefs, aspirations, etc.) characteristics (Lazarsfeld & Merton, 1964; McPherson et al., 2001). People may prefer to interact with similar others for ease and effectiveness of communication based on shared knowledge, beliefs, and understanding (McPherson et al., 2001; Rogers, 2003) because the cost of forming and maintaining ties is lower among similar others, as well as for other reasons (Kossinets & Watts, 2009).

While Rogers (2003) defines homophily as "the degree to which two or more individuals who interact are similar in certain attributes, such as beliefs, education, socioeconomic status and the like," homophily is generally measured based on people's perceived similarity to others (see McCroskey, Richmond, & Daly, 1975 for examples of scales that measure *perceived homophily*). Homophily, in terms of interpersonal similarity, is assumed to affect perceived benefits and risks of social interaction. Similarity to others may make it easier to predict others' behavior, which can increase trust and lower perceived risk of association; and homophilous ties may be perceived as likely to be more stable and to last longer (Kossinets & Watts, 2009). A meta-analysis of the relationship between liking and disclosure shows that perceived similarity is a determinant of liking others, which leads to higher levels of trust and self-disclosure (Collins & Miller, 1994).

The effect of perceived similarity on self-disclosure might extend to the context of SNSs. When SNS users think their social network connections (e.g., Facebook friends, Instagram followers, etc.) are similar to them, they may feel more comfortable about sharing personal information. Social identity theory (Tajfel & Turner, 1979) suggests that ingroups (who tend to have more similar members) provide members a sense of solidarity, and that ingroup members are less likely to judge fellow ingroup members harshly; as a consequence, people may be more willing to disclose information to ingroup rather than to outgroup members. In addition, when SNS users think their social network connections are dissimilar to them, they may feel less comfortable sharing personal information or opinions because of possible social risks, such as criticism or conflict. Research on the spiral of silence (Neubaum & Krämer, 2017; Noelle-Neumann, 1984) supports the logic underlying this hypothesis. The homophily heuristic triggered by dissimilarity to the audience could be particularly salient on SNSs because users cannot easily determine their general similarity to all of their SNS connections due to collapsed contexts that merge people from different social circles into one large audience.

Bandwagon Heuristic

The bandwagon effect refers to people's propensity to go along with the crowd when they can perceive a general trend in terms of beliefs, ideas, and behaviors. This cognitive heuristic was first applied to online communication in Sundar's (2008) Modality, Agency, Interactivity, and Navigability (MAIN) model, and is triggered when people can see others' attitudes or behaviors (Lee & Sundar, 2013; Sundar, 2008). The logic behind this cognitive heuristic is similar to the one embedded in the social influence model, which is exemplified in well-known studies by Asch (1951, 1956) and Lewin (1947, 1948) that show how people's attitudes and actions are influenced by group majority. Similarly, the bandwagon heuristic

can influence many decisions online, such as credibility assessment, purchase intention, and online news article selection (Knobloch-Westerwick et al., 2005; Lee & Sundar, 2013; Sundar, 2008). For example, people are more likely to select articles if they have explicit recommendations from others or click on articles if they are included in a list of articles that have been most emailed by other readers (Knobloch-Westerwick et al., 2005; Sundar, 2008).

The bandwagon heuristic may also affect people's information disclosure decisions by reducing their risk assessments (e.g., "If the majority of other users have revealed information to a website, then it's probably safe for me to do the same"). Research on herding behavior suggests that if large numbers of other people reveal some kind of information, then people feel the risk of revealing that information about themselves is low and that there may even be benefit to doing so (Devenow & Welch, 1996). Based on that work, Acquisti, John, and Lowenstein (2012) found that providing people with information about higher admission rates of engagement in sensitive behaviors by others (e.g., cheating on taxes, fantasizing about nonconsensual sex, etc.) leads to increased admission rates by those participants themselves.

Some research has applied this reasoning to online information. For example, in a small-scale study, Rosson and Ge (2016) presented participants (N = 6) with the proportion of users who had already filled out a specific type of information on a prototype of a professional networking site, and participants reported that seeing this information would prompt them to share their own information. More recently, Spottswood and Hancock (2017) similarly provided subjects with an explicit cue (e.g., proportion of users who have shared their email addresses) to trigger the bandwagon heuristic on a fictitious SNS. They found that participants were more likely to share their information when they were in a condition that provided the explicit social disclosure cue. On real SNSs, users can see how other users share

information or interact with others (e.g., Facebook's News Feed, comments, etc.), so the visibility of other users' disclosure patterns and interactions may trigger the bandwagon heuristic to affect SNS users' disclosure and other privacy-related decisions.

Inequity Aversion

Inequity aversion describes people's tendency to resist unfair outcomes (Fehr & Schmidt, 1999). Inequity aversion leads people to prefer equal outcomes to either advantageous or disadvantageous outcomes (Loewenstein, Thompson, & Bazerman, 1989).[1] Inequity aversion helps explain why people feel discontent when they perceive others are unjustly getting more or better rewards than they are (Acquisti & Grossklags, 2007; Fehr & Schmidt, 1999). For example, behavioral economists find that people show strong inequity aversion when they think others are unfairly getting more income than them, such that in experimental contexts involving income distribution, people make decisions to minimize inequity (Clark & Oswald, 1996; Fehr & Schmidt, 1999).

People might also feel inequity aversion in the context of online interactions. For example, Acquisti and Grosslags (2007) suggest that people may become sensitive to online privacy invasions from companies if they feel like the companies are using their personal information without offering appropriate reward or consideration. Similarly, in terms of *social* inequity aversion in SNSs, if a person perceives that others are getting social benefits through using or being members of SNSs that he or she is not getting, that person may be motivated to become a more active SNS user. Findings from recent studies show that users' fear of missing out (FOMO), which is "a pervasive apprehension that others might be having rewarding experiences from which one is absent," motivates people to engage more on SNSs

[1] If forced to choose one of the two, however, people prefer outcomes that are relatively more advantageous for them to disadvantageous outcomes (Loewenstein et al., 1989).

(Przybylski, Murayama, Dehaan, & Gladwell, 2013, p. 1841). Buglass, Binder, Betts, and Underwood (2017) similarly found that SNS users who report higher FOMO engage in self-promoting behaviors (e.g., editing and updating content on their profiles, making emotional disclosures, etc.) to gain more social capital or social rewards commensurate to what they perceive others receive. These respondents also reported greater self-disclosure overall on SNSs, potentially making them more vulnerable to privacy risks.

The foregoing studies suggest that social inequity aversion in the SNS context can increase the salience of perceived benefits of SNS use for some users, and make the costs seem more distal. For example, seeing pictures of others having fun or number of likes on certain posts could all serve as cues that trigger users' sense of inequity aversion. At the same time, social inequity aversion triggered by these cues could lead SNS users to ignore or discount the risks associated with greater information disclosure in their quest to equalize benefits to self (e.g., "I know there are risks, but I don't want to miss out on the benefits that I see others getting from posting on SNSs"). For these reasons, it is reasonable to predict that inequity aversion may influence SNS users' privacy-related behavior.

Hyperbolic Discounting

Hyperbolic discounting refers to the idea that people do not discount distant and close events in a consistent way (Rachlin, Brown, & Cross, 2000; Read & Loewenstein, 2000). This term stems from economic theory and research that finds people tend to choose smaller immediate rewards over larger later rewards (i.e., immediate gratification) (see, for example, Ainslie & Monterosso, 2003; Laibson, 1997). Hyperbolic discounting has been seen to affect decision making in a wide range of issues including self-regulation, information acquisition, job search, procrastination, addiction, etc. (Rubinstein, 2003).

In the context of privacy decisions online, when people feel the benefits of disclosure are immediate while the risks of that disclosure to privacy are more distal, people may cognitively perceive benefits to loom larger than risks (Wilson & Valacich, 2012). Due to hyperbolic discounting, it has been suggested that people discount the likelihood of experiencing privacy violations in the future as they pursue immediate social gratification from SNS use, and thus feel comfortable about sharing information in that moment (Acquisti et al., 2015; Acquisti & Grossklags, 2005, 2007; Kokolakis, 2017). For example, hyperbolic discounting could lead SNS users to share personal or sensitive information for immediate gratification, and such risky disclosures based on hyperbolic discounting might lead users to feelings of regret (instead of immediate gratification) or result in unexpected privacy violations as that information is shared by others on SNSs. An aim of this dissertation is thus to see if empirical evidence exists to support hyperbolic discounting as a mechanism that affects SNS users' privacy behavior.

Ephemerality Heuristic

The ephemerality heuristic describes the process of deciding to share information based on people's belief that their online disclosure will not leave a permanent record, and thus poses less risk. The ephemerality heuristic is triggered by features that signal to people that the information (e.g., data, text, pictures, videos, etc.) they share online will become invisible to their audience or any potential message recipients after a short period of time (e.g., 24 hours). The rise in popularity of ephemeral features in messaging applications (e.g., private messaging on Snapchat, Line, WeChat, etc.) prompted Gambino and colleagues (2016) to coin the term "ephemerality heuristic" as a motivator for in-the-moment thinking or decision making based on ephemeral features (also see Sundar et al., 2016). In their focus group interviews, some participants reported that they felt more comfortable or secure about

sharing information if they believed the information will disappear without being stored (Gambino et al., 2016; Sundar et al., 2016). This finding suggests that users' sense of security when using ephemeral features might lower their risk perception associated with self-disclosure, thereby allowing users to be more open and share more information. As these ephemeral features are now being implemented on SNSs (e.g., Instagram Stories, Snapchat Stories, etc.), it is reasonable to hypothesize that the ephemerality heuristic might also influence how much and perhaps even what kinds of information users share on SNSs.

Research Plan

The overarching goal of this project was to make predictions about how each heuristic may influence SNS users' privacy-related behavior in unique ways along two dimensions: (1) the *amount* (and in some cases the type) of information that users disclose when using SNSs, and (2) their *use of the privacy settings* available from the platforms to help SNS users protect their privacy (e.g., the degree to which users restrict access to their information). For example, since Instagram offers three different levels of privacy settings that range from (1) public (i.e., users' posts are visible to everyone on Instagram) to (2) private (i.e., users' posts are visible to their followers only) and (3) custom Story setting (i.e., users' posts are visible to their followers only and their Stories are visible to selected followers only), Instagram users can select the most restrictive privacy settings (i.e., custom Story setting) to make their information visible to the smallest number of people, or they can select the least restrictive privacy setting (i.e., public) to make their content reach the greatest number of people.

Hypotheses that predict how each heuristic may affect SNS users' disclosure and privacy-related decisions (e.g., selecting the most restrictive privacy settings) were derived from the research and reasoning presented in this chapter. For example, in light of prior

studies that demonstrate how the affect heuristic leads people to underestimate risks associated with a certain activity, when considering the privacy risk associated with disclosure on SNSs, it can be hypothesized that feeling positively about using an SNS may lead to greater disclosure on that SNS. And given the dialectical relationship between disclosure and privacy, it can be further hypothesized that positive affect toward using a SNS leads people to select less restrictive privacy settings on that SNS. Similarly, based on previous research about how the bandwagon heuristic leads people to feel more comfortable about engaging in a certain behavior while tempering the risk associated with that behavior, it can be hypothesized that the degree to which users believe in the bandwagon heuristic (e.g., "It is safe to engage in certain behaviors if others have done them too") might be positively associated with the amount of information they share on SNSs. In addition, accounting for the dialectical relationship between disclosure and privacy-enhancing behaviors, it can be hypothesized that the degree to which users believe in the bandwagon heuristic is negatively associated with the restrictiveness of their privacy settings on SNSs.

Prior to developing specific hypotheses and research questions, however, it was important to establish proof-of-concept for the foundational proposition of this dissertation that heuristics affect SNS users' attitudes and behavior at all. Thus focus group interviews were first conducted to determine (1) whether the identified cognitive heuristics are salient to SNS users, and (2) if the cognitive heuristics described in this chapter affect disclosure and other privacy-related decisions in the specific context of SNSs based on users' personal experiences and reflections about their SNS use. Chapters 3 and 4 present the method and results of Study 1, which examines if there is empirical evidence that the heuristics described in this chapter are indeed applicable to SNS users' privacy-related decision making. Findings from Study 1 were used to augment the theoretical rationale provided in this chapter and

develop specific predictions about how each heuristic might impact disclosure and privacy behaviors among SNS users. Study 2 then employed survey methods to test the specific hypotheses and research questions posed in in Chapter 5. Finally, the methods and results of Study 2, which has two parts, will be presented in Chapters 6 through 9. Implications of the results of Studies 1 and 2 for both theory and future research will be discussed in the final chapter.

Chapter 3: Method for Study 1

To explore the extent to which there is evidence of the nine heuristics described in the previous chapter among SNS users, semi-structured focus group interviews were conducted in November-December of 2017, February of 2018, and February-March of 2019. A total of 119 students participated in 21 interview sessions. The group size in these sessions ranged from 3 to 9 (M = 5.62, SD = 1.56). Participants were recruited from an IRB-approved pool of undergraduate students who were enrolled in pre-Communication courses at a large public university located in the western U.S. 92 participants (77.3%) identified as female, and 27 (22.7%) as male. Participant ages ranged from 18 to 26 (M = 19.79, SD = 1.52). Almost all participants described themselves as "active" SNS users. 106 (89.1%) used Facebook, 116 (97.5%) used Instagram, and 108 (90.7%) used Snapchat.

The focus group interviews were conducted at a communication research laboratory, and participants were seated around a table upon arrival. Video and a backup audio recorder were used to record each session. During each focus group interview, participants answered questions designed to examine their impressions of the existence, prevalence, and possible effects of privacy heuristics on their decisions to share information on the most popular SNSs among the participant population (e.g., Facebook, Instagram, Snapchat, and Twitter) based on participants' own experiences. The interviewer invited participants to share relevant examples or experience they have had on any popular SNSs they use. The interview protocol was approved by the local IRB committee prior to data collection.

It is important to recognize that people may not be truthful or accurate when reporting about their own privacy behaviors, especially if those behaviors place them in an unfavorable light (e.g., lax on protecting their privacy). In other words, social desirability effects may influence people to report their privacy behavior to be more diligent or rational than it

actually is. To help guard against this, and based on previous experience conducting focus group interviews about privacy-related behaviors, the interview questions were phrased in such a way to ask whether the participants think either *their own or others'* behavior might be affected by heuristics. Specifically, when the participants stayed silent in response to questions about the possibility of cognitive heuristics affecting their own behaviors, the interviewer asked them to think about the same possibility for others. This strategy was developed to take advantage of the strength of focus groups versus individual one-on-one interviews because focus groups can allow participants to feel more comfortable admitting to making seemingly rash or irrational disclosure decisions when seeing that others, too, make similar decisions. In many cases, when one participant shared how he or she witnessed the effect of a cognitive heuristic on disclosure decisions by someone that he or she knew, other participants in the same focus group remembered and shared similar cases where they witnessed or experienced similar things themselves.

Because the focus group participants were likely to be unfamiliar with the concept of cognitive heuristics, the interviewer explained this concept and provided examples of heuristics (although not privacy heuristics specifically so as not to prime the participants) to make sure everyone had the same understanding of what cognitive heuristics are in general at the outset of each interview session. Also, as heuristic effects are mostly subconscious, the explanation about cognitive heuristics was important for helping participants attune to finding relevant memories of making decisions by relying on cognitive heuristics and discuss subconscious processes they may not have thought about before. Participants were invited to ask further clarification questions before the interviewer began facilitating the discussion. The protocol was developed to examine (1) whether the participants have noticed examples of the nine heuristics presented in Chapter 2 in their own or others' SNS use, and (2) if so,

whether and how they think these heuristics have or may influence disclosure and other privacy-related decisions on SNSs. For example, to study the availability heuristic, which is conceptualized as people's ready recall of a past negative experience for this study, the interviewer first asked, "Have you ever had a bad experience concerning privacy as a result of posting information on a social network site like Facebook, Instagram, or Snapchat?" And then, the interviewer asked, "Do you feel that this experience affected the things that you do to protect privacy on social network sites after it happened? For example, do you share less information as a result of it?"). The length of each focus group interviews ranged from 51 to 102 minutes (M = 68.90, SD = 12.13). See Appendix A for the full protocol.

After each focus group interview, the audio recordings were transcribed, and the transcripts were analyzed to understand the presence and/or effects of cognitive heuristics on participants' disclosure and privacy-related decisions in SNSs. The researcher and trained coders went through two phases of analysis. First, upon completing 10 interviews in 2017 and 2018, I trained research assistants to take a mostly confirmatory approach to data analysis based on the literature review while being open to finding themes that emerge in addition to the nine hypothesized heuristics and their effects. This sort of thematic analysis has a primary goal of "[describing] and [understanding] how people feel, think, and behave within a particular context relative to a specific research question" (Guest, MacQueen, & Namey, 2014, p. 11). The research assistants and I developed codes to represent themes that were developed based on the literature review on the nine cognitive heuristics and their possible effects on disclosure and use of privacy settings. The codes were applied as we found evidence of the heuristics and their effects in the transcripts. Unlike a classic content analysis, we did not count every occurrence of those codes or every co-occurrence of different codes, but we instead focused on compiling textual evidence (i.e., "data extracts")

that reflect the codes and used that textual evidence to understand how cognitive heuristics might operate to impact SNS users' privacy-related behavior. We followed the procedure for thematic analysis outlined in Braun and Clarke (2006), which involves (a) generating initial codes, (b) defining and naming themes, (c) reviewing themes, and (d) searching for themes. This was done because the goal of this first exploratory phase of analysis was to produce a "purely qualitative, detailed, and nuanced account of data" (Braun & Clarke, 2006; Vaismoradi, Turunen, & Bondas, 2013, p. 400).

When generating initial codes, our research team tried to find themes that might indicate the existence of additional heuristics that were not identified in the literature review by examining the parts of the transcripts where participants detracted from discussing cognitive heuristics they were asked about, and also participants' responses to the final question ("Would you like to add anything else to the interview?"). However, many participants expressed that they had never thought about the potential effects of cognitive heuristics before, and so mostly only provided responses to the questions about the specific cognitive heuristics already identified in the literature review. As such, we could not find any salient themes in the data to suggest the existence of additional heuristics that might influence SNS users' decisions.

After conducting the focus group interviews, the research team took an iterative approach to code participants' understanding of each of the cognitive heuristics and their effects on participants' disclosure as well as other privacy-related behaviors on SNS (e.g., use of privacy settings, withholding information, etc.). In this thematic analysis, we used both the findings from prior studies about heuristics in other online (but non-SNS) contexts (e.g., Gambino et al., 2016; Sundar, Kang, Wu, Go, & Zhang, 2013) and themes that emerged from the earlier focus group interviews analyzed. These served as interpretive anchors to look for

evidence of the nine heuristics we suspected might affect SNS users' privacy-related decisions. During this process, we read the transcripts multiple times and had several rounds of discussion to solidify our understanding of the themes in our data and their corresponding codes. For example, the theme that pertains to the effect of the bubble heuristic on people's perceived comfort could be supported by multiple codes, such as quotes that describe participants' use of restrictive privacy settings and quotes that describe their creation of "finstas" (fake Instagram accounts that users create to share content with a select number of close friends) to make their SNS content visible to a very select number of people. Through this process, we developed an analytic narrative based on a subset of the transcripts that we felt best described the role and effect of nine cognitive heuristics on the focus group participants' SNS use.

Lastly, we applied the narrative we developed on four reserved (i.e., unanalyzed) transcripts to conduct a content analysis to measure the reliability of the coding procedure on a new subset of the transcripts. After extensive training sessions in which the coders and I worked together to develop a comprehensive codebook, two coders (myself and one newly-trained coder) then independently coded the four focus group transcripts. Each unit of analysis contained a statement given by one participant during a single turn-at-talk in the interview. In these transcripts, there were a total of 776 statements, and the two coders coded each statement as either demonstrating an example of one of the nine heuristics or "N/A." The codes assigned by the two coders matched for 747 out of 776 (96.26%) statements (see Table 1). These data demonstrate that the coding scheme developed and used in Study 1 results in a high degree of agreement across several coders and rounds of focus group interviews. As will be detailed in the next chapter, anecdotal evidence about the role of each

heuristic in SNS users' decision-making processes from the participants' own experiences on different SNSs was found.

Table 1

Results from Content Analyses of Four Interview Transcripts

Heuristic	# of Statements	# of Matches	Agreement (%)
Bubble Heuristic	151	150	99.34%
Bandwagon Heuristic	126	117	92.86%
Affect Heuristic	106	106	100.00%
Hyperbolic Discounting	82	79	96.34%
Availability Heuristic	79	76	96.20%
Inequity Aversion	78	71	91.03%
Homophily Heuristic	59	57	96.61%
Ephemerality Heuristic	59	56	94.92%
Comparative Optimism	36	35	97.22%
Total	776	747	96.26%

Chapter 4: Results from Study 1

The following chapter is organized into sections that describe the findings about each cognitive heuristic that was included in the focus group interview protocol. In each section, I discuss participants' conceptualization of each cognitive heuristic in the context of SNSs and their response to possible effects of cognitive heuristics on their disclosure and/or other privacy-related decisions on SNSs with anecdotes about specific instances in which they feel cognitive heuristics were triggered to influence their privacy perceptions and/or decisions. The findings demonstrate the possible roles of cognitive heuristics in SNS users' decision-making processes.

Using the dialectic framework that views disclosure and privacy as two opposing counterparts (Petronio, 2002), the nine heuristics presented in Chapter 2 were expected to have opposite effects on SNS users' disclosure and privacy-related behavior. Interestingly, the focus group interviews revealed that the nine cognitive heuristics examined sometimes operate to affect users' decisions concerning whether and what information to share with others (and thus are termed "disclosure heuristics" from here forward) and other times work to influence SNS users' decisions about how they protect (e.g., by restricting) their information from others (which are termed "privacy heuristics" from here forward). The data show that heuristics including the affect heuristic, bubble heuristic, homophily heuristic, hyperbolic discounting, and ephemerality heuristic frequently influence users' disclosure behavior, whereas other heuristics including the availability heuristic and bandwagon heuristic seemed to influence both disclosure and users' strategies to protect their privacy by restricting their information in various ways.

Affect Heuristic

The affect heuristic, which refers to positive or negative feelings that serve as mental shortcuts (Slovic et al., 2007), was mostly discussed as participants' liking or disliking of using SNSs. As active SNS users, many participants reported that they liked using SNSs, and some participants said their positive feelings about a particular SNS made them want to share more on that SNS. In response to a question about whether liking a particular platform leads them to use it more, one Snapchat user said, "It was Snapchat [that I said was my favorite SNS], and I'd say yeah, I Snapchat a lot" (21-year-old female). Another participant echoed a similar idea and said, "Like other ones you might just post every once in a while, but with the one that you prefer the most, you might just post all sorts of stuff about what you're doing because you feel good about it" (18-year-old female). While several participants thought their positive feelings about using an SNS made them disclose more information on that SNS, others did not feel there was a strong relationship between liking an SNS and posting a lot of information on that platform: "For me personally, I love using Instagram, but I post like once a year. I like looking at other people's stuff, but I'm not really posting about my life" (19-year-old-female).

Interestingly, having *negative* feelings about particular SNSs seemed to have greater impact on how some participants used SNSs. Some participants' negative feelings about a certain SNS's business motivations were tied to their privacy concerns: "I feel like I don't want to post that much because I feel like I know they're just trying to get information" (19-year-old female). Another participant did not feel comfortable about targeted advertising on SNSs and reported that she deleted the apps as a result of her negative feelings: "I don't want to be advertised to based on conversations I've had… So, I've deleted the apps and stuff before" (21-year-old female). Also, the focus group discussions show that these negative feelings became more intense for some users as Facebook's scandal around its involvement

with Cambridge Analytica became highly publicized in 2018: “I mean I think I know Facebook’s got in trouble with privacy, especially lately, and so that definitely makes me feel less like I want to use it” (21-year-old female). Although he did not have correct facts, one participant noticed a change in others’ Facebook use after negative media coverage about the Cambridge Analytica scandal: “When Facebook was on the stand of the Supreme Court or whatever, a lot of kids stopped using the app altogether, just to retract their data, or try to anyways” (20-year-old male). Unlike their positive affect toward SNSs, the participants’ negative affect toward SNSs seemed to stem from their negative feelings about the SNS companies (e.g., Facebook, Inc.), rather than their feelings about the features of SNS platforms.

Overall, the focus group interview data suggest that negative rather than positive affect is a stronger driver of people’s disclosure decisions, as negative affect about SNS companies can lead users to disclose less information on a SNS or stop using a SNS altogether. This finding is consistent with the affect heuristic, and might be further explained by the principle of loss aversion when making risky decisions under uncertainty (Tversky & Kahneman, 1991, 1992). The logic of loss aversion rests on the fact that losses loom larger than corresponding gains in cognition, and so something “is worth more when it is considered something that could be lost or given up than when it is evaluated as a potential gain” (Kahneman, 2003, p. 705). Applying this logic to SNSs, when SNS users feel good about a SNS, they might not consider privacy risk (or feel safer) about sharing information on that SNS as much as when they feel negatively toward the SNS. The results showing negative affect to be more influential than positive affect are interesting because prior

research that examined the affect heuristic in online contexts has only compared the effect of positive affect to a neutral condition (Kehr et al., 2015; Wakefield, 2013).[2]

Availability Heuristic

The availability heuristic, which refers to people's biased probability judgement about a certain event that is more recent, familiar, or cognitively salient (Tversky & Kahneman, 1974), seemed to be triggered by negative privacy-related experiences on SNSs. Many participants reported that they have had negative privacy-related experiences on SNSs in the past. The most frequently-reported negative incident was getting messages from strangers, but the severity of these experiences varied from getting into trouble after a co-worker shared the participant's Snapchat Story with her boss to having a sexual post leaked to a fake Instagram account. A few participants explicitly said their personal negative experience became an availability heuristic in their future use of SNSs. For example, one participant who was reprimanded by her sorority sisters for posting a picture of herself engaging in an illegal activity said she has noticed a change in her mindset when she used SNSs after that experience: "I think it made me a lot more cognizant of what I was posting"

[2] At the same time, it may be premature to conclude that positive affect is a weaker predictor of SNS users' disclosure decisions. Because the questions about the affect heuristic were asked at the beginning of each interview, participants' responses may have been affected by social desirability effects, such that they may have wanted to present themselves as users who share information carefully, and not just because they like an SNS platform. Evidence for this is that several participants contradicted themselves in their statements to emphasize that privacy concerns do not affect their SNS use because they are already cautious about what they disclose on social media platforms. For example, one participant who explicitly stated that she deleted her SNS apps because she was concerned about the privacy risk corrected herself within seconds: "I deleted my apps because the privacy thing bothered me…It's not really the privacy aspect as much because you can choose what you share" (21-year-old female). It seemed like she did not want to acknowledge that her privacy on SNSs was out of her control. In any case, the effect of the affect heuristic should be examined in future studies using a method that minimizes social desirability responses to determine how much this heuristic factors into SNS disclosure decisions.

(18-year-old female). Several other participants said that having had a negative privacy experiences on SNSs led them to use different strategies to protect their privacy than they did before the incident happened, including staying away from SNSs, posting less frequently, deleting information (e.g., phone number), changing their posting strategies (e.g., posting "family-friendly" information only, not responding to public event invites, etc.), changing privacy settings, and contacting the app to report the incident.

In addition to the participants who shared their personal negative privacy-related experience, there were many participants who reported hearing of *other* people's negative privacy-related experiences on SNSs. These experiences included having nude photos leaked and having their identity stolen to create fake social media accounts. Perhaps due to the comparative severity of these experiences, hearing about others' experiences also served as an availability heuristic for some participants. After witnessing the consequences of having nude photos leaked, one participant said "Their nudes got leaked, and it was the worst thing ever 'cause it was in high school and she was underage, and…it taught me to not take nudes and send them" (21-year-old female). Because the participants recruited for the interviews were college students who recently lived with their parents, some participants reported that their parents' stories about negative SNS experiences also triggered the availability heuristic in their current use of SNSs. One participant described how her parents' fear-based teachings about SNS use shaped how she makes disclosure decisions on SNSs: "My parents drilled in scary stories, the worst-case scenarios to me, and that definitely impacted what I choose to post…it's just always in my head…I definitely don't post anything that I wouldn't care if anyone saw" (20-year-old female).

The participants conveyed a wide array of personal anecdotes about how having experienced or having heard about negative privacy-related events on SNSs later triggered

the availability heuristic in their SNS use. The focus group interview data provide evidence that the availability heuristic can be a reason that prevents people from engaging in specific risky disclosure behavior (e.g., sending nude photos) or can affect people's general use of SNSs (e.g., becoming more cautious about posting information on SNSs).

Optimistic Bias

Comparative optimism is a type of optimistic bias that refers to people's tendency to believe they are less susceptible to particular risks than are others (Radcliffe & Klein, 2002; Weinstein, 1980). Evidence about comparative optimism with regard to privacy risks on SNSs has been found in prior studies (e.g., Metzger & Suh, 2017), but a sense of comparative optimism was not pervasive among participants in the focus group interviews. That said, when prompted to think about their susceptibility to a negative privacy experience on SNSs compared to "an average SNS user," a few said things like: "I would just say probably others are more likely to have a bad privacy experience than I am" (20-year-old female), "I'm less likely [to have a bad privacy experience], so it's the average person" (22-year-old female), or simply responded, "average user" (21-year-old male) or "definitely not me" (19-year-old female). In one group where many participants were quick to respond that an average user is more likely to have a negative privacy experience compared to themselves, one participant described how irrational it feels to feel optimistically biased: "You feel like all this stuff is not going to happen to you, but you're like, 'oh, this would happen to someone else,' but you never think of yourself" (18-year-old female). Yet at the same time, a good number of participants reported that they do not feel comparatively optimistic about their privacy risks compared to average users because they had trouble conceptualizing what an "average user" means to them. Many participants considered themselves to be average users: "I feel like I'm an average user, I guess" (21-year-old female), or "I don't know what an average user really

is" (21-year-old female). One participant asked the interviewer: "What differentiates us from an average user?" (19-year-old female).

Moreover, most of the participants who felt comparatively optimistic about privacy risks reported that they think they are less likely to have a negative privacy experience compared to average users *because* they are more cautious about what they post in general. One participant believed that she is not susceptible to having a negative privacy experience on SNSs because of the way she uses social media: "Definitely not me, I'm like locked down" (19-year-old female). Another participant similarly thought his optimism was due to his particular style of SNS use: "I would say I'm less susceptible because I share less. And that gets reaffirmed just by hearing more stories on the news about people who did get things shared that were not supposed to be shared" (20-year-old male).

The interview participants were all young adults, and some of them attributed their comparative optimism to their tech-savviness. These participants believed that being a "digital native" made them invincible to privacy threats because they knew how to protect themselves: "We grew up using social media, so I feel like we kind of just know the ins and outs of it" (20-year-old male). Also, one participant referred to young adults including herself as "we" to indicate that they, as a group, are less likely to have a negative privacy experience because of the way they manage their privacy on SNSs: "I feel like we still think before we post. We're not just going to post everything and anything" (18-year-old female). These responses seems to reflect a group-level optimistic bias, in which a group of young adults feel that they are less likely to have a negative privacy experience than users in other age groups.

Among the participants who felt comparatively optimistic about privacy risks, only a few explicitly said that their sense of comparative optimism makes them feel more

comfortable about sharing information on SNSs. For example, one participant described how she feels comparatively optimistic (because she believes she is more cautious about posting information on SNSs than others are) and how that optimism makes her feel safer to post information on SNSs: "I have best friends that post things that they wouldn't allow normal, just anybody to see. So I definitely think that by being overly cautious and having so many privacy settings on and then only allowing your friends to see, I do think in that situation you are more likely to share more about yourself because you feel like it's safer" (21-year-old female). While instances like this were rare in the interviews, they show how a sense of optimism, combined with some sense of security that comes from the bubble heuristic in the above case, could increase the impulse to disclose information, which lies at the heart of how the comparative optimism heuristic is theorized to influence disclosure.

Interestingly, although comparative optimism is known to be a robust phenomenon that operates across contexts and affects most people, a few female participants said they felt comparatively *pessimistic* about their privacy risk on SNSs. These participants stated that they believed that women are more likely to have a negative privacy experience on SNSs than are men, and thus thought they would be more susceptible to privacy risk because they are women. For example, one participant described the gender difference in users' privacy risk based on what she observed on SNSs: "I feel like probably [I am more susceptible], not because of past experience, but because I'm female, and I feel like women typically have worse experiences with it…I just feel like the standards are a lot higher [for women]" (18-year-old female). Another similarly said: "I feel like it's more like young females that are more likely [to have a negative privacy experience on SNSs]" (21-year-old female). Both male and female participants in focus groups that discussed the gender difference in privacy risk on SNSs generally agreed that women are more vulnerable to privacy risks on SNSs than

are men. Even though he had a negative privacy experience in the past, one male participant reported that he feels less susceptible to privacy risk compared to women: "I also know that I have been personally friended by a weird account, a nude account or something like that, from someone I don't know. But I do find it's more often that it happens to girls than guys" (21-year-old male).

In sum, although the evidence of comparative optimism is well-documented in multiple domains (e.g., Dillard, McCaul, & Klein, 2006; Helweg-Larsen & Shepperd, 2001; Shepperd, Helweg-Larsen, & Ortega, 2003; Wei, Lo, & Lu, 2007; Weinstein, 1980), the focus group data were somewhat inconsistent with existing findings on comparative optimism about privacy risks on SNSs. As mentioned above, Metzger and Suh (2017) found empirical evidence of comparative optimism about privacy risks on SNSs in a sample of 1156 nationally representative Facebook users using the same question (i.e., "Who do you think is more likely to have a bad privacy experience as a result of using SNSs, you or an average user?"), whereas several participants in the current focus group interviews had trouble imagining and conceptualizing an average SNS user. This finding might be unique to this sample, which is entirely comprised of young college students, and/or it might be a result of the differences in research methods used in the two studies. While the 2017 study collected anonymous self-report data, the current focus group study method forced participants to state aloud to fellow students if they felt superior to others. This type of face threat may have made it difficult for them to admit to comparative optimism. The current results could also reflect a shift in SNS users' privacy perception as a result of extensive media coverage of privacy scandals in social media in the last two years, most notably widespread news coverage of the Cambridge Analytica scandal and its political fallout, such as Mark Zuckerberg's congressional testimony.

While the focus group interview data do not provide strong evidence of optimistic bias in general, it is interesting to note that many participants thought that gaps in SNS users' susceptibility to privacy threats was determined as a function of users' gender and age. These factors should be examined further using a larger and more generalizable sample of SNS users. Such a study might help to explain why the current data did not provide as much evidence of optimistic bias as has been found in previous studies since it is based on a sample that consisted of young adults who were mostly (77%) female.

Finally, in contrast to prior findings about how optimistic bias leads people to engage in *riskier* behaviors because they feel like they are less susceptible to harms than are others, this may not be the case for optimistic bias about privacy risk on SNSs. As demonstrated by some participants' responses in the current focus group data, their optimistic bias about privacy risks on SNSs might be justified because they reflect a realistic assessment of their privacy risk on SNSs in the sense that they are comparatively more cautious about their privacy and disclosure compared to others. In other words, although optimistic bias has been treated as a positive predictor of risky privacy behavior, SNS users' optimistic bias about privacy risk may instead be a result of their *cautious* disclosure and privacy-related decisions. Recent findings by Yu and colleagues (2015) support this (reverse) causal direction between SNS users' optimistic bias and disclosure decisions, as they suggest that SNS users may be assessing their privacy risk based on what they have already disclosed. However, since Yu and colleagues measured people's perception of their general online privacy risk, but not their optimistic bias, the relationship between users' optimistic bias about privacy risk on SNSs and their disclosure decisions should be further examined in future studies.

Bubble Heuristic

Consistent with the bubble heuristic, which refers to online enclosures that provide a sense of security for people (Gambino et al., 2016), many participants discussed how they create a "safe space" for themselves by managing the membership and size of their audience on SNSs. They use privacy settings and/or let only certain people follow their account to make sure that their information is shared with a curated group of people. The focus group data show that feeling like they are in an "enclosed" space online triggers the bubble heuristic and makes them feel safer about posting on SNSs. One participant talked about how she feels safer about sharing her location on Instagram after she made her account private: "Before I was really nervous about saying my location is at UCSB because anyone can see this, but now that it's on private, I feel more okay…it's not like the whole world is going to see where I am" (21-year-old female). Another participant compared how she feels about posting on different SNSs depending on the followers of these accounts:

> When I post on Instagram, I don't really think about it too hard because I know who all of my followers are…Whereas with Twitter I think about it way more because I know it's not only getting to my followers, but if they like it, then it gets to their followers and so on and so forth. (20-year-old female)

Feeling safer in a self-created online bubble not only makes users post more, but also post more private content. One participant reported how using privacy settings makes her feel safer to post more on Snapchat: "I think privacy settings makes me post more. For Snapchat, you can control who sees your Stories, but you can also control who you send the individual snaps to, so it makes me send more" (19-year-old female). Another participant talked about how the bubble heuristic affects the way she posts on SNSs: "For me, [feeling safe] makes me share more, just because if I know it's on private, none of my family is going to see anything…but something as simple as a bikini picture, I wouldn't post something like that if

I had family on there" (19-year-old female). Types of private content participants mentioned they would share on SNSs when they feel safe include their locations, pictures or videos from parties, and alcohol and drug use.

Many participants discussed the trend of making a "finsta" (i.e., fake Instagram), which is a private Instagram account users create to share private content with a small number of followers whom they trust. One participant talked about the strict standards he applies to decide whether he would let someone follow his finsta: "[Finsta is] having even more select group of people that are all my close friends. I wouldn't let anyone follow me on finsta…unless I personally trusted them—trust them not to show it to other people as well" (20-year-old male). The popular trend of creating finstas reflects how users want an online enclosure for themselves to safely disclose information on SNSs. The interview data show that being on a finsta triggers the bubble heuristic for users to share a greater amount of information that includes more private content compared to their other social media accounts. One participant described how her finsta is different from her public account: "I share more on finsta because it's just my very close friends, because I'm not opening up, and I have a public Instagram, so it's a really big difference to me… So on finsta, it feels more safe" (21-year-old female).

Participants who reported to have a finsta discussed how the bubble heuristic affects what they share information in their finsta. One participant said she feels comfortable posting anything on her finsta: "I definitely think that smaller community and knowing that privacy is there has allowed me to just post whatever I want" (21-year-old female). They report that the content on their finstas includes posts that contain more authentic or personal emotions. One participant described her finsta as an "emotional diary" (19-year-old female), and another participant also discussed how her finsta serves as a platform for a "raw, emotional

post" (21-year-old female). Participants who had finstas often mentioned their alcohol and drug use as a topic they would discuss on this account. One participant described an example of a post that she would share on her finsta: "If I have bags of weed, I'll be like, 'oh my god, look at all this weed that I have'… No, they would never end up anywhere near my main account" (21-year-old female). Another participant shared the types of posts she often saw on others' finstas: "Like, drunk pictures a lot. I've seen a lot of drunk videos, or you know, like obvious references, like 'I was so high in this picture' or 'I was like…rolling or something'…most people wouldn't put that on their regular Instagram" (21-year-old female). Lastly, many participants also listed nude photos or videos as a type of content that would often appear only on finstas. When one participant mentioned how she frequently sees nude photos on others' finstas, another participant in the group added, "Yeah, like all my friends do" (19-year-old female). The amount and types of content users report to share on finstas in the interview data provide evidence of how the bubble heuristic can influence people's disclosure on SNSs.

In sum, the focus group interview data show that the feeling of being in a safe space with other users that they have carefully selected triggers the bubble heuristic and makes them feel more comfortable and safer about posting greater amounts and/or more sensitive or private information on SNSs. Moreover, participants' responses to our questions on this topic suggest that users do not think much about other privacy risks associated with posting such information, such as lower chance of employability, information misuse by others, or negative judgments by those in their social networks, when the bubble heuristic is triggered.

Homophily Heuristic

Consistent with the homophily heuristic, which refers to people's tendency to associate more with similar others than with dissimilar individuals (Lazarsfeld & Merton,

1964; McPherson et al., 2001; Rogers, 2003), most participants reported that they feel more comfortable about posting on SNSs and post more when they felt similar to their followers. The homophily heuristic appears to reduce their worries about being judged negatively on SNSs and lets them feel like their posts (and thus their selves) would be approved by others. One participant explained that he would post more if he felt similar to his followers "because you think people are going to [better] understand what you post" (21-year-old male). Another participant assumed that similar people post similar types of posts and thought feeling similar to her followers made her feel safer to post information on SNSs: "Because you know that they're going to be posting or sharing the same things, so no one can really judge anyone. Everyone's doing the same thing" (21-year-old female).

The homophily heuristic seemed to have a stronger effect on users' disclosure decisions when they felt *dissimilar* to their followers. The interview data showed that users hold back from posting certain information when they do not feel similar to their followers. In many focus groups, participants listed sensitive topics they would not discuss on SNSs if they did not feel similar to their followers, including religion, mental health, and alcohol and drug use. The most frequently-mentioned topic they said they would avoid discussing on their SNSs was politics, especially when their contacts were more politically diverse. Many participants thought discussing politics could result in disagreements or arguments with some of their followers: "Politics is something I avoid on Facebook because I don't like to get in heated conversations on a public platform… I don't want thousands of people to see this thread of argument about abortion or something" (21-year-old female). Participants' feelings about sharing their political views is consistent with the Pew Research Center's (2019) recent survey results about discussing politics on SNSs based on a nationally representative sample

of U.S. adults. More than two-thirds (68%) of U.S. adults find it stressful and frustrating to talk politics with people they disagree with politically on SNSs (Anderson & Quinn, 2019).

Because the focus group participants were young adults with more politically liberal views, having older family members as their followers triggered the homophily heuristic for them: "I'm a big LGBTQ supporter, and I can't really post much about that on my Instagram especially because I have family members who are way older, and they don't support that" (18-year-old female). Moreover, a few participants mentioned that just one follower who they consider to be dissimilar to them could trigger the homophily heuristic: "My 65-year-old English teacher follows me on Instagram, my main [account] and my Twitter, so that's kind of my gauge of appropriateness. Like 'would Mr. Gage want to see this?' Probably not" (19-year-old female). These examples show that the homophily heuristic is triggered when SNS users feel dissimilar to their followers in such a way as to influence what they choose to disclose on those platforms.

Bandwagon Heuristic

Participants in the focus groups provide evidence that the bandwagon heuristic—people's propensity to go along with the crowd in terms of beliefs, ideas, and behaviors (Lee & Sundar, 2013; Sundar, 2008)—influences participants to create specific posts that are similar to others' disclosure (i.e., posts) on SNSs. When users see others creating posts about a specific topic on SNSs, they feel compelled to create a similar post on their account. One participant reported that she felt a type of social pressure to post about Halloween: "During Halloween there's a lot of pressure. Everyone is posting their cute Halloween pictures, and I'm like, 'Oh dang, I have to post, too,' which is weird because you don't have to post, but I feel like…I should include mine" (19-year-old female). The focus group data provided a long list of examples that the participants have posted after seeing others do so, including posts

about: holidays (e.g., Halloween, New Year, Mother's Day, etc.), party pictures, pop culture references, profile pictures that are relevant to current events (e.g., profile picture with a rainbow filter to celebrate the legalization of gay marriage in the U.S., painting that combines the peace sign and the Eiffel Tower in response to terrorist attacks in Paris in 2015, etc.), posts that support a social cause (e.g., ALS ice bucket challenge to promote the awareness of amyotrophic lateral sclerosis, etc.), music festivals, and more.

Seeing other people create posts also led participants to engage in activities just to upload a similar post on their SNS accounts. One participant reported that she painted her own version of a "Peace for Paris" symbol to be part of the movement she saw others on her SNS doing: "I felt like I was a part of like a movement where I was just making it aware…all my artist friends were posting their own versions of it, so it was kind of cool to be part of that." (21-year-old female). Another participant described the experience of going to a trendy location to take pictures, so that she could post a photo from that location like others she saw on SNSs: "It sounds so stupid, but sometimes my friends and I will go to the city just to take pictures…we went to the Museum of Ice Cream in San Francisco, and we paid 50 bucks for tickets to go take pictures" (19-year-old female). The interview data showed that the bandwagon heuristic has a very strong impact on users' decisions to share information. Several participants mentioned the phrase "Do it for the 'gram" (20-year-old female), which reflects users' impulse to engage in a certain activity just to share that experience on their Instagram, especially if they saw others doing the activity.

When asked to answer the question, "What is the motivation for posting what others post?" participants listed several different reasons within seconds, including: "To fit in and be accepted" (20-year-old female), "To solidify yourself as part of something" (21-year-old female), and "To show that you share common ideas" (22-year-old female). These sorts of

reasons for sharing information as a result of the bandwagon heuristic were observed across many of the focus groups.

Another aspect of the bandwagon heuristic is that participants reported they use specific features on SNSs because they see others using them: "I didn't start posting on Snapchat Stories until I saw that all my friends are doing it…I was like, 'okay, this is a normal thing that people are doing, so I'll do it, too'… it's just kind of pack mentality" (19-year-old female). Others explained that it makes them feel safer when they use SNSs in a way that others do, even for more risky or sensitive information, because it lowers the amount of felt risk they feel: "It makes me feel a little more comfortable because like the odds of something super great or horrible happening to me isn't great because of how many people there are" (19-year-old female), whereas another participant said "the idea is that if you're at risk, they're at risk too, you're in this together" (26-year-old female).

The bandwagon heuristic not only appears to affect SNS users' decision to disclose certain kinds of information on SNSs, but other privacy-related decisions as well, including selecting privacy settings for their accounts. One participant discussed how she considered selecting a more restrictive setting that could help manage her information better: "I have a few friends who go on private…and the reason for it is because they're trying to get hired for a job or something…it always reminds me, 'oh, I should be a little more cautious" (21-year-old female). A few participants have also reported that they have actually selected more restrictive privacy settings as a result of noticing others' privacy settings. For example, one participant said she began using the "ghost mode," a new privacy setting that disables the Snapchat Map (i.e., a new feature that shows the location of Snapchat users on a map) as a result of seeing others using that setting: "At first when the [Snapchat Map] came out, everyone had theirs on, so I didn't care. But then I noticed people…turning ghost mode on,

and so I put mine on too" (19-year-old female). One participant explained that seeing others' more restrictive privacy settings made her feel uncomfortable about having her privacy setting as public and eventually led her to change her privacy setting:

> I just recently changed mine to private…I just started noticing a lot of people here at school had theirs on private, and mine was on public, and I was just like, is it kind of icky? Is it a bad idea for it to be on public? (21-year-old female)

On the other hand, a few participants' responses show that seeing others' privacy settings can lead them to change their own privacy settings in a way that exposes them to *more* privacy risk. One participant said, "a lot of my friends aren't private on Instagram, so I thought maybe I should just not be private, who cares" (18-year-old female), and another said, "A lot of my friends don't have their [privacy settings] on, so I turned mine off and get more followers that way" (18-year-old female). This is further evidence of a bandwagon effect. However, because changes in others' privacy settings are usually not visible once users are connected on SNSs, information about updates on others' privacy settings come from these users themselves, which is rare. Consequently, only a few focus group participants mentioned the bandwagon heuristic affected their decisions to review or adjust their own privacy settings on SNSs.

In sum, the bandwagon heuristic appeared to influence users' decisions about disclosure on SNSs because other users' disclosures (i.e., posts) are usually readily visible on a feed that is prominently placed on the SNS (e.g., News Feed on Facebook, etc.). In most cases, privacy risk as a result of bandwagon forces is minimal; however, sometimes when users decide to disclose information on SNSs because they see others posting the same type of information, they expose themselves to privacy risk. For example, selecting profile pictures that are related to current events such as a concert or protest can reveal users'

location, tastes, or political views to unknown others. In other words, the bandwagon heuristic may increase privacy risks in some situations. And like others who have found the bandwagon heuristic to have a positive impact on behaviors that can protect SNS users from privacy risks (Lewis, Kaufman, & Christakis, 2008), we found a few instances of users adjusting their privacy settings to be more restrictive because their friends did so. And, also consistent with the bandwagon heuristic, we observed that users sometimes made their privacy settings more public when they saw others reaping the social benefits of having a public profile (e.g., receiving more likes or getting more followers to their account), which is also a form of the bandwagon heuristic.

Inequity Aversion

The focus group interview data provided some evidence of inequity aversion—people's tendency to resist unfair outcomes (Fehr & Schmidt, 1999)—as either a disclosure or privacy heuristic operating to affect SNS users, albeit only among a small proportion of the interviewees. For example, one participant described how she thought certain posts made people enjoy the social benefit of "looking cool" and wanted to create similar posts: "I know when I look at other people's Instagrams, and it's really cool, and they look really good, it makes me go, 'dang, I should do that because I want to look cool and pretty, too' [group laughs]" (18-year-old female). Another participant shared a thought he has when he sees others' posts receive positive reactions on SNSs: "I think it can get competitive in a way, 'so she got this many 'likes,' I bet I can post this picture and get even more" (20-year-old male). Similarly, another participant discussed how she decides the number of likes she needs to be content with as the reaction to her posts: "my standard in my head of how many likes my picture should be getting is definitely compared to my friends…I'll definitely notice as I scroll…how many likes my friends' pictures are getting—and that's how I build my

standard" (21-year-old female). In addition, one participant explained how she coordinates the timing of when she posts on SNSs with her friends to make sure everyone's posts get a similar amount of exposure and potentially positive reactions:

> Me and my friends do this where we show similar pictures and make a schedule of when we're going to post them because we do have the same following, [and] we don't want them to be repetitive. We schedule it out because we think it does matter...basically to show it was cool. (19-year-old female)

On the other hand, many participants indicated that they did not think SNS users feel a need to avoid unfair social outcomes in their SNS use, and thus inequity aversion was not a motivator for disclosure on SNSs. When asked to discuss the role that inequity aversion plays in their SNS use, some participants even denied that they compared themselves to others or that their impression management efforts were at least partially caused by social comparison: "I want to get more likes, but I don't necessarily compare myself to [other users]. I got 300 likes this time, next time I'll try to get 350" (20-year-old male). And while some participants reported that they do experience fear of missing out (FOMO) when viewing others' SNS posts, they then said that it did not affect their disclosure behaviors. These participants explained that their experience of FOMO only affected their offline activities, but not their online activities, for example: "Sometimes I'm home, and everyone is out and about…and I'm like, 'dang, they're doing cool things. I want to get out there.' So I guess that influences what I do. It's not to share necessarily, but to do something" (18-year-old female).

Interestingly, while the majority of the participants did not think inequity aversion affected how they disclose information on SNSs themselves (which may be difficult to admit), some participants said they could see it affecting *others'* disclosure. For example, instead of describing her own experience, one participant discussed how she thinks inequity

aversion could influence others' behaviors: "People always want to prove that they're doing something better or more exciting than you…I definitely think people go to things sometimes specifically motivated for a picture" (21-year-old female). Later in the interview, the same participant admitted that inequity aversion used to affect her own SNS use:

> I would see someone else who posted right before or right after me, and I'd be like 'oh my god, they're getting more likes, and then I'd check their followers, and I'd be like 'oh, they have more followers,' or 'oh, they have less followers, no!' It became one of those things where I was like 'this is not a healthy self-talk,' so I just kind of like put it away and started posting less. (21-year-old female)

So, although only a few participants discussed how inequity aversion influences their SNS use, some participants' comments seemed to indicate that inequity aversion might affect more people than the participants were willing to discuss in the focus group interviews. One participant shared a thought that implies that people add posts to their SNSs to get the social recognition for engaging in a certain activity: "There's a phrase, well it's more like a joke, but it's that 'if you don't post a picture about something, did you even go?'" (20-year-old female). Another participant shared a similar phrase in response: "Pics or it didn't happen" (21-year-old female). These examples seem to suggest that SNS users gain positive social recognition for posting about their activities, and that individual users are motivated to add posts to their accounts to get positive social recognition on SNSs.

In a way, inequity aversion affects SNS behavior similarly as the bandwagon heuristic because it leads people to post more when they see that others are gaining social benefits from posting on SNSs. One participant described the experience of seeing other users getting positive reaction to their posts and feeling motivated to create a similar post: "[When I see cool posts], I'll remember it, and then when I'm out and doing something

fun…I'll be like 'oh, I'm gonna pose in this certain way because that one picture looked really cool, and I'm gonna copy that'" (21-year-old female). This example illustrates that the effects of the bandwagon heuristic and inequity aversion may be too highly intertwined for them to be considered as two separate heuristics. Noticing others' posts and deciding to post similar content as others to get more positive responses could be simultaneously motivated by both the feeling of safety or comfort when users see others post a similar type of content and by the desire to receive favorable social feedback on their content to reap the same social benefits as other users do. Although the scant evidence about the effect of inequity aversion on users' disclosure decisions found in the focus group interview data is not enough to settle the question, it is also possible that the few anecdotes showing an effect of inequity aversion on privacy-related behavior reflect a specific type of instance that should be better categorized as a subset of the bandwagon heuristic. In any case, these results suggest more research is needed.

Hyperbolic Discounting

Hyperbolic discounting refers to inconsistent time discounting that is often used to explain people's preference for immediate gratification rather than delayed rewards (Ainslie & Monterosso, 2003; O'Donoghue & Rabin, 2000). Hyperbolic discounting in the SNS privacy context implies that a user is aware of a distal privacy risk from disclosing some information in the moment, yet decides to disregard it for immediate gratification and disclose the information anyway. To get at this idea, participants in the focus groups were asked if they could recall an experience in which they later regretted posting some information on SNSs. Many of the participants, who are young adults, discussed the experience of regretting and/or deleting a post they had created while they were intoxicated. However, these instances do not really reflect the hyperbolic discounting heuristic because

they may not have been aware of any potential privacy risk associated with sharing a "drunken post" at the moment of sharing due to their inebriation. Rather the awareness of risk only occurred once they sobered up later. For example, one participant reported that she deleted a post that she shared while intoxicated, but said that she was not thinking about the potential risk when she created that post: "When I am drunk, mostly I'm just like, 'Yay, this is fun,' and not thinking about it too hard. And then the next day, it's kind of weird that I did that, and then I just delete it" (19-year-old female). In response to this statement, another participant questioned whether that participant's decision was affected by hyperbolic discounting: "But do you know that you're going to regret it [in that moment]? Because you're just so in the moment sometimes that you're not really thinking about the consequences" (22-year-old female). Another participant replied "I think you're just in the moment and do it, and then when you get out of the moment, it's just, 'wait, I didn't need to do this'" (20-year-old female), which seems to indicate that posting while intoxicated is not a result of hyperbolic discounting.

Evidence for hyperbolic discounting was, however, mentioned by some participants, and it typically had to do with emotion. These participants shared experiences where they regretted posting on SNSs later but decided to post anyway in the heat of the moment because they were experiencing intense emotions. In particular, anger and sadness led to hyperbolic discounting of distal privacy risks, where users recognized the risk at the time, but created posts they knew they might later regret anyway. For example, one participant explained how she understands the risk of sharing emotional posts on SNSs, but she shares them despite the risk due to the immediate benefit she gains from the act of sharing her feelings (e.g., about romantic relationships) with her social network: "I might tweet if I'm really upset, and I just need to let it out…I have friends I can tell, but…I don't know why I

look to Twitter to do that. And then I'd regret it" (21-year-old female). Another participant described how her awareness of potential risks does not stop her from sharing emotional posts on SNSs: "Like in heat of the moment or anger, I used to post stuff that I knew was just going to start fires, start drama, and then I would definitely regret it later, like 'why would I do this?'" (21-year-old female).

Because hyperbolic discounting requires users' awareness of distal privacy risk, it likely involves a more rational decision-making process than the other heuristics. As hyperbolic discounting resembles the process of privacy calculus—deciding to share information despite the awareness about potential risks—our data show that it does not seem to be triggered easily in users' SNS use except in rare and extreme cases in which users feel intense negative emotions. In any case, hyperbolic discounting might be a result of a quick privacy calculus calculation that suggests to users that the immediate benefit (e.g., cathartic release of emotional expression) outweighs any potential distal privacy risk.

Ephemerality Heuristic

Consistent with Gambino and colleagues' (2016) evidence of the ephemerality heuristic, which is triggered by the use of ephemeral features in messaging applications that makes people feel safer about sharing information, most participants reported that they feel safer to share posts that disappear in 24 hours on SNS platforms as well (e.g., Snapchat, Instagram Stories). When asked to select an SNS that feels safest to them, many participants chose Snapchat because it is a platform where users mainly share ephemeral posts. For example, one participant said, "I would say Snapchat is probably the safest just because…it disappears after you view it or after 24 hours" (20-year-old male), while another said, "probably Snapchat [feels the safest to me] because it disappears" (19-year-old female). The

fact that their posts will not be online permanently instilled a sense of safety among the participants.

The ephemerality heuristic seemed to have a similar effect on participants' SNS use as the bubble heuristic because in this case it provided a temporal "enclosure" that made them feel safer. When participants were asked to compare the degree of safety they feel when sharing ephemeral posts compared to permanent posts, many participants agreed that they notice a difference between the two. One said, "I feel like it's gonna go away, so [I feel] a little bit better [sharing ephemeral posts]" (20-year-old female), and another said: "I think I do feel safer because some people are not active users on their account, so they won't see it, and it's going to disappear anyway" (19-year-old female). In addition, one participant even stated that the ability to share ephemeral posts made her trust that SNS as a whole: "I've always kind of trusted Snapchat because your stuff gets deleted instantly, so I do whatever…I'll post Stories without really thinking twice about it just cause it's kinda trustworthy, and I never felt like I'm putting myself at risk" (19-year-old female).

This heuristic appears to lead users to post a greater amount and a wider variety of content in their posts. One participant viewed this effect of ephemeral heuristic to be positive, reporting that she could be more genuine on SNSs when she can share ephemeral posts: "I feel like I can be more myself on there, because it's going to go away" (19-year-old female). On the other hand, many participants admitted that they could not care less about the consequences associated with ephemeral posts: "Because it's up for such a short time, it doesn't feel as important as posting something that will be there for a long time" (19-year-old male). Another participant similarly admitted that she thinks less about ephemeral posts: "For Snapchat, because it just like disappears, you don't really put as much thought into it." (19-

year-old female); she then shared a time that she felt embarrassed due to an ephemeral post, and how the ephemerality heuristic may have exposed her to privacy risk:

> It's kind of less safe, like you're moving really fast when you're on Snapchat…you just post it because you think it's low risk because it just disappears, but I think that kind of creates a false safety net because you're moving so fast. I know I've sent stuff to people that I didn't mean to send it to before…so it was hella embarrassing. So, I think in that way if you're moving fast through it, [it involves] higher risk at least when I think about it. (19-year-old female)

This quote implies that the effect of ephemerality heuristic on privacy reasoning is sometimes subconscious and occurs because people do not think as carefully about the risks of disclosure when they know a post disappears quickly. Similar to this participant, many others explicitly remarked that they felt safer about posting any type of content, ranging from mundane daily activities to "promiscuous pictures" (19-year-old female) via SNS platforms that offer ephemeral features.

Conversely, many participants felt that posting on permanent platforms (e.g., Instagram grid, etc.) requires a rational decision-making process because they are reserved for "special" (i.e., more thought out and higher quality) posts: "[Compared to Instagram Stories], I feel like for Instagram itself, you kind of have an expected quality of content you have to produce" (21-year-old female). Furthermore, a participant reported that her posts on the permanent platform not only have to be good in quality, but also need to go well with the rest of the posts she has on that platform: "I feel like Instagram posts have to line up with your aesthetic…Stories can just be whatever" (19-year-old female). The distinctions users make between sharing permanent and ephemeral posts highlight the effect of the ephemeral

heuristic, which can make people feel more comfortable about posting greater amounts and types of content using ephemeral features.

While most participants shared evidence of how the ephemerality heuristic affected their disclosure decisions, some reported that they rationally assess the risk associated with *all* of their disclosures on SNSs. One participant reported that ephemeral features do not affect the way she discloses information on SNS because she believed that "24 hours is a long time" (21-year-old female). Nonetheless, overall the focus group data provided ample anecdotes that demonstrate the effect of the ephemerality heuristic on users' disclosure decisions.

Summary

The exploratory focus group interview data provide insight into the extent to which the nine privacy heuristics may influence users' privacy-related decisions and behavior on SNSs (see Table 2 for a summary of findings). Overall, the data show that people have stronger recognition of and perceive stronger effects of some of the hypothesized heuristics than others. Plenty of anecdotes illustrate the role of the availability heuristic, bubble heuristic, and bandwagon heuristic in SNS usage regarding disclosure and privacy. Focus group participants discussed many ways that these heuristics affected both their privacy and disclosure decisions. Besides these three, the focus group data revealed that other privacy heuristics seemed to affect users' decisions and behaviors under more limited conditions. For example, the affect heuristic operated primarily to deter people from using or disclosing more information on a SNS when they had negative views of the company that owns an SNS, rather than spur disclosure due to positive affect as most accounts of the affect heuristic predict. That said, the findings still support the reasoning underlying the affect heuristic. Also, the homophily heuristic was more instrumental in influencing users' behavior when

they thought their audience was *dissimilar* to them, rather than when users felt *similar* to their social media audience, which it is important to note also supports the logic underpinning the homophily heuristic.

A few heuristics, however, seemed to have a relatively small influence on SNS users' decisions. While comparative optimism is known to be present in people's process of assessing most risks (e.g., health-related risks, likelihood of getting into a car accident, etc.), the focus group data provided only a few anecdotes linking participants' comparative optimism about privacy risks to their privacy and disclosure behavior on SNSs. In addition, the majority of the focus group participants did not seem to think that their privacy-related decisions were affected by feelings of inequity aversion during their SNS use. However, participants' answers to some of the questions may have been affected by social desirability biases that could be induced by being in focus group interviews which are relatively public. This would be especially so when admitting to engaging in social comparison (i.e., admitting inequity aversion or perceiving comparative optimism) in front of others. Thus, further investigation of these heuristics using other methods is warranted.

Relatedly, while the focus group data help explain how heuristics affect SNS users' privacy-related decisions, this method may have resulted in two limitations to understanding the role of cognitive heuristics in SNS users' decisions. First, it does not provide insight into a representative population of SNS users because the small sample used in these interviews consisted entirely of college students who share very specific demographic and other characteristics—young adults who have high level of education and reside in the same city, who have more politically liberal attitudes than the general U.S. public, and who have spent a greater proportion of their lives interacting with others via social media. Second, although it might seem easier for participants to admit to making decisions that exposed themselves to

greater privacy risk if they see and hear other participants in the focus groups admitting to doing the same thing, the opposite may also be true. As noted above, focus group participants might not have felt comfortable admitting to falling prey to some of the heuristics (e.g., inequity aversion) that they were asked about; therefore, this method may have prevented or decreased some participants' willingness to share personal anecdotes that illustrate the effect of those heuristics in a nonrandom manner.

Because the focus group interview data showed that the participants report a stronger recognition of some heuristics operating to affect disclosure and privacy decisions on SNSs but not others, addressing these limitations in future studies using different methodological approaches might help shed better light on how each heuristic that was assessed in our focus group interviews might affect SNS users' privacy-related behavior. One way to complement the current focus group interview data is to take a quantitative approach by conducting a survey-based study. Doing so could help more clearly understand how these heuristics affect SNS users by using a larger and more representative sample and by giving participants the chance to answer the same questions anonymously without others' presence. It also offers an opportunity to measure the magnitude of correlations between the heuristics and SNS users' privacy and disclosure behaviors.

Table 2

Privacy and Disclosure Heuristics on SNSs: Summary of Findings from Study 1

Heuristic	Heuristic Triggers	Possible Effects on Disclosure	Possible Effects on Privacy Settings
Affect Heuristic	People's liking of SNS platforms	When people like using SNSs, they share more information on those platforms.	N/A
	People's negative feelings about SNS companies	When people have negative feelings about SNS companies, they share less information on those platforms.	
Availability Heuristic	People's recall of personal and/or others' negative privacy-related experience on SNSs	People who have had a negative privacy-related experience on SNSs and/or have heard of others' negative privacy-related experience on SNSs share less information on SNSs.	People who have had a negative privacy-related experience and/or have heard of others' negative privacy-related experience on SNSs engage in privacy protection strategies, such as changing privacy settings, blocking or restricting people, or contacting SNS platforms for support.
Optimistic Bias	People's belief that they are less likely to have a negative privacy-related experience on SNSs compared to an average user	People might share more information when they feel comparatively optimistic about privacy risk on SNSs.	N/A
		Alternatively, people might feel comparatively optimistic about privacy risk on SNSs because they are cautious about what they share on SNSs	
Bubble Heuristic	People's sense of safety, security, or comfort that	When people have restricted their privacy settings, people feel more comfortable about sharing information on	N/A

Heuristic	Heuristic Triggers	Possible Effects on Disclosure	Possible Effects on Privacy Settings
	comes for privacy settings "Finsta" (Fake Instagram)	SNSs. When people have restricted their SNS audience to a select number of people, they share not only greater amounts of information, but also more sensitive information.	
Homophily Heuristic	People's perceived interpersonal similarity to their friends and followers (e.g., in terms of age or political views)	When people feel similar to their friends and followers, they share more information on SNSs, and vice versa.	N/A
Bandwagon Heuristic	People's attention to (pattern in) others' posts (e.g., holiday photos, social media challenge, etc.)	When people see others posting a particular type of content, they feel more comfortable about doing the same.	When people notice that others are changing their privacy settings, they also change their privacy settings to become either more public or private.
Inequity Aversion	People's perception of comparative social benefit from SNS use (e.g., likes, attention, etc.)	When people see that others are getting more social benefits from disclosure than themselves, they *might* post more information on social media to gain as much social benefit as others.	N/A
Hyperbolic Discounting	People's intense emotions that make them more susceptible to impulses	When people experience an intense emotion, they share information on SNSs to release or express their emotion despite their awareness of possible privacy risk associated with their action.	N/A

Heuristic	Heuristic Triggers	Possible Effects on Disclosure	Possible Effects on Privacy Settings
Ephemerality Heuristic	People's use of ephemeral features	When people use SNS features that allow them to share ephemeral posts, they feel more comfortable about sharing information on SNSs, and thus share more information on SNSs, which could range from content about daily activities to more sensitive or unpolished content.	N/A

Chapter 5: Hypotheses for Studies 2A and 2B

As described in the previous chapter, the results from Study 1 showed that the nine heuristics explored in the study are perceivable by SNS users and may be related to their decisions related to disclosure and/or privacy. Moreover, data from Study 1 showed that some heuristics influence SNS users' decisions about disclosure (i.e., sharing information), whereas others influence their decisions about privacy (i.e., limiting others' access to their information or engaging in behaviors that result in the opposite effect of disclosure), and still others affect both disclosure and other privacy-related decisions (i.e., these heuristics may function as both "disclosure" *and* "privacy" heuristics. The findings from the focus group interviews also reflect the dialectical framework that considers disclosure and privacy as opposites (CPM theory; Petronio, 2002) and inform the development of specific hypotheses for the next study. In light of the findings from Study 1, below I advance specific hypotheses and research questions about how each of the nine cognitive heuristics likely impact SNS users' decisions regarding (a) disclosure and (b) privacy (e.g., use of available privacy settings), which are also listed in Appendix B.

Affect Heuristic

As discussed in Chapter 2, the affect heuristic refers to using emotions—both positive and negative—as mental shortcuts to make judgments or decisions (Slovic et al., 2007). Carey and Burkell's (2009) then-untested hypothesis that predicted positive feeling about self-expression activities on SNSs to lead people to underestimate the risk of disclosing personal information was first addressed by Yu and colleagues (2015), who found that positive affect about SNSs indirectly affects users' disclosure. The data from Study 1 also showed that the affect heuristic is a disclosure heuristic that affects SNS users' decisions to share information. The focus group interview data from Study 1 provided a number of

anecdotes about the effect of positive affect (e.g., liking of using SNSs) on SNS users' decisions to share more information, as well as the effect of negative affect on SNS users' decision to *not* disclose information on SNSs.

While findings from Study 1 provide some insight on the possible effect of the affect heuristic on SNS users' disclosure, the mechanism by which this heuristic affects SNS users' judgments or decisions needs further investigation. The mechanism undergirding the relationship between affect heuristic and disclosure on SNSs could be explained by research that shows how positive affect can lead people to underestimate the risks and overestimate the benefits associated with a certain activity or technology, and how negative affect can have the opposite effect on people's perceived risk and benefit (Alhakami & Slovic, 1994). This finding stems from prior research findings that demonstrate how people's perceived benefit and perceived risk about various hazards—which ranged from cigarette smoking and alcohol to vaccines and insulin to nuclear power and airplane travel—are inversely related regardless of the actual relationship between the benefits and risks associated with those hazards (Fischoff et al., 1978). This inverse relationship present in people's perception of risk and benefit is consistent with cognitive consistency theories (Heider, 1946; McGuire, 1968) that explain people's need for consistency across their beliefs; when people judge an activity or technology to be favorable, it is consistent for them to also believe that the same activity or technology is associated with little risk, and vice versa. The study by Yu and colleagues (2015) provides some partial support for these mechanisms because they found positive affect toward an SNS leads people to amplify the benefits of self-disclosure. Using this logic and prior research, I hypothesize that:

H1a: The affect heuristic, as reflected in the degree to which users feel affectively

positive about a specific SNS, is positively associated with their amount of disclosure on that SNS.

H1b: The affect heuristic, as reflected in the degree to which users feel affectively positive about a specific SNS, is negatively associated with their perceived risk about disclosure on that SNS.

Availability Heuristic

The availability heuristic is known to bias people's probability judgment, such that people tend to think an event that is more recent, familiar, or cognitively salient to them is more likely to occur again in the future (Tversky & Kahneman, 1973). If this event is associated with negative consequences or risk (e.g., plane accidents), the availability heuristic could influence people to avoid certain behaviors. For example, people who have experienced plane accidents or frightening incidents (e.g., severe air turbulence, emergency landing, etc.) would avoid plane travel to avoid the dire consequences they now associate with plane accidents. Prior research suggests that the availability heuristic would operate similarly with regard to privacy risk on SNSs (Debatin et al., 2009; Litt, 2013; Litt & Hargittai, 2014). A salient memory of past privacy-related negative experiences on SNSs could trigger the availability heuristic regarding users' future SNS use, which would bias users' probability judgment about the likelihood of another negative experience occurring on SNSs, and thus increase perceived privacy risk. The effects of the availability heuristic on SNS users' perception of privacy risk and their privacy-related behaviors are reflected in prior research findings that show how having a negative privacy-related experience on SNSs could trigger higher risk perceptions about future use, which could in turn influence users to select more restrictive privacy settings (Debatin et al., 2009; Litt, 2013; Litt & Hargittai, 2014).

Similarly, the focus group interview data from Study 1 show that SNS users make biased probability judgments about future privacy-related events if they had a past negative privacy-related experience on SNSs or have heard of others' negative experiences. Anecdotes from Study 1 suggest that recency, salience, and perceived severity of these negative privacy-related experiences influence how SNS users judge the possibility of having a(nother) similar experience on SNSs, how they perceive risk associated with using or disclosing information on SNSs, and how they manage their privacy on SNSs. More specifically, the findings from Study 1 show that while not all past negative privacy experience (both personal and others') affects SNS users' judgments, more severe experiences that remained salient in participants' memory were influential on their judgments about privacy on SNSs. In addition, the focus group data from Study 1 demonstrate that the availability heuristic could influence people's risk perception and decisions about both disclosure and privacy on SNSs. For example, many participants in Study 1 reported that they began to share less information on SNSs, adjusted their privacy settings to be more restrictive, or used other privacy-protecting strategies (e.g., blocking or reporting other users' accounts), as a result of having had (or heard of others having a negative privacy-related experience or incident on SNSs in the past. Given that the qualitative data from Study 1 is consistent with prior research about the role of the availability heuristic across various contexts that involve risk, the next set of hypotheses are:

H2a: The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is negatively associated with the amount of disclosure.

H2b: The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is positively associated with the perceived risk about disclosure on SNSs.

H2c: The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is positively associated with the restrictiveness of their privacy settings.

Optimistic Bias

Optimistic bias is known to be a robust phenomenon that explains people's tendency to think they are less susceptible to risks than are others (Weinstein, 1980). Optimistic bias leads people to underestimate their risk regardless of actual risk. Decades of research has shown that optimistic bias affects many types of risk perceptions (e.g., perceived likelihood of injury, disease, natural disasters, crime, etc.) and leads people to engage in risky behaviors (Dillard et al., 2006; Helweg-Larsen & Shepperd, 2001; Radcliffe & Klein, 2002; Shepperd et al., 2003; Wei et al., 2007; Weinstein, 1980). Furthermore, more recent research has also demonstrated that optimistic also affects people's online privacy risk perceptions (Acquisti & Gross, 2006; Baek et al., 2014; Campbell et al., 2007; Cho et al., 2010; Debatin et al., 2009).

However, recent empirical research shows mixed results about the effect of optimistic bias about privacy risk on SNSs (Baek et al., 2014; Metzger & Suh, 2017). These findings show that while SNS users do have optimistic bias about their privacy risk on SNSs, this does not necessarily lead them to make riskier choices on SNSs, and optimistic bias about privacy risk is sometimes higher among users who made safer decisions. In other words, optimistic bias about privacy risk was negatively associated with the amount of disclosure, which could expose them to a lower level of privacy risk. As noted in Chapter 4, the fact that there was not robust evidence for optimistic bias in Study 1 may have been caused by social desirability biases whereby focus group participants might have been reluctant to admit that they engage in social comparisons. Therefore, more data is needed to conclude if and how SNS users' optimistic bias about privacy risk affects their disclosure and privacy-related

decisions. Thus, Study 2 examines these dynamics further by proposing the following research questions:

RQ1: Is users' optimistic bias, as reflected in the perceived likelihood of having a negative privacy experience on SNSs compared to others, related to the amount of information users disclose on SNSs?

RQ2: Is users' optimistic bias, as reflected in the perceived likelihood of having a negative privacy experience on SNSs compared to others, related to the restrictiveness of users' privacy settings on SNSs?

Bubble Heuristic

The bubble heuristic has been found to evoke a sense of security that leads people to engage in behaviors that might expose them to more privacy risks (Gambino et al., 2016). For example, as noted in Chapter 2, participants in a recent study admitted that they were willing to share more information when they use personal versus public Wi-Fi networks, and that public networks do not feel like a safe space for them (Gambino et al., 2016). Consistent with this finding, the focus group interview data provided many anecdotes about how bubble heuristic influences people's privacy risk perceptions and their disclosure decisions on SNSs. Interviewees noted that the bubble heuristic was triggered when they were on specific SNSs that they thought were safer than others or when they had limited visibility of their information to a specific group of people by adjusting their privacy settings or creating finstas. SNS users reported that these actions created a sense of safety that made them feel more comfortable about sharing not only greater amounts of information, but also more private or sensitive content. Based on prior research and anecdotal evidence that describe the bubble heuristic as a disclosure heuristic, the following hypothesis are advanced:

H3a: The bubble heuristic, as reflected in the restrictiveness of users' privacy settings, is positively associated with their amount of disclosure on SNSs.

H3b: The bubble heuristic, as reflected in the restrictiveness of users' privacy settings, is negatively associated with their perceived risk about disclosure on SNSs.

Homophily Heuristic

According to the homophily principle, people tend to associate with similar others because they can communicate with similar others more easily and more effectively based on shared knowledge, beliefs, and understanding (Lazarsfeld & Merton, 1964; McPherson et al., 2001; Rogers, 2003). People's perceived similarity to others often makes them see more benefits associated with their interaction (e.g., effective communication) and lower risk associated with their integration (e.g., less likelihood of criticism or conflict), allowing similar individuals to build increased trust (Kossinets & Watts, 2009; Neubaum & Krämer, 2017). Studying the heuristic effect of homophily is especially interesting in the context of SNSs where users are connected to others from various social contexts that can range from family and friends to work colleagues and mere acquaintances or contain a high percentage of homogeneous contacts, yet the homophily heuristic has not yet been thoroughly examined in this context. The data from Study 1 revealed that the homophily heuristic could be triggered both when SNS users feel similar to their audience and also when they feel dissimilar to their audience. Participants' anecdotes showed that they felt more comfortable about sharing information when they thought their audience was similar to them, and they reported having held back from sharing information when they did not feel similar to their audience. Based on this, it is expected that:

H4a: The homophily heuristic, as reflected in users' perceived similarity to their social network connections, is positively associated with their amount of disclosure on SNSs.

H4b: The homophily heuristic, as reflected in users' perceived similarity to their social network connections, is negatively associated with their perceived risk about disclosure on SNSs.

Bandwagon Heuristic

Much prior research has shown that the bandwagon heuristic—people's tendency to go along with the crowd in terms of beliefs, ideas, and behaviors—affects many decisions online, for example, credibility assessment, purchase intentions, and online news article selection (Knobloch-Westerwick et al., 2005; Lee & Sundar, 2013; Sundar, 2008). Some recent research has also demonstrated that this heuristic affects people's decisions about online disclosure as well. Findings discussed in Chapter 2 show that people who were influenced by bandwagon cues felt more comfortable about sharing information when others provided similar information online, and this was because they perceived less risk associated with disclosing that information (Rosson & Ge, 2016; Spottswood & Hancock, 2017). The focus group interview data from Study 1 also illustrated that the bandwagon heuristic affects SNS users' disclosure decisions when using SNSs, such as Facebook, Instagram, and Snapchat. According to the findings from Study 1, SNS users indicated that they felt more comfortable about sharing information or using specific features of SNSs if they saw that others were doing the same.

In addition, Study 1 provided some preliminary information about how the bandwagon heuristic operates not only as a disclosure heuristic, but also a privacy heuristic that affects SNS users' decisions about which privacy settings to use on SNSs. Specifically,

some participants reported that they thought about or actually changed their privacy settings when they saw that others have privacy settings that do not match theirs. A few of the participants in Study 1 reported that they made their privacy settings more restrictive when they saw that others had adjusted their privacy settings to be more private, and others reported making their profiles public when they saw that others had made their profiles public. This finding is consistent with prior research that showed "network effects" in Facebook users' privacy settings (Lewis et al., 2008). Lewis and colleagues (2008) found that Facebook users are more likely to have more private profiles if their Facebook friends also have more private profiles. Based on these findings, I advance the following hypotheses:

H5a: The bandwagon heuristic, which is reflected in the extent to which users pay attention to others' posts on SNSs, is positively associated with their amount of disclosure on SNSs.

H5b: The bandwagon heuristic, which is reflected in the extent to which users pay attention to others' posts on SNSs, is negatively associated with their perceived risk about disclosure on SNSs.

H5c: The bandwagon heuristic, which is reflected in the extent to which users pay attention others' privacy settings, is positively associated with the restrictiveness of their own privacy settings.

Inequity Aversion

Research in behavioral economics shows that people resist unfair outcomes and make decisions to minimize unequal results as a consequence of inequity aversion (Clark & Oswald, 1996; Fehr & Schmidt, 1999), but it is not yet known whether inequity aversion affects people's perceptions of social benefits compared to others in the context of SNSs. It is reasonable to expect that it would, given that the visibility of social rewards on SNSs (e.g.,

number of likes that each post receives) could serve as a cue that triggers inequity aversion. Relatedly, and as discussed in Chapter 2, some prior research has shown that the "fear of missing out" (FOMO), which stems from people's need to be included in positive social experiences, presumably to receive similar rewards as others, motivates people to engage more on SNSs (Przybylski et al., 2013). Also, people compete to try to improve their "public status marker" through receiving more likes on their posts or more followers on their profiles (Herman, 2019; Rodriguez, 2019). The competitive nature of posting on SNSs may be a result of inequity aversion, which could lead users to share more information to get as much benefit as others.

Despite prior research and increasingly popular rhetoric about "toxicity" that comes from competition over social currency on SNSs, the data from Study 1 did not provide much evidence to show that SNS users resist social inequity or change their behaviors to minimize perceived inequity. But as noted in the previous chapter, social desirability effects in the context of focus group interviews may have led participants to deny their perceived inequity aversion in front of others. Thus, the role of inequity aversion on SNSs should be further investigated using a different methodology. The following research questions are proposed to further explore whether inequity aversion exists in the context of SNS use when it is studied with a method that allows participants to complete an anonymous questionnaire in private, and thus is less likely to elicit social desirability responses:

RQ3: Is inequity aversion, as reflected in the degree of users' perceived benefit compared to other users, related to their amount of disclosure on SNSs?

RQ4: Is inequity aversion, as reflected in the degree of users' perceived benefit compared to other users, related to their perceived risk about disclosure on SNSs?

Hyperbolic Discounting

Hyperbolic discounting describes people's tendency to prefer immediate rewards to later rewards (Laibson, 1997). For example, people prefer to get "one apple today" to "two apples tomorrow" (Rubinstein, 2003; Thaler, 1981). As hyperbolic discounting could be used to understand people's decisions in a wide variety of contexts (e.g., growth, self-regulation, job search, etc.) (Rubinstein, 2003), several scholars have suggested that hyperbolic discounting may influence SNS users to discount the privacy risk associated with sharing information on SNSs and decide to disclose information for immediate benefits (Acquisti et al., 2015; Acquisti & Grossklags, 2005, 2007; Kokolakis, 2017; Wilson & Valacich, 2012). Despite discussion about the possibility of hyperbolic discounting influencing people's privacy-related decisions, there is no empirical research on the effect of hyperbolic discounting on people's decisions about their privacy or disclosure. The focus group interview data provided some preliminary findings about how hyperbolic discounting could affect SNS users' disclosure decisions. As reported in Chapter 4, some participants in Study 1 said that they shared posts on SNSs on an impulse for immediate gratification, even when they were aware of the potential risks associated with that disclosure and that they have regretted making such decisions afterward. For example, those participants explained that they shared posts on SNSs when they were experiencing intense emotions for immediate gratification (e.g., cathartic release of emotional expression) even though they were aware of possible negative consequences resulting from that disclosure. Thus, I hypothesize the following:

> H6a: Hyperbolic discounting, as reflected in the degree to which users make decisions about disclosure on an impulse on SNSs, is positively associated with their amount of disclosure on SNSs.

H6b: Hyperbolic discounting, as reflected in the degree to which users make decisions about disclosure on an impulse on SNSs, is negatively associated with their perceived risk about disclosure on SNSs.

Ephemerality Heuristic

The ephemerality heuristic describes the effect of features that allow people to exchange messages that disappear after a short period of time in messaging applications (e.g., private messaging on Snapchat, Line, WeChat, etc.). As mentioned previously, Gambino and colleagues (2016) found qualitative evidence that illustrates how people feel greater comfort about sharing information if they believe that it will disappear without being stored permanently. The focus group interview data provide further qualitative support showing how the ephemerality heuristic is also applicable in the context of SNSs. Such features that allow users to share ephemeral posts that disappear in 24 hours have been introduced in many popular SNSs, such as Facebook, Instagram, and Snapchat. According to the findings from Study 1, the ephemerality heuristic makes users feel safer and more secure about sharing not only greater amounts of information, but also more sensitive information. Given that the findings from Study 1 are consistent with prior research, the next hypotheses predict that:

H7a: The ephemerality heuristic, as reflected in the extent to which users use ephemeral features on SNS, is positively associated with the amount of their overall disclosure on SNSs.

H7b: The ephemerality heuristic, as reflected in the extent to which users use ephemeral features on SNS, is negatively associated with their perceived risk about disclosure on SNSs.

Measuring Heuristic Effects: Study 2A and 2B

Because relying on cognitive heuristics to make judgments or decisions is usually a subconscious process (Bellur & Sundar, 2014; Sundar et al., 2019), it is difficult to empirically measure the presence and/or effect of cognitive heuristics. Therefore, in addition to conducting focus group interviews to gain a qualitative understanding about how cognitive heuristics operate on SNSs, two other approaches were used to provide quantitative insights into SNS users' attitudes about cognitive heuristics and their relationships to two key behaviors that have implications for their privacy risk on SNS (e.g., disclosing information and managing privacy through adjusting the restrictiveness of their account settings).

The first, or "direct," approach involves measuring the strength of SNS users' self-reported agreement with whether each specific cognitive heuristic influences their perceived risk about disclosure and their decision to disclose information and/or adjust the restrictiveness of their privacy settings in specific SNSs. This approach directly measures the effect of cognitive heuristics on people's risk perceptions and behaviors on SNSs. Using this approach, the aim of Study 2A is to assess the generalizability and quantify the findings from Study 1, while addressing the hypotheses and research questions proposed in this chapter.

Study 2B takes a more "indirect" approach to measuring the effect of cognitive heuristics on SNS users' privacy-related attitudes and behaviors. To the extent that cognitive heuristics influence people's judgments and decisions subconsciously, SNS users might not readily agree with statements that describe possible effects of cognitive heuristics on their risk perceptions and behaviors. Therefore, Study 2B will provide inferential evidence about the effect of cognitive heuristics by first measuring SNS users' predisposition or susceptibility to being influenced by cognitive heuristics, their perceived risk about disclosure, and their decisions about disclosure and privacy separately, and then studying their correlations. As described in this chapter, the ways of measuring SNS users'

predisposition to different heuristic effects (e.g., the extent to which users feel positive about a specific SNS reflects the likelihood of being influenced by the affect heuristic on that SNS) were developed based on prior research and findings from Study 1. Using this indirect approach to measure the effect of cognitive heuristics can complement the findings from using the direct measurement approach described above because it is possible that SNS users are unaware of their susceptibility to certain heuristic effects, and thus cannot self-report how much they agree with those heuristic effects.

Chapter 6: Method for Study 2A

Sample

450 participants who live in the U.S. were recruited through Amazon's Mechanical Turk (MTurk). The final sample after data cleaning included 411 U.S. adults (246 male and 165 female) between the ages of 20 and 88 years (M = 38.93, SD = 11.09). In terms of race/ethnicity, participants consisted of White/Caucasian (71.3%, n = 293); Black or African American (11.2%, n = 46); American Indian or Alaska Native (1.0%, n = 4); Asian (14.1%, n = 58); Hispanic (9.73%, n = 40) or Latino (1.22%, n = 5); multiracial (0.6%, n = 7); and "other" (non-specified) races (0.5%, n = 2). Most (89.3%, n = 367) of the respondents had attended at least some college, and 63.8% (n = 262) had earned a bachelor's degree or higher.

More than half (53.5%, n = 220) reported that they have a religion, and of those people, 40.9% (n = 90) were Christian and 36.4% (n = 80) were Roman Catholic. About a quarter (26.0%, n = 108) of the sample identified as Republican, 30.8% (n = 128) as Independent, 41.9% (n = 174) as Democrat, and the rest (1.2%, n = 5) as "other." Most (91.1%, n = 378) identified as heterosexual.

In terms of social media use, most participants (90.0%, n = 370) used Facebook, 62.8% (n = 258) used Instagram, 26.5% (n = 109) used Snapchat, and 70.3% (n = 289) used Twitter. More than half (51.1%, n = 210) of the participants reported that they used at least three of the four SNSs (Facebook, Instagram, Snapchat, and Twitter) included in this study.

Procedure

Participants completed an online survey on Qualtrics. On average, participants took about 10.5 minutes (median) to complete the survey. Responses from participants who had duplicate IP addresses (n = 2), people who appear to have lost their attention to the survey after 1 hour (n = 4), "speedsters" defined as people who completed the survey in less than 5

minutes (n = 20), and those who did not get the correct answer to two attention check questions (n = 13) were removed from the dataset. IRB approval was obtained prior to data collection.

Measures

Heuristic Effects

As described in the previous chapter, the effect of each of the heuristics on SNS users' privacy-related judgments and behaviors was measured using the approach where the participants reported their agreement with statements that describe the effect of cognitive heuristics on their risk perceptions and behaviors on SNSs (i.e., the "direct" measurement approach). The measures used in Study 2A for each heuristic are described below, but see also Appendix C for a complete list all items.

Affect Heuristic. Six items were created based on the findings from Study 1, which illustrated that both positive and negative affect about using SNSs and SNS companies influence users' perceptions of risk concerning disclosure on SNSs and their actual disclosure decisions. Participants were asked to indicate their agreement with the six items, and each item contained a statement that described how the affect heuristic, as reflected by the extent to which they feel positive about a specific SNS, influences their risk perceptions and behaviors on SNSs. Example items include, "The more I like a particular social media platform (e.g., its features), the more information I share on that platform" and "How good or bad I feel about a particular social media company affects how comfortable I feel about sharing information on its platform." These items were measured on a scale of 1 ("Strongly disagree") to 7 (Strongly agree"). The average of the six items was computed to indicate participants' agreement with the effect of affect heuristic on their judgments of privacy risk

and decisions about disclosure. Factor analysis showed this scale to be unidimensional and Cronbach's $\alpha = .85$.

Availability Heuristic. The measure for the availability heuristic was developed based on findings from Study 1, which showed that at least among many of the focus group participants, having a negative privacy experience and/or hearing about others' negative privacy experiences on SNSs influenced their subsequent privacy-related decisions. Participants were asked to indicate in two items: (1) whether they ever had a negative experience concerning privacy on SNSs and (2) if they have heard of others having negative experiences on SNSs by answering "yes" (coded as 1) or "no" (coded as 0) for each item. Participants who answered "yes" to either of these questions were then asked to report the extent to which they took action to protect their privacy as a result of their experience with negative privacy-related events on SNSs with five items (e.g., "As a result of this experience, to what extent did you reduce the amount of information you share on social media?"). This procedure resulted in two measures for the availability heuristic—one for the availability heuristic triggered by participants' own experience and another triggered by others' experience of negative privacy-related events on SNSs. Responses to the items for both scales could range from 1 ("Not at all") to 7 ("A whole lot"), and the average of the five items comprising each scale was computed to represent participants' agreement with the effect of the availability heuristic on their privacy-related decisions on SNSs. Factor analysis showed that both 5-item scales are unidimensional. Cronbach's α for the scale that measured the effect of availability heuristic triggered by the participants' personal experiences was .82, and Cronbach's α for the scale that measured the same heuristic triggered by hearing about others' experiences was .92.

Optimistic Bias. Findings from Study 1 and prior literature that examined the effect of optimistic bias in non-SNS contexts were used to develop four items to measure participants' agreement with statements that describe the effect of optimistic bias on their privacy decision-making processes on SNSs (e.g., "Because I feel I am less likely to have a negative privacy experience on social media than most people, I feel comfortable sharing my information there"). Factor analysis revealed that one item about restrictive privacy settings as a heuristic cue that could trigger optimistic bias ("I feel like other people are more likely to have a negative privacy experience on social media than I am because I have selected restrictive privacy settings") did not correlate well with the scale overall, so it was dropped, which left three items in the scale. The remaining items described the possible effects of optimistic bias on their risk perception and their decisions about disclosure or privacy on SNSs. The average of the remaining three items was used to measure participants' agreement with the effect of optimistic bias on SNSs. Factor analysis revealed the scale with three items to be unidimensional, and Cronbach's $\alpha = .83$.

Bubble Heuristic. Four items were developed based on findings from Study 1 that described the bubble heuristic as a disclosure heuristic (e.g., "Using the privacy settings on social media to restrict who can see my profile or posts makes sharing information feel less risky," "The privacy settings a platform offers users is a big factor in how much information I share on social media," etc.). Participants were asked to indicate their agreement with the four statements, and each item was measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree"). The effect of the bubble heuristic on privacy decision making was measured as the mean of responses across the four items, and factor analysis showed the scale to be unidimensional (Cronbach's $\alpha = .86$).

Homophily Heuristic. Based on numerous anecdotes from Study 1 about the effect of the homophily heuristic on people's decision to disclose information on SNSs, four items were developed to measure the effects of the homophily heuristic on disclosure (e.g., "The more similar my friends and followers on social media are to me, the less risk I feel about posting things on those platforms," "I am less likely to post my feelings or opinions when I think my social media connections [e.g., friends and followers] will disagree with me," etc.). Each item was measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree"), and the average of these four items was computed for the measure. Factor analysis showed the scale to be unidimensional (Cronbach's $\alpha = .84$).

Bandwagon Heuristic. Using the findings from Study 1 that suggested the bandwagon heuristic to be both a disclosure and a privacy heuristic, six items were developed to measure people's agreement with statements that describe the effect of bandwagon heuristic on their disclosure decisions (e.g., "If my friends and followers use specific social media features [e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.], I am more likely to use them, too") as well as their use of privacy settings (e.g., "If my friends change their privacy settings to be more or less private, I am more likely to do it, too"). Each item was measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree").

An exploratory factor analysis was conducted on the six items with oblique rotation (oblimin) using a random half of the dataset. The Kaiser-Meyer-Olkin measure verified the sampling adequacy for the analysis (KMO = .85), and all KMO values for individual items were > .81, which is well above the acceptable limit of .5. Bartlett's test of sphericity (χ^2 [15] = 603.54, $p < .001$) indicated that correlations between items were sufficiently large for the analysis. An initial analysis was run to obtain eigenvalues for each component in the data.

Two components had eigenvalues over Jolliffe's criterion of 0.7 and in combination explained 64% of the variance (see Table 3). The first factor is referred to as "effect of the bandwagon heuristic on decisions about information access" and consists of three items that explain how the bandwagon heuristic affects people's decision to share information or limit others' access to their information. The second factor represents the "effect of the bandwagon heuristic on feature selection," which refers to people's decisions to use specific features or social media platforms as a result of seeing others using those same features or platforms. Confirmatory factor analysis on the other half of the dataset revealed that the measure indeed has two components. Goodness-of-fit indicators of the CFA model were all acceptable and are summarized in Table 3. Both subscales—about the effect of the bandwagon heuristic on decisions about information access and on feature selection, which were identified by the factor analysis—had high reliabilities. The Cronbach's α for both subscales was .84. The two average values of three items in both subscales were used to measure participants' agreement with the effect of the two types of the bandwagon heuristic on their risk perception and behaviors on SNSs.

Table 3

Results of Exploratory Factor Analysis (EFA) of Bandwagon Heuristic Measure

Items	Components	
	1	2
When I see my friends or followers post about something personal or sensitive on social media, I feel more comfortable about posting something similar myself.	**0.93**	-0.07
If I see my friends or followers post about something on social media (e.g., holiday photos, etc.), I am more likely to post something similar myself.	**0.60**	0.26
If my friends change their privacy settings to be more or less private, I am more likely to do it too.	**0.69**	0.06

Items	Components	
	1	2
If my friends and followers use specific social media features (e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.), I am more likely to use them too.	-0.03	**0.98**
When my friends and followers use specific social media features (e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.), it feels safer for me to use them too.	0.30	**0.52**
If I were to hear about my friends using a new social media platform, I would probably feel more comfortable about trying that platform myself.	0.28	**0.40**

Confirmatory Factor Analysis (CFA) Results for Bandwagon Heuristic Measure

Model	χ^2	*df*	CFI	GFI	RMSEA
One Factor	81.11***	9	0.90	0.86	0.20
Two Factor	10.56	7	0.995	0.98	0.05

Inequity Aversion. Prior literature on inequity aversion and the fear of missing out (FOMO) on SNSs cited earlier was used to develop five items to measure the effect of inequity aversion on privacy-related attitudes and behaviors on SNSs. Each item contained a statement that described the possible effect of inequity aversion in the context of SNSs (e.g., "I feel motivated to post on social media when I see others getting more benefits than me [e.g., getting more likes, more attention, invitations, etc.]," "I feel motivated to use social media more often when I see others getting more benefits than me [e.g., getting more likes, more attention, invitations, etc.]," etc.). Items were measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree"), and participants' responses to the five items were averaged. Factor analysis showed the scale to be unidimensional and have high reliability (Cronbach's α = .94).

Hyperbolic Discounting. Findings from Study 1 and prior literature on hyperbolic discounting were used to develop six items to measure the effect of hyperbolic discounting on people's decisions about disclosure and/or privacy (e.g., "When debating whether to post some information, I sometimes feel the immediate benefits of posting outweigh the risks I might experience later," "I tend to post things on social media in the spur of the moment to express my feelings, even if I know I might regret it later," etc.). Participants were asked to indicate their agreement with the four statements, and each item was measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree"). An initial factor analysis showed that one item measuring people's relative perceptions of short-term and long-term privacy risks ("Avoiding future privacy-related risk is more important than enjoying the benefit of sharing posts on social media now") did not correlate well with the scale overall and the other individual items. Dropping this item left five items in the scale, and the mean of these five items indicated how strongly the participants agree that hyperbolic discounting affects their risk perceptions and behavior on SNSs. Factor analysis showed the resulting scale to be unidimensional and to have good reliability (Cronbach's $\alpha = .86$).

Ephemerality Heuristic. Anecdotes from Study 1 were used to develop three items to measure the effect of the ephemerality heuristic on people's risk perception and disclosure (e.g., "I post more Stories than permanent posts because I feel like there is less risk in posting content that disappears within 24 hours," "I am more comfortable posting on social media platforms where content disappears within 24 hours," etc.). Each item was measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree"), and the average of the three items was used to measure the effect of the ephemerality heuristic on SNS users' disclosure and privacy management behaviors. Factor analysis based on data from those who indicated they use at least one of the three SNSs that offer ephemeral features (Facebook, Instagram, and

Snapchat) and did not select "None at all" in response to "How much information do you share on Stories on the following social media platform(s): [Facebook/Instagram/Snapchat]?" showed the scale to be unidimensional and to have high reliability (Cronbach's $\alpha = .93$).

Data analysis for understanding the role of the ephemerality heuristic was limited to the sample described above ($n = 59$) because people who only use Twitter, which does not yet have ephemeral features, or who do not use ephemeral features even when they are available to them on an SNS platform are likely not affected by the ephemerality heuristic, which is a term born out of the introduction of ephemeral features (e.g., Stories) on messaging applications and SNSs. One notable characteristic about this subset of the sample is that close to 90% of these participants use all four of SNSs listed in this survey (Facebook, Instagram, Snapchat, and Twitter). On the other hand, the proportion of all Study 2A participants who used all four of these SNSs was only 20.2%. This difference in this characteristic shows that findings about ephemerality heuristic in Study 2A would mostly reflect the experience of SNS users who keep active accounts on many SNSs, and that the effect that comes from having varying numbers of SNS accounts should be controlled for in future studies that investigate the effect of ephemerality heuristic.

Chapter 7: Results from Study 2A

Data from Study 2A will augment the findings from the focus group interviews that were conducted with participants who represented a very narrow segment of SNS users (i.e., college students who generally hold liberal values and are more than 75% female) to a larger, more representative sample of SNS users. Generalizing the findings from the focus group interviews is an important intermediate step to identifying predictors of specific heuristic effects (i.e., it helps understand SNS users' susceptibility to the effect of different cognitive heuristics) on users' decisions about disclosure and privacy to address the hypotheses and research questions developed in Chapter 5.

For each cognitive heuristic in this study, descriptive analyses of individual items in the scales will provide insight into participants' opinions about or agreement with how different cognitive heuristics are related to their risk perceptions and decisions about disclosure and privacy. In addition, descriptive analyses about aggregate measures of each cognitive heuristic (i.e., the means of all items in each of the scales described in Chapter 6) will gauge participants' overall agreement or disagreement with statements that reflect the effect of the cognitive heuristics on their risk perceptions and privacy and disclosure behaviors. As all items were measured on 7-point Likert scales, one-sample t-tests will test whether the participants' agreement or disagreement with the effect of cognitive heuristics is significantly different from the midpoint of 4 ("Neither agree nor disagree"). If the measure is significantly above the midpoint of 4, this value would indicate that people agree with the effect of a particular cognitive heuristic on SNS users' self-reported privacy-related perceptions and behaviors, and any value significantly below 4 would suggest the opposite.

Affect Heuristic

Descriptive analyses of the individual items in the scale that measures the effect of affect heuristic show agreement with the effect of the affect heuristic on SNS users' perceived comfort about disclosure, perceived risk about disclosure, and their amount of disclosure on SNSs, and thus provide support for H1a and H1b (see Table 4). The mean of all items that measure agreement with the effect of affect heuristic (M = 4.75, SD = 1.26) was significantly greater than the midpoint of 4 (t[408] = 12.09, p < .001). This result reflects participants' belief that positive affect about SNSs can lead them to perceive less risk about disclosure on SNSs and share more information on SNSs and that negative affect can have the opposite effect on their risk perception and disclosure decisions.

Table 4

Descriptive Summary of the Items that Measure the Effects of the Affect Heuristic

	Item	*N*	*M*	*SD*	Min	Max
Perceived Comfort	The more I dislike a particular social media platform (e.g., its features), the less comfortable I feel about sharing my information on that platform.	410	5.09	1.64	1.00	7.00
	How good or bad I feel about a particular social media company affects how comfortable I feel about sharing information on its platform.	410	4.93	1.59	1.00	7.00
Perceived Risk	The more I like a particular social media platform (e.g., its features), the less risk I feel when sharing my information on that platform.	411	4.30	1.78	1.00	7.00
	How good or bad I feel about a particular social media company affects how much risk I feel when sharing information about myself on its platform.	411	4.83	1.60	1.00	7.00
Disclosure	The more I like a particular social media platform (e.g., its features), the more information I share on that platform.	411	4.52	1.68	1.00	7.00
	How good or bad I feel about a particular social media company affects how much information I tend to share on its platform.	411	4.89	1.58	1.00	7.00

Availability Heuristic

As the availability heuristic can be triggered by both people's memory or salience of their own or others' negative privacy experience on SNSs, two measures were created to assess the participants' agreement with both kinds of prior negative experience. Descriptive analyses of the individual items used to measure the effect of the availability heuristic show that the availability heuristic is both a disclosure heuristic and privacy heuristic that affects the amount of disclosure as well as the restrictiveness of users' privacy settings on SNSs. These analyses show that the availability heuristic might have greater influence on the restrictiveness of users' privacy settings than on their amount of disclosure, as the means of participants' agreement with the statements about the heuristic's effect on privacy settings are both above 5, while the means of agreement with statements about the heuristic's effect on the amount of disclosure is above the midpoint of 4 only when the heuristic is triggered by their own personal negative privacy experience on SNSs (M = 4.71, SD = 1.83), but not when it is triggered by hearing about others' negative privacy experience on SNSs (M = 3.65, SD = 2.02) (see Table 5). Overall, the results from these analyses show support for H2a-c, which predicted the effect of availability heuristic on SNS users' perceived risk about disclosure, amount of disclosure, and restrictiveness of their privacy settings on SNSs.

When the individual items were aggregated into two scales, the mean value of the measure that assessed people's agreement with the effect of availability heuristic that stems from their own negative privacy experience (M = 5.41, SD = 1.19) was significantly above the midpoint of 4 (t[78] = 12.46, p < .001). The mean of participants' agreement with the effect of availability heuristic triggered by others' negative privacy experience (M = 4.61, SD = 1.69) was also significantly above the midpoint of 4 (t[243] = 5.69, p < .001). A comparison of these two group means shows a difference of 0.9, which suggests that

availability heuristic is more influential on people's decision-making processes when it is triggered by one's own negative privacy experience rather than hearing about others' negative privacy experience on SNSs.

Table 5

Descriptive Summary of the Items that Measure the Effects of the Availability Heuristic

Item			*N*	*M*	*SD*	Min	Max
As a result of this experience about [self/other], to what extent did you…							
Perceived Comfort	Self	… feel less comfortable sharing information about yourself on social media?	79	5.29	1.63	1.00	7.00
	Other	… feel less comfortable sharing information about yourself on social media?	247	4.78	1.85	1.00	7.00
Disclosure	Self	… reduce the amount of information you share on social media?	79	4.71	1.83	1.00	7.00
	Other	… reduce the amount of information you share on social media?	245	3.65	2.02	1.00	7.00
Privacy Settings	Self	… change your account settings in ways to better protect your privacy?	79	5.87	1.39	1.00	7.00
	Other	… change your account settings in ways to better protect your privacy?	247	5.01	2.04	1.00	7.00

Optimistic Bias

Consistent with the focus group data from Study 1, the descriptive analyses of individual items reflect participants' disagreement with the effect of optimistic bias on perceived comfort about disclosure, amount of disclosure, and the restrictiveness of privacy settings on SNSs (see Table 6). The mean of three items that measure participants' agreement with the effect of optimistic bias ($M = 3.07$, $SD = 1.50$) was significantly lower than the midpoint of 4 ($t[410] = -12.59$, $p < .001$). Again, these values show no support for the effect

of optimistic bias on people's decisions about disclosure or privacy in the predicted direction and provide answers for RQ1 and RQ2. See Table 6.

Table 6

Descriptive Summary of the Items that Measure the Effects of Optimistic Bias

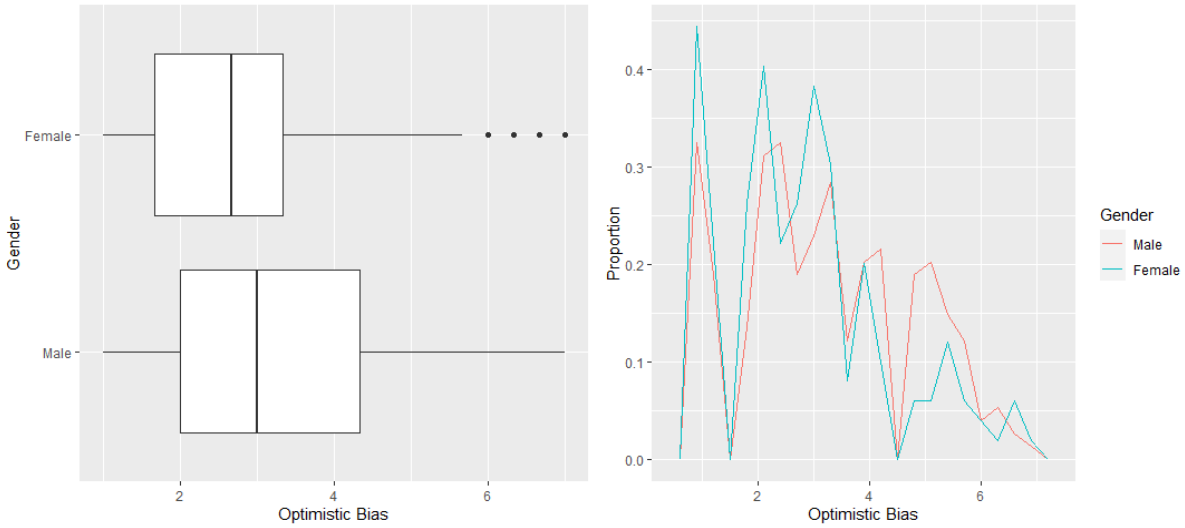
Item	*N*	*M*	*SD*	Min	Max
Because I feel I am less likely to have a negative privacy experience on social media than most people, I **feel comfortable** sharing my information there.	411	3.33	1.75	1.00	7.00
I **share more** of my information on social media because I feel less likely to have a negative privacy experience than others.	411	2.72	1.73	1.00	7.00
I do not **select restrictive privacy settings** on social media because I feel like other people are more likely to have a negative privacy experience than I am.	411	3.15	1.73	1.00	7.00

While the participants in the sample did not agree with the statements that explain the effect of optimistic bias overall, a possible difference in the effect of optimistic bias depending on gender was also tested. The impetus for this analysis came from the considerable number of participants (both male and female) in Study 1 who discussed how they believe there is more risk associated with disclosure for women than men. This perception may influence people's optimistic bias differently depending on their gender. The mean of men's agreement with optimistic bias (M = 3.23, SD = 1.51) was significantly (t[361.92] = 5.69, $p < 0.01$) greater than that of women's (M = 2.82, SD = 1.45), which is consistent with the focus group results. See Figure 1 for group comparison. While it is true that men are more likely to be optimistically biased about privacy risks on SNSs than are women, these results do not suggest that men in general agree with the effect of optimistic bias on their decisions about disclosure or privacy, as the means of each gender group are

still both below the midpoint of 4. As the method used in this study show the mean of participants' agreement with the statements about optimistic bias, the current finding also does not mean that all SNS users do not agree with the effect of optimistic. Future research could segment their sample using additional demographic and/or control variables to identify whether there is a specific group of SNS users that does agree with the effect of optimistic bias on their decisions.

Figure 1

Agreement with Optimistic Bias by Gender



Note. Lower numbers suggest that the participants are less optimistically biased, and higher numbers suggest the opposite, which means they believe they are less likely to have a negative privacy experience on SNSs compared to others.

Bubble Heuristic

Descriptive analyses of the individual items in the scale that measures the effect of the bubble heuristic show participants' agreement that the bubble heuristic affects their perceived comfort and risk about disclosure, and also the amount that participants disclose on SNSs, and thus they provide support for H3a and H3b (see Table 7). The aggregated mean of

all items that measure the participants' agreement with the effect of the bubble heuristic (M = 5.51, SD = 1.34) was significantly greater than the midpoint of 4 (t[407] = 26.95, p < .001). See Table 7.

Table 7

Descriptive Summary of the Items that Measure the Effects of the Bubble Heuristic

Item	*N*	*M*	*SD*	Min	Max
Having privacy settings available makes me **feel more comfortable** about sharing information on social media.	410	5.60	1.26	1.00	7.00
Using the privacy settings on social media to restrict who can see my profile or posts makes sharing information **feel less risky**.	409	5.45	1.35	1.00	7.00
The privacy settings a platform offers users is a big factor in **how much information I share** on social media.	410	5.47	1.35	1.00	7.00

Homophily Heuristic

Descriptive analyses of the items in the scale that comprise the homophily heuristic measure support H4a and H4b because they reveal participants' agreement with the heuristic's effect on participants' perceived comfort and risk about disclosure, and their amount of disclosure on SNSs. The aggregated mean of all items on the measure of participants' agreement with the effects of homophily heuristic (M = 4.68, SD = 1.13) was significantly greater than the midpoint of 4 (t[409] = 10.24, p < .001). See Table 8.

Table 8

Descriptive Summary of the Items that Measure the Effects of the Homophily Heuristic

Item	*N*	*M*	*SD*	Min	Max
When I feel more similar to my friends and followers on social media, I **feel more comfortable** posting information.	410	4.86	1.59	1.00	7.00

Item	*N*	*M*	*SD*	Min	Max
The more similar my friends and followers on social media are to me, the **less risk I feel** about posting things on those platforms.	409	4.67	1.66	1.00	7.00
I **share more posts** with my friends and followers on social media who are more similar to me (in age, political opinions, background, etc.).	411	4.83	1.52	1.00	7.00

Bandwagon Heuristic

Descriptive analyses of individual items in the subscale about the effect of bandwagon heuristic on specific feature selection show participants' agreement with statements about the effect of bandwagon heuristic on their perceived comfort (*M* = 4.32, *SD* = 1.72), perceived safety (*M* = 4.17, *SD* = 1.64), and their decisions about their use of specific social media features (e.g., Stories, stickers, GIFs, etc.) (*M* = 4.66, *SD* = 1.49) (see Table 9). In terms of SNS users' decisions about disclosure through their use of specific social media features, these results support H5a and H5b.

Table 9

Descriptive Summary of the Items that Measure the Effects of the Bandwagon Heuristic on Decision-Making Processes about Feature Selection

Item	*N*	*M*	*SD*	Min	Max
If my friends and followers use specific social media features (e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.), I am **more likely to use them** too.	411	4.32	1.72	1.00	7.00
When my friends and followers use specific social media features (e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.), it **feels safer** for me to use them too.	411	4.17	1.64	1.00	7.00
If I were to hear about my friends using a new social media platform, I would probably **feel more comfortable** about trying that platform myself.	411	4.66	1.49	1.00	7.00

On the other hand, looking at the means of individual items in Table 10 show participants' disagreement with the statements that describe the effect of bandwagon heuristic on their perceived comfort about disclosure (M = 3.38, SD = 1.88), decisions about disclosure (M = 3.93, SD = 1.81), and the restrictiveness of their privacy settings (M = 3.39, SD = 1.89). In addition, a one-sample t-test shows that the mean of the single item that measures participants' agreement with the statement that describes the heuristic effect on their decisions about disclosure in Table 10 is not significantly different from the midpoint of 4 ("Neither agree nor disagree") (t[410] = -0.82, p = 0.41). This result suggests that the mean for this particular item does not indicate outright disagreement with the heuristic effect on their disclosure decisions. None of the results about the effect of bandwagon heuristic on people's decision-making processes about information control, however, support H5b and H5c, but they do suggest that testing of H5a requires additional analyses.

Table 10

Descriptive Summary of the Items that Measure the Effects of the Bandwagon Heuristic on Decision-Making Processes about Information Control

Item	*N*	*M*	*SD*	Min	Max
When I see my friends or followers post about something personal or sensitive on social media, I **feel more comfortable** about posting something similar myself.	411	3.38	1.88	1.00	7.00
If I see my friends or followers post about something on social media (e.g., holiday photos, etc.), I am more likely to **post something** similar myself.	411	3.93	1.81	1.00	7.00
If my friends **change their privacy settings** to be more or less private, I am more likely to do it too.	411	3.39	1.89	1.00	7.00

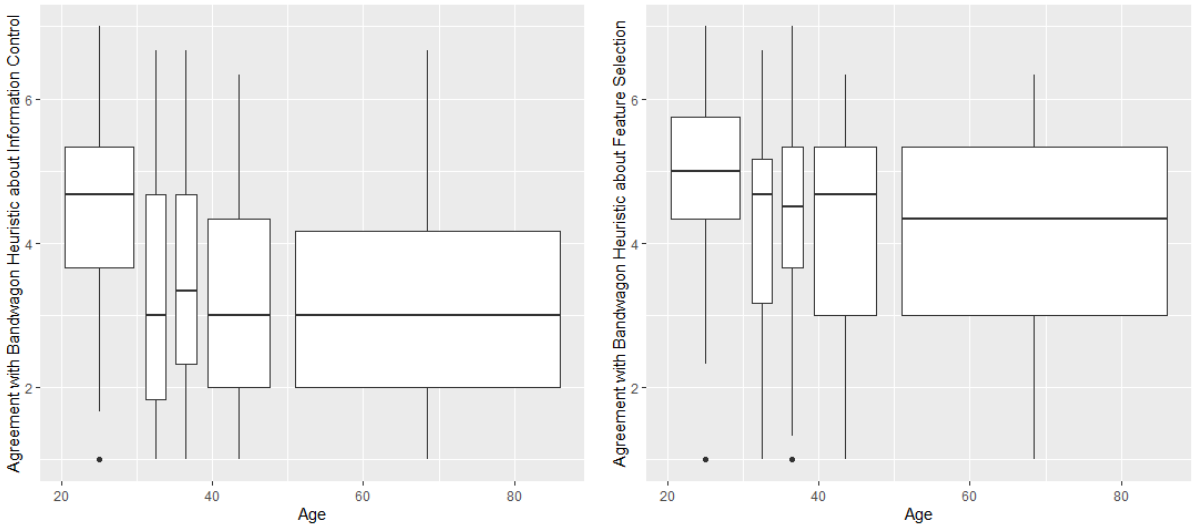
Consistent with the results from the descriptive analyses of individual items, the mean of participants' agreement with the statements in the subscale about the effect of the bandwagon heuristic on people's control over information access (M = 3.56, SD = 1.62) was significantly lower than the midpoint of 4 (t[410)] = -5.44, p < .001). On the other hand, the mean of participants' agreement with the statements in the subscale about the effect of the bandwagon heuristic on people's selection of specific features (M = 4.38, SD = 1.40) was significantly greater than the midpoint of 4 (t[410] = 5.55, p < .001). These findings suggest that the bandwagon heuristic functions to influence participants' judgments and decisions when they see others' use of specific features (e.g., Stories, stickers, hashtags, etc.), but not when they are deciding to share specific content or control others' access to such content. This result is somewhat inconsistent with the findings from Study 1 that provided numerous anecdotes about the effect of the bandwagon heuristic on SNS users' decisions about their disclosure, ranging from posting specific content that other users are posting (e.g., holiday photos, etc.) to using specific features that others are using on SNSs (e.g., GIFs, hashtags, poll features, recommendation features, etc.).

In addition, to understand how Study 1 resulted in anecdotes that describe the effect of bandwagon heuristics, while the results from the current study show the effect of bandwagon heuristic under certain conditions (e.g., when selecting specific SNS features), the role of age was assessed to see if the anecdotes from Study 1 are unique to the sample of young adults used in that study. When correlations between the measures of bandwagon heuristic and participants' age were computed, both kinds of bandwagon heuristic, as measured by the two subscales described above, had significant inverse relationships with participants' age (r = -.24, p < .001 for bandwagon heuristic about information control and age; r = -.23, p < .001 for bandwagon heuristic about feature selection) (see also Figure 2).

These inverse relationships show that younger SNS users are more likely to agree with the effect of bandwagon heuristic than are older users, perhaps because they are more susceptible to peer pressure. This result suggests that the effect of the bandwagon heuristic likely varies as a function of age, so age should be controlled, or examined more closely, in further examinations of the effects of the bandwagon heuristic on SNS users' privacy-related perceptions and behaviors.

Figure 2

Agreement with Bandwagon Heuristic by Age Groups



Inequity Aversion

The means of the individual items that measured participants' agreement with the effect of inequity aversion on their perceived risk (M = 3.21, SD = 1.82) and amount of disclosure (M = 3.44, SD = 1.94) provide answers for RQ3 and RQ4, as they show that participants disagreed that inequity aversion motivates their SNS use (see Table 11). The mean of all items that measure participants' agreement with the effects of inequity aversion (M = 3.36, SD = 1.70) on disclosure and privacy risk perception was significantly lower than

the midpoint of 4 (t[409] = -7.87, p < .001). This result is consistent with the findings from Study 1 that indicated inequity aversion may not influence SNS users' decision-making processes about disclosure or privacy in the hypothesized direction.

Table 11

Descriptive Summary of the Items that Measure the Effects of Inequity Aversion

Item	*N*	*M*	*SD*	Min	Max
Seeing others benefit (e.g., getting more likes, more attention, etc.) more than I do from posting information on social media makes me **feel less concerned about the privacy risks** of using social media.	411	3.21	1.82	1.00	7.00
I feel motivated to **post on social media** when I see others getting more benefits than me (e.g., getting more likes, more attention, invitations, etc.).	411	3.44	1.94	1.00	7.00

As discussed in Chapter 4, the findings from Study 1 show that the behavioral implications of inequity aversion and bandwagon heuristic are very similar and that it might be difficult to distinguish between the two in the context of SNSs. Inequity aversion, if it affects SNS users, would lead them to engage more on SNSs to receive the same benefits that they see others benefitting from. This process is very similar to the bandwagon heuristic's propensity to make people feel more comfortable about sharing information in a similar way as others. Therefore, the relationship between people's agreement with the effects of inequity aversion and the bandwagon heuristic was explored. As participants' age affects their agreement with the two types of bandwagon heuristic investigated in this study, partial correlations between participants' agreement with both types of bandwagon heuristic and inequity aversion were computed while controlling for age. As expected, participants' agreement with both types of the bandwagon heuristic and with inequity aversion were highly correlated. The partial correlations between participants' agreement with the inequity

aversion scale items and (a) the effect of the bandwagon heuristic on information control strategies ($r = 0.79$, $p < .001$) and (b) the effect of the bandwagon heuristic on selection of specific features on SNSs ($r = 0.63$, $p < .001$) were positive and highly significant. This result could suggest that users' sense of inequity aversion might manifest through the bandwagon heuristic in the context of SNSs.

Hyperbolic Discounting

Descriptive analyses of the individual items used to measure participants' agreement with the effect hyperbolic discounting on their privacy risk perception ($M = 3.73$, $SD = 1.77$) and amount of disclosure ($M = 3.54$, $SD = 1.99$) revealed that participants did not agree that hyperbolic discounting affected their SNS use (see Table 12). The aggregated mean of all the items comprising the hyperbolic discounting scale measure ($M = 3.09$, $SD = 1.36$) was significantly lower than the midpoint of 4 ($t[409] = -13.46$, $p < .001$). These results about hyperbolic discounting do not support H6a and H6b.

Table 12

Descriptive Summary of the Items that Measure the Effects of Hyperbolic Discounting

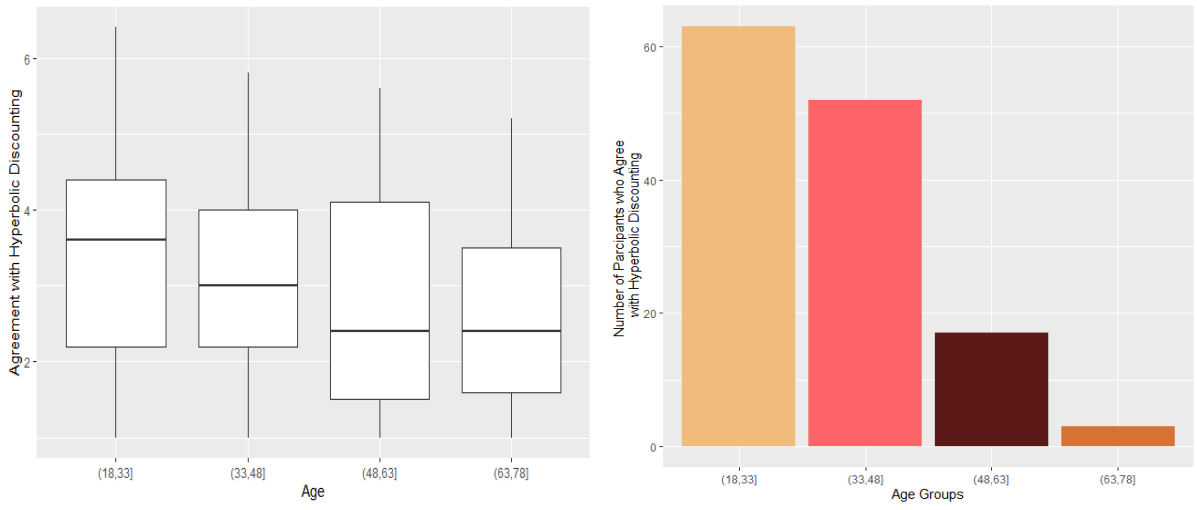
Item	*N*	*M*	*SD*	Min	Max
I **posted something** on social media "in the heat of the moment," which I later regretted.	411	3.54	1.99	1.00	7.00
When debating whether to post some information, I sometimes feel the immediate benefits of posting **outweigh the risks** I might experience later.	410	3.73	1.77	1.00	7.00

However, as Study 1 provided many accounts from the college-age participants about the effect of hyperbolic discounting leading to disclosures that they later regretted, the influence of age on the survey participants' agreement with the internal logic behind hyperbolic discounting was examined. There was a significant negative correlation ($r = -$

0.21, $p < .001$) between participants' agreement that hyperbolic discounting affects their SNS use and their age. Figure 3 shows that younger SNS users' level of agreement with the effect of hyperbolic discounting on disclosure is higher than that of older SNS users. It also shows that almost half (46.7%, $n = 63$) of the participants who agree that hyperbolic discounting affects their SNS behavior are below the age of 33, and a large majority (85.2%, $n = 115$) of the same group is under the age of 48. This result suggests that hyperbolic discounting may be more relevant to younger SNS users, such as those who participated in Study 1, and provides conditional support for H6a and H6b. Also, this finding is consistent with previous reports from the Pew Research Center (Madden, 2012), which found that young adults between 18-29 years old are more likely to regret the content they posted than are older adults. This result suggests that age should be controlled when studying the effect of hyperbolic discounting and that H6a should be further investigated to see whether the relationship predicted in H6a can be supported under certain conditions.

Figure 3

Agreement with Hyperbolic Discounting by Age Groups



Ephemerality Heuristic

Descriptive analyses of the individual items used to assess participants' agreement with the effect of ephemerality heuristic on risk/comfort perceptions and disclosure in SNSs demonstrate their agreement that this heuristic affects their perceived comfort (M = 4.80, SD = 1.77) and amount of disclosure (M = 4.56, SD = 1.74) on SNS, and thus provide support for H7a and H7b (see Table 13). The aggregated mean of all items for the ephemerality heuristic scale (M = 4.73, SD = 1.66) was significantly higher than the midpoint of 4 (t[58] = 3.37, p = .001). This result is consistent with findings from Study 1 that provided many anecdotes about the effect of the ephemerality heuristic on SNSs users' privacy-related perceptions and behavior.

Table 13

Descriptive Summary of Items that Measure the Effects of the Ephemerality Heuristic

Item	*N*	*M*	*SD*	Min	Max
I am **more comfortable** posting on social media platforms where content disappears within 24 hours.	59	4.80	1.77	1.00	7.00
I am inclined to **post more information** on social media platforms where the content disappears after a short period of time (e.g., 24 hours).	59	4.56	1.74	1.00	7.00

Summary

The results about the effect of cognitive heuristics on SNS users' risk perceptions and decisions about disclosure and privacy from using the direct approach of measuring heuristic effects show that five heuristics influence SNS users as predicted in the hypotheses proposed in Chapter 5. In terms of SNS users' amount of disclosure, participants agreed that the affect heuristic, bubble heuristic, homophily heuristic, and ephemerality heuristic lead them to share more information, while availability heuristic leads them to share less information. In terms of risk perception, participants agreed that the affect heuristic, bubble heuristic, and

homophily heuristic lead them to feel less risk about disclosure, and that affect heuristic, bubble heuristic, homophily heuristic, and ephemerality heuristic lead them to feel more comfortable about disclosure. They also agreed that availability heuristic—especially when it is triggered by their own negative privacy experience in the past—makes them feel less comfortable about disclosure on SNSs.

In addition, participants showed significant agreement with the aggregate measures of these five heuristics. Together, the results show that the affect heuristic, availability heuristic, bubble heuristic, homophily heuristic, and ephemerality heuristic are disclosure heuristics that influence SNS users' decisions about disclosure, while impacting their risk perceptions in a way that is consistent with their decisions to either disclose more or less information. Moreover, participants also agreed that the availability heuristic, in particular, leads them to have more restrictive privacy settings, and shows that availability heuristic can also be a privacy heuristic. Table 14 provides a summary of results for all of the heuristics.

Table 14

Participants' Agreement with the Heuristic Effects in Descending Order

Heuristic	*Effect*	*M*	*Diff*	*t*
Bubble Heuristic	Disclosure	5.51	1.51	26.95***
Availability Heuristic (personal experience)	Disclosure & Privacy	5.41	1.41	10.46***
Affect Heuristic	Disclosure	4.75	0.75	12.09***
Ephemerality Heuristic	Disclosure	4.73	0.73	3.37**
Homophily Heuristic	Disclosure	4.68	0.68	10.24***
Availability Heuristic (others' experience)	Disclosure & Privacy	4.61	0.61	5.69***
Bandwagon Heuristic (feature selection)	Disclosure & Privacy	4.38	0.38	5.55***
Bandwagon Heuristic (information access)	Both disclosure & privacy *for younger users*	3.56	-0.44	-5.44***

Heuristic	*Effect*	*M*	*Diff*	*t*
Inequity Aversion	Neither	3.36	-0.64	-7.87***
Hyperbolic Discounting	Disclosure *for younger users*	3.09	-0.91	-13.46***
Optimistic Bias	Neither	3.07	-0.93	-12.59***

Note. "Diff" = difference between the mean of each measure and the midpoint of 4.

***$p < .001$. **$p < .01$.

Findings about the bandwagon heuristic and hyperbolic discounting show that hypotheses about these heuristics may need further investigation to see if the predicted relationships can be supported. First, participants agreed that the bandwagon heuristic leads them to share more information by using specific features they see others use, but does not lead them to share specific types of information that others post; as the mean of participants' agreement with the effect of bandwagon heuristic on sharing specific types of information is significantly lower than the midpoint of 4, it is possible that seeing others post specific types of features actually leads people share less of that information. This result is somewhat inconsistent with findings from Study 1, so further investigation is warranted. Consistent with the results about the effect of the bandwagon heuristic on disclosure decisions, participants agreed that seeing others use specific social media features makes them feel safer to use them in their posts, but they disagreed that seeing other people post specific types of information makes them feel more comfortable to do the same. Moreover, despite the anecdotes about the effect of bandwagon heuristic on SNS users' decisions about privacy settings from Study 1, participants in Study 2A did not think they become more likely to adjust their privacy settings as a result of bandwagon heuristic. In order to reconcile these contradictory findings, the hypotheses about the bandwagon heuristic also need further investigation.

While some participants in Study 1 provided specific anecdotes about the effect of hyperbolic discounting on their risk perceptions about disclosure and impulsive disclosure decisions, many participants in Study 2A did not agree that hyperbolic discounting leads them to share more information. Though younger participants were more likely to agree with the effect of bandwagon heuristic on their decisions about disclosure, which suggests that age should be controlled in future research on hyperbolic discounting. In terms of risk perception, participants did not agree that hyperbolic discounting affects them to believe that the benefit of immediate gratification from disclosure outweighs their perception of underlying or distant privacy risks. However, as hyperbolic discounting affects quick and in-the-moment decisions, participants may have expressed disagreement with the statements that describe the effect of hyperbolic discounting because they could carefully process the statements when they were taking the survey. Moreover, these participants were likely not influenced by intense emotions, which seem to accompany the effect of hyperbolic discounting. Therefore, hyperbolic discounting is perhaps best studied using a different methodological approach.

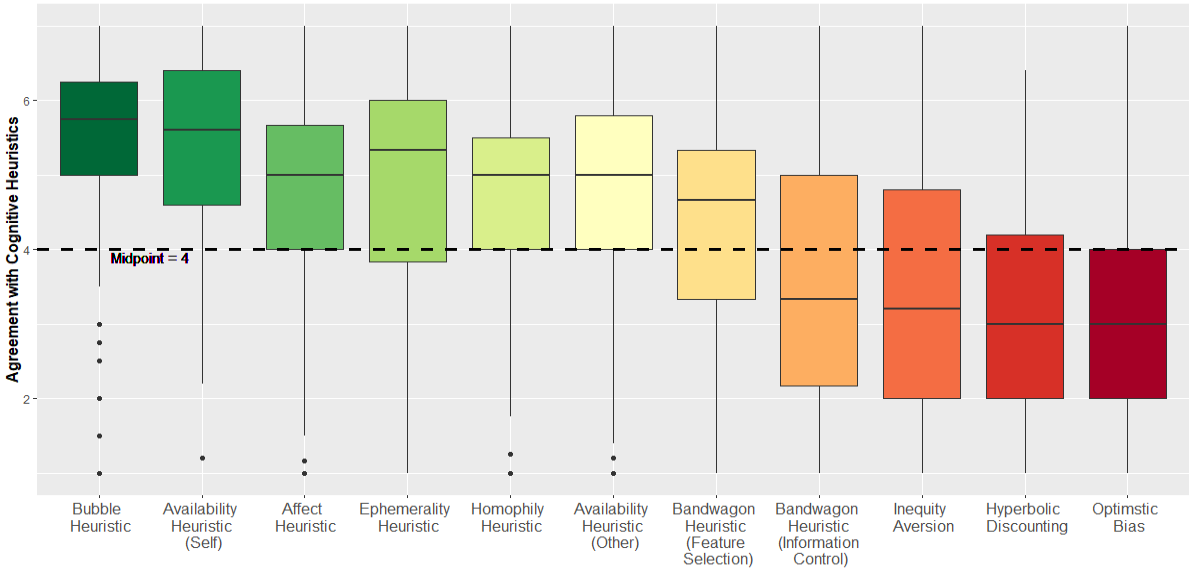
Lastly, consistent with the results from Study 1, the results from the present study also show the optimistic bias and inequity aversion are likely not related to the amount information users share on SNSs or the restrictiveness of their privacy settings on SNSs. Participants disagreed that optimistic bias and inequity aversion lead them share more information on SNSs and that optimistic bias leads them to select less restrictive privacy settings.

In addition to addressing the proposed hypotheses and research questions, the distance between the mean of each aggregate measure of participants' agreement with the heuristic's effects on their perceptions and behaviors on SNSs and the scale midpoint of 4 seems to be a simple and direct, but not definitive, measure of heuristic effects on SNSs. As

presented in Table 14 and Figure 4, these analyses can provide additional insights on the heuristics' effects by offering a way to think about the comparative effect of the different heuristics examined in this study. These additional analyses help answer the question of not only *whether* cognitive heuristics influence SNS users' perceptions and behaviors, but also *to what extent* they influence these dependent variables in either positive or negative direction and how the size of each heuristic effect compares to one another.

Figure 4

Participants' Agreement with the Effects of Each Cognitive Heuristic in Descending Order



This type of comparative analysis could help illuminate which cognitive heuristics might play a bigger role in SNS users' privacy and disclosure decision-making processes. Figure 4 shows that the bubble heuristic, availability heuristic, affect heuristic, ephemerality heuristic, and homophily heuristic (in descending order) likely have stronger positive influence on SNS users' risk perception and behaviors compared to the other cognitive heuristics examined. These results suggest that when people are exposed to multiple triggers of cognitive heuristics, they might be more strongly influenced by one heuristic over another

(e.g., the availability heuristic might play a greater role in preventing users from disclosing information even when they feel very positive about using a particular SNS, and thus are susceptible to the affect heuristic). It would be valuable to continue exploring the interactive and comparative effects of cognitive heuristics. The comparative strength of heuristic effects should be further analyzed using different measurement approaches to see how the self-reported measure of heuristic effects in the current study compares to other datasets measuring heuristic effects using other methodological approaches.

Chapter 8: Method for Study 2B

In contrast to Study 2A that used a direct approach to measuring heuristic effects, Study 2B tests the hypotheses and research questions advanced in Chapter 5 using an indirect approach to measure the effects of the heuristics. This approach may be better to capture heuristic processes that are deeply subconscious, and thus cannot be easily self-reported by participants even if they take the time to think about their experiences and decision-making processes (see Nisbett & Wilson, 1977). In this study, the dependent variables (e.g., disclosure, risk perceptions, and privacy management strategies through the use of available SNS account settings) and possible predisposition to cognitive heuristics (i.e., factors that measure participants' susceptibility to the effect of specific heuristics based on findings from Study 1) will be measured separately in order to examine their correlational relationships. More details on these measures will be provided in this chapter.

Sample

444 participants who live in the U.S. were recruited through Amazon's Mechanical Turk (MTurk). The final sample after data cleaning included 415 U.S. adults (233 male and 181 female) between the ages of 18 and 78 years (M = 39.04, SD = 11.40). In terms of race/ethnicity, participants consisted of White/Caucasian (72.0%, n = 299); Asian (14.2%, n = 59); Black or African American (11.8%, n = 49); Hispanic (7.9%, n = 33), Latino (1.2%, n = 5), or Spanish (0.5%, n = 2); American Indian or Alaska Native (1.2%, n = 5); Native Hawaiian or Pacific Islander (0.2%, n = 1); multiracial (0.2%, n = 1); and "other" (non-specified) races (0.2%, n = 1). Most (88.7%, n = 368) of the respondents had attended at least some college, and 60.7% (n = 252) had earned a bachelor's degree or higher.

More than half (57.3%, n = 238) reported that they have a religion, and of those people, 37.4% (n = 89) was Christian and 41.6% (n = 99) was Roman Catholic. Almost half

(48.2%, *n* = 98) of the sample identified as Democrat, 29.4% (*n* = 121) as Independent, and 21.7% (*n* = 89) as Republican, and the rest (0.5%, *n* = 2) as other. Most (90.5%, *n* = 372) identified as heterosexual.

Most participants (91.1%, *n* = 378) used Facebook, 68.7% (*n* = 285) used Instagram, 25.5% (*n* = 106) used Snapchat, and 73.25% (*n* = 304) used Twitter. More than half (55.4%, *n* = 230) of the participants reported that they use at least three of the four SNSs, including Facebook, Instagram, Snapchat, and Twitter.

Procedure

Participants completed an online survey on Qualtrics. On average, participants took about 8 minutes (median) to complete the survey. Responses from participants that had duplicate IP addresses (*n* = 3), people who may have lost their attention to the survey after 40 minutes (*n* = 7), "speedsters" defined as people who completed the survey in less than 200 seconds (~ 3.5 minutes) (*n* = 11), and those who did not select the correct answer to an attention check question (*n* = 6) were removed from the dataset. IRB approval was obtained prior to data collection.

Measures

Dependent Variables

The dependent variables in this study center on SNS users' disclosure, privacy management strategies (e.g., public-private account settings), and risk perceptions. At the outset of the survey, participants were asked to indicate which of the four SNSs (Facebook, Instagram, Snapchat, Twitter) they used. As situation-specific factors (e.g., situation-specific risk assessment depending on the platform used) may override dispositional factors (e.g., general privacy concern about SNSs) (Kehr et al., 2015; Li, Sarathy, & Xu, 2011; Wilson & Valacich, 2012), most items in the survey were measured for each SNS that participants

reported using. Indeed, prior research about situation-specific privacy calculus (Kehr et al., 2015) highlights how people's perceived privacy risk and behaviors on one platform may be different from their perceptions and behaviors on another platform. Therefore, with only one exception noted below, all items that measured the dependent variables were repeated for each SNS platform that a participant reported to use.

The dependent variables were measured separately for each SNS to reflect important differences across how people use different SNSs. As revealed in data from Study 1, individual SNS users have different attitudes about specific SNSs because (1) users have different audiences on different SNSs, (2) different SNSs offer different features, and (3) norms in user behaviors vary across SNSs. For example, many participants noted that they are more careful about sharing posts on Facebook because they usually have the largest audience on that platform, as they are connected with not only close friends in their age group, but also parents, distant family members, colleagues, and even former teachers. Also, while most SNSs offer features that are permanently visible to network connections (e.g., friends and followers), Snapchat was introduced as an SNS app that primarily offers ephemeral features that allow users to share information that disappears in 24 hours. Therefore, many participants recognized the differences in the types of content they post on Snapchat compared to other SNSs. Moreover, many participants recognized that users behave differently on different SNSs to follow the norms that are already in place; for example, many participants from Study 1 reported that they felt the pressure to share only polished content on Instagram because its user interface highlights photos and videos over text-based content. These participants explained that they even think about how multiple posts over time fit together on their profile to have a similar aesthetic feel, and thus make their overall profile more coherent and visually appealing. Because of these differences

across SNSs, it is possible that different cognitive heuristics become more salient on these SNSs, and the results in the following chapter can be used to assess how different cognitive heuristics operate on each SNS.

Disclosure. The amount of information that participants disclose on the SNS(s) they reported to use was measured with the following question stem: "How much information do you post on the following social media platform: [Facebook/Instagram/Snapchat/Twitter]?" Each of the items was measured on a scale of 1 ("None") to 7 ("a great deal"), and they were asked separately for each platform.

Sensitive Disclosure. Two additional items were created based on findings from Study 1 that showed how some cognitive heuristics influence people to share not only greater *amounts* of information in general, but also more *sensitive* information. These two questions were asked to measure the amount of specific types of information they disclose on SNSs. Participants were first asked to indicate the extent to which they share information on 10 different topics that varied in topic sensitivity on every SNS they reported to use. The topics ranged across a wide range of information (e.g., news and daily activities, romantic relationships, opinions, feelings, etc.). Each of these 10 items were measured on a scale of 1 ("None") to 7 ("A great deal"). Then, participants were asked to rate these topics in terms of their sensitivity when discussing these topics on SNSs in general. Each of these 10 items were measured on a scale of 1 ("Not sensitive at all") to 7 ("Extremely sensitive").

Levene's test revealed that the variances in the perceived sensitivity of 10 topics were significantly different from one another ($F[2, 4132] = 13.77$, $p < .001$), so it was assumed that population variances were different across groups. A one-way ANOVA applying Welch's F shows that different topics have significant differences on perceived sensitivity, $F(9, 1682.8) = 132.87$, $p < .001$. Bonferroni tests revealed that most means of perceived

sensitivity of different topics were significantly different from one another. The mean perceived sensitivity of contact information was significantly different from all other means of perceived sensitivity. The mean perceived sensitivity of deep feelings and emotions and the mean perceived sensitivity of romantic relationships was significantly different from eight out of nine other means. The mean perceived sensitivity of photos of themselves and the mean perceived sensitivity of negative things that happened to them was significantly different from six out nine other means. See Table 15 for means of perceived sensitivity for each topic in descending order.

Table 15

List of Topics Discussed on SNSs and Their Perceived Sensitivity by Users

Topic	*M*	*SD*
Contact information (e.g., cell phone number, mailing address, etc.)	6.09	1.48
Deep feelings and emotions	5.45	1.5
Romantic Relationships	5.16	1.68
Photos of you	4.75	1.84
Negative things that happened to you	4.7	1.72
Political opinions and preferences	4.45	1.75
Controversial social issues or news topics	4.45	1.76
Positive things that happened to you	3.72	1.8
Photos of things you like (e.g., hobbies, interests, etc.)	3.47	1.91
News (e.g., local, national, international, etc.)	2.98	1.78

Perceived Risk. Three items were asked to assess participants' perceived risk about disclosure on each of the four SNSs (Facebook, Instagram, Snapchat, and Twitter). These

items were created based on the data obtained in Study 1, which showed that focus group participants often used "comfortable," "safe," and "risky" interchangeably when discussing their risk perceptions regarding SNS use. Thus, these three items were asked for each SNS platform participants reported to use. The three items were measured on 7-point scales, ranging from 1 ("Not risky at all") to 7 ("Very risky"); 1 ("Very uncomfortable") to 7 ("Very comfortable"); 1 ("Not safe at all") to 7 ("Very safe"). Two items were reverse-coded so that a higher value on the combined scale refers to higher perceived risk, as opposed to higher perceived comfort and safety. Factor analysis revealed that the two items that measure participants' perceived comfort and safety about disclosure were highly correlated with each other, but they did not hold well with the item that measured their perceived risk about disclosure. Therefore, participants' perceived risk about disclosure was measured with one item that directly asked participants to indicate their perceived risk of disclosure. The two other items were averaged to measure participants' perceived comfort and safety about disclosure and were analyzed separately from participants' perceived risk of disclosure.

Privacy Management Strategies. SNS users can employ multiple strategies to manage their privacy by adjusting the restrictiveness of different privacy settings. Cho and Filippova's (2016) scale that was developed to measure people's networked privacy management strategies on Facebook was adapted for this study to reflect more recent privacy settings across multiple SNS platforms (Facebook, Instagram, Snapchat, and Twitter). The new scale items contained statements to indicate the kind of privacy management strategies participants may use to protect their privacy on SNSs (e.g., "I have limited people from searching my profile on social media"). Participants were asked to indicate the extent to which they agree with these statements, ranging from 1 = ("Strongly disagree") to 7 = ("Strongly agree"). Three items were reverse-coded so that higher values on the scale

reflected participants' greater use of strategies to make their privacy settings on SNSs more restrictive. An initial EFA suggested that several original items lack convergent or discriminant validity (i.e., low factor loadings [<.40] with their parent factors or high cross loadings [>.40]). Once those problematic items were removed, factor analysis revealed the five remaining items to be unidimensional (Cronbach's α = .83) (see Table 16). The average of these five items was used to measure the restrictiveness of participants' privacy settings.

Table 16

Scale for Privacy Management Strategies

Item	*M*	*SD*
I have restricted who can view my posts on social media.	5.30	1.74
I have customized the privacy setting of individual posts to restrict who can view my posts on social media.	5.21	1.77
I have limited people from searching my profile on social media.	4.79	1.96
I have restricted or blocked accounts on social media.	5.18	1.92
I have restricted who can directly contact or message me on social media.	4.88	1.91

Heuristics

While the measures of cognitive heuristics in Study 2A directly asked about participants' agreement with statements that describe the theorized effects of the cognitive heuristics on SNS users' privacy-related perceptions and behaviors, the present study used an indirect approach to measure the effect of cognitive heuristics. In this study, participants' predisposition to heuristic effects, their risk perceptions, and their behaviors were measured separately to explore their correlational or linear relationships. The validity of measures for participants' predisposition to heuristic effects was assessed in Study 2A, as they were included in the statements that described the effect of different cognitive heuristics on SNS

users' perceived risk and decisions about disclosure and privacy. For example, many participants in Study 2A agreed with the item, "I share more posts with my friends and followers on social media who are more similar to me (in age, political opinions, background, etc.)." In this case, people's perceived similarity to their friends and followers on a particular SNS platform can measure their predisposition to the effect of homophily heuristic, which refers to their susceptibility to being influenced by the homophily heuristic. Therefore, this type of question was used in Study 2B as a measure of participants' predisposition to the effect of the homophily heuristic to see how it is related to their disclosure and privacy behaviors on SNSs. Specific measures of participants' predisposition to the effects of seven cognitive heuristics are detailed below. Because there was not enough support in either Study 1or 2A to continue examining the role of optimistic bias and inequity aversion in people's SNS use, these two heuristics were dropped from the analyses in the present study. All items are listed in Appendix D.

Affect Heuristic. Findings from Study 2A showed that both positive and negative affects were related to participants' perceived risk and their decisions about disclosure on SNSs. For each SNS that participants reported to use, their affect toward that particular SNS platform was thus measured with 8 items on a semantic differential scale that measured the extent to which participants feel either positive or negative affect about the SNS platform. Eight sets of antonyms (e.g., bad <> good, trust <> suspicion, etc.) were included in the scale, and each item was measured on a 7-point scale. The average across the eight items was computed to measure the study participants' affect about the SNS(s) they use. Four items were reverse-coded to ensure that higher scores indicate more positive affect toward a platform. Factor analysis showed that the scale of 8 items was unidimensional, and it had

high reliability across the four SNS platforms: Facebook (Cronbach's α = .92), Instagram (Cronbach's α = .91), Snapchat (Cronbach's α = .94), and Twitter (Cronbach's α = .94).

Availability Heuristic. The availability heuristic was measured as the perceived severity of past negative privacy experience(s) on SNSs for the participants who have reported to have had such experience. Participants were asked to first select the SNS platforms on which they had negative privacy-related experience(s), and then were asked in one item to indicate the perceived severity of their experience on each SNS platform they have selected. Each item was measured on a scale from 1 ("Not severe at all") to 7 ("Very severe").

Bubble Heuristic. The findings from both Study 1 and Study 2A illustrate that how much people restrict their SNS privacy settings seemed to impart a sense of safety. The bubble heuristic, which is reflected in the restrictiveness of SNS users' privacy settings, was measured with one item that asked: "How public or private are your privacy settings on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]?" This question was asked for each SNS that a participant reported to use, and this item was measured on a scale of 1 ("Public") to 7 ("Very private").

Homophily Heuristic. Participants' perceived similarity to their social network connections (e.g., friends and/or followers) was measured to gauge the effect of the homophily heuristic on SNS users' privacy-related perceptions and behavior. Participants were asked to indicate their perceived similarity to their friends and followers on each of the SNSs they reported to use. The question read, "People may be similar to one another in terms of their age, background, political views, or other things. How similar or dissimilar do you feel to your connections (e.g., friends, followers, etc.) on

[Facebook/Instagram/Snapchat/Twitter]?" Response options ranged from 1 ("Not similar at all") to 7 ("Very similar").

Bandwagon Heuristic. Study 1 provided numerous anecdotes about how the bandwagon heuristic could affect SNS users' decisions about both disclosure and privacy. Study 2A also found that the bandwagon heuristic may play a role in people's decision-making processes, especially when observing and following other SNS users' specific behaviors. Therefore, participants were asked to indicate the extent to which they pay attention to what others post on SNSs ("To what extent do you pay attention to what others post on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]?"). This question was asked for each SNS platform that the participants reported to use, and each item was measured on a scale of 1 ("Not at all") to 7 ("Very much").

Hyperbolic Discounting. Study 1 and Study 2A showed that hyperbolic discounting may influence SNS users to share information on an impulse despite their awareness about the possible privacy risk associated with that disclosure. Also, these instances seemed to lead people to regret their decisions to disclose information on SNSs. These findings suggest that whether hyperbolic discounting affects SNS users' decisions about disclosure depends on users' tendency to act on an impulse and/or a repeated pattern of regretting their disclosure decisions. Four items were thus created to measure people's tendency to share information on impulse. The question stem for all four items read, "Looking back on your experience using [Facebook/Instagram/Twitter/Snapchat], to what extent have you shared something…" and then participants were presented with "…in the heat of the moment?" "...because you had to express or release my emotions (e.g., happiness, sadness, anger, etc.)?" ...and then regretted your decision later?" and "...on an impulse?" Each item was measured on a scale of 1 ("Never") to 7 ("Many times"). As with other measures, this scale was used to assess

participants' susceptibility to hyperbolic discounting for each SNS they reported to use. The average across the four items was computed to measure participants' experience with impulsive decisions about disclosure on four different SNSs examined in the study. Factor analysis showed that the four-item scale measured for each SNS was unidimensional, and these scales had high reliability on each SNS platform: Facebook (Cronbach's $\alpha = .90$), Instagram (Cronbach's $\alpha = .93$), Snapchat (Cronbach's $\alpha = .94$), and Twitter (Cronbach's $\alpha = .92$).

Ephemerality Heuristic. The ephemerality heuristic was measured by asking participants to indicate how frequently they share Stories on SNSs that offer this ephemeral feature (Facebook, Instagram, and Snapchat). Each item was measured on a scale from 1 ("Never") to 7 ("Very often"). Twitter does not offer any ephemeral features, so it was not included here.

Control Variables

Demographics. As individual differences influence how people disclose information (Hoy & Milne, 2010; Shi, Xu, & Chen, 2013; Sundar et al., 2019; Yu et al., 2015), several demographic variables (e.g., age, sex, ethnicity, race, sexual orientation, education level, religious affiliation, and political affiliation) were measured as control variables for the analyses.

Privacy concern on SNSs. Similarly, because SNS users' privacy concern could influence how much information they disclose on SNSs or how they select privacy settings on SNSs independent of cognitive heuristics, all participants' level of privacy concern was measured with three items derived from prior studies (e.g., Malhotra, Kim, & Agarwal, 2004; Smith, Milberg, & Burke, 1996; Westin, 1967) but adapted for the SNS context. These items asked how much they worry about their privacy as a result of using SNSs (e.g., "Compared

with other topics, privacy in social media is not very important to me," "I do not feel especially concerned about my privacy in social media," and "The danger to people's privacy when they use social media has been overblown"). Participants' agreement with the statements in each item was measured on a scale of 1 ("Strongly disagree") to 7 ("Strongly agree"). All of the items were reverse-coded so that a higher value on the scale indicated higher level of privacy concern. Their overall privacy concern was aggregated as the mean of three items, and factor analysis showed this scale to be unidimensional (Cronbach's $\alpha = .83$).

Number of SNSs used. The number of SNSs used was measured with a single item that asked the participants to select all of the SNSs they use out of the four popular SNSs (Facebook, Instagram, Snapchat, and Twitter).

Frequency of SNS use. Participants' frequency of SNS use was measured with a single item that asked how frequently they use SNSs they have reported to use in the question above. Each item was measured on a scale of 1 ("Rarely") to 7 ("Very frequently").

Chapter 9: Results from Study 2B

This chapter will describe how the hypotheses and research questions in Chapter 5 were examined in Study 2B and will present the results grouped by the dependent variables, which include three different aspects of privacy-related attitudes or behaviors (disclosure, perceived risk, and restrictiveness of privacy settings). As mentioned in the previous chapter, optimistic bias and inequity aversion were not included in the data analyses for Study 2B, as there was not enough evidence in Studies 1 and 2A to warrant continued investigation of the role that these two cognitive heuristics play in SNS users' decision-making processes about privacy.[3]

Effect of Heuristics on the Amount of Disclosure on SNSs

H1a, H3a, H4a, H5a, H6a, and H7a predicted a positive relationship between the affect heuristic, bubble heuristic, homophily heuristic, bandwagon heuristic, hyperbolic discounting, and ephemerality heuristic and SNS users' amount of disclosure on different SNSs. These six heuristics were included in the analyses because, as detailed later in this chapter, the availability heuristic was analyzed separately because of the limited sample size

[3] However, for purely exploratory purposes, these heuristics were included in preliminary hierarchical regression analyses. Results showed that optimistic bias was not significantly associated with the amount of disclosure on any of the SNS platforms, and it was not significantly associated with users' perceived risk about disclosure on Facebook, Instagram, and Snapchat. While prior literature suggests that optimistic bias would lower people's perceived risk about an activity, it was positively associated with perceived risk of disclosure on Twitter. These results show that optimistic bias about privacy risk likely does not serve as a mental shortcut in people's decision-making processes on SNSs or lead them to engage in riskier behaviors.

Similarly, inequity aversion was either not significantly associated or was negatively associated with the amount of disclosure on SNSs, and was either not significantly associated or positively associated with participants' perceived risk about disclosure, which is in the opposite direction from what is suggested in prior literature. As people in Study 1 and 2A report that they do not feel inequity aversion on SNSs or agree with its effect on their decisions on SNSs, the results about optimistic bias and inequity aversion from these hierarchical regression analyses are difficult to interpret and not very meaningful.

available to study that cognitive heuristic. Hierarchical regression analyses were performed for four SNSs (Facebook, Instagram, Snapchat, and Twitter) to test these hypotheses by first entering control variables (age, sex, education level, ethnicity, race, sexual orientation, religious views, political views, frequency of SNS use, number of SNSs used, and privacy concern on SNSs), and then in a second block entering the six variables associated with each of the heuristics above to assess their influence on the amount of disclosure on the four SNSs.

Overall, as predicted by H6a and H7a, SNS users' amount of disclosure on specific SNS platforms was positively associated with hyperbolic discounting and the ephemerality heuristic across all SNS platforms examined in this study. Moreover, users' amount of disclosure on Facebook appears to be the most affected by cognitive heuristics compared to the three other SNS platforms, as the amount of disclosure on Facebook is positively associated with five out of the six cognitive heuristics that were predicted to increase disclosure on SNSs. See Table 17 for full regression results. Findings specific to each platform are discussed next.

Facebook

Overall, the six predictors explained a significant amount of variance in Facebook users' amount of disclosure on the platform. As predicted by H1a, H4a, H5a, H6a, and H7a, Facebook users' amount of disclosure was positively predicted by the affect heuristic, homophily heuristic, bandwagon heuristic, hyperbolic discounting, and ephemerality heuristic measures. However, while H3a predicted that the bubble heuristic would also be positively associated with the amount of disclosure, the regression analysis showed that the bubble heuristic measure negatively predicted users' amount of disclosure.

Table 17

Cognitive Heuristics and the Amount of Disclosure on SNSs

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
Model 1: Control Variables												
Constant	.30	.50	.00	-.36	.75	.00	-.87	1.26	.00	-.29	.70	.00
Age	.00	.00	.00	-.01	.01	-.05	.01	.01	.04	.00	.01	.01
Sex	.06	.10	.02	.00	.14	.00	.44	.23	.13	-.07	.15	-.02
Education Level	.05	.03	.05	.04	.04	.04	.20	.07	.18**	.07	.04	.07
Ethnicity	-.25	.18	-.05	-.21	.23	-.04	.19	.30	.04	-.36	.27	-.06
Race	.09	.12	.03	-.14	.15	-.04	-.22	.25	-.06	-.16	.16	-.04
Sexual Orientation	.04	.17	.01	.14	.22	.03	-.62	.38	-.11	-.02	.23	.00
Religion	.01	.03	.01	.06	.04	.07	.03	.06	.04	.14	.04	.18**
Political views	.02	.03	.02	.01	.04	.01	.07	.06	.08	.02	.05	.03
Frequency of SNS Use	.03	.04	.03	.22	.06	.22***	.18	.10	.19	.07	.06	.07
Number of SNSs Used	.16	.05	.09**	.11	.09	.05	.06	.19	.02	.25	.09	.13**
Privacy Concern on SNSs	-.12	.04	-.11**	-.07	.05	-.06	-.13	.08	-.12	-.14	.05	-.12*
R^2 change		.42			.43			.54			.34	

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
F for change in R^2		25.49***			19.7***			11.61***			14.97***	
Model 2: Heuristic Effects on the Amount of Disclosure on SNSs												
Affect Heuristic	.14	.05	.11**	.07	.07	.04	.04	.11	.03	.12	.006	.09†
Bubble Heuristic	-.13	.03	-.14***	.03	.03	.04	-.03	.07	-.03	-.04	.04	-.05
Homophily Heuristic	.19	.04	.18***	.16	.05	.15**	.14	.08	.14†	.22	.05	.21***
Bandwagon Heuristic	.18	.05	.18***	.01	.06	.01	.10	.09	.10	.00	.06	.00
Hyperbolic Discounting	.31	.04	.32***	.25	.06	.26***	.29	.08	.34***	.31	.05	.33***
Ephemerality Heuristic	.13	.04	.16***	.20	.05	.25***	.15	.07	.18*	No ephemeral features available on Twitter		
R^2 change		.23			.15			.13			.13	
F for change in R^2		40.47***			15.91***			13.05***			15.52***	
N		356			258			84			279	

Note. ***p <.001. **p < .01. *p < .05. †p < .10.

Instagram

The six predictors explained a significant amount of variance overall in Instagram users' amount of disclosure as well. As predicted by H4a, H6a, and H7a, Instagram users' amount of disclosure was positively associated with the homophily heuristic, hyperbolic discounting, and ephemerality heuristic. However, H1a, H3a, and H5a were not supported on Instagram, as the amount of disclosure was not significantly related to the affect heuristic, bubble heuristic, or bandwagon heuristic measures.

Snapchat

The six predictors explained a significant amount of variance in Snapchat users' amount of disclosure on that platform. Snapchat users' amount of disclosure was positively associated with hyperbolic discounting and ephemerality heuristic, as predicted by H6a and H7a. On the other hand, H1a, H3a, H4a, and H5a were not supported on Snapchat, as users' amount of disclosure was not significantly predicted by the affect heuristic, bubble heuristic, homophily heuristic, and bandwagon heuristic measures.

Twitter

On Twitter, the five heuristics tested (all except the ephemerality heuristic which does not apply to Twitter) explained a significant amount of variance in Twitter users' amount of disclosure. As predicted by H4a and H6a, Twitter users' amount of disclosure was positively associated with the homophily heuristic and hyperbolic discounting measures. However, H1a, H3a, and H5a were not supported, as the amount of disclosure by Twitter users was not significantly related to the affect heuristic, bubble heuristic, and bandwagon heuristic measures. As mentioned above, H7a was not tested for Twitter users because Twitter does not offer ephemeral features like Stories.

Effect of Heuristics on Perceived Risk about Disclosure on SNSs

H1b, H3b, H4b, H5b, H6b, and H7b predicted effects of the affect heuristic, bubble heuristic, homophily heuristic, bandwagon heuristic, hyperbolic discounting, and ephemerality heuristic on SNS users' perceived risk about disclosure on SNSs. Similar to the analyses above, hierarchical regression analyses were performed by first entering control variables (age, sex, education level, ethnicity, race, sexual orientation, religious views, political views, frequency of SNS use, number of SNSs used, and privacy concern on SNSs), and then entering the six predictor variables corresponding to each heuristic to examine how they are related to participants' self-reported perceived risk about disclosure on SNSs.

Across all four platforms tested, only the affect heuristic predicted risk perceptions. More positive affect was associated with less perceived risk about disclosure across all four SNS platforms. None of the other heuristics seemed to lower SNS users' privacy risk overall. However, the relationship between cognitive heuristics (except for the affect heuristic) and users' perceived risk about disclosure varied across SNSs, as discussed next. See Table 18 for full regression results.

Table 18

Cognitive Heuristics and Perceived Risk about Disclosure on SNSs

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
Model 1: Control Variables												
Constant	2.39	.78	.00	.00	.96	.00	2.75	2.06	.00	2.71	.91	.00
Age	.00	.01	.01	.00	.01	.00	.01	.02	.04	.00	.01	.03
Sex	-.20	.16	-.06	-.11	.18	-.03	-.79	.38	-.22*	-.24	.19	-.07
Education Level	.02	.05	.02	.05	.06	.05	.10	.12	.09	.03	.06	.03
Ethnicity	.47	.28	.08	.28	.30	.05	.47	.49	.09	.57	.36	.09
Race	.44	.19	.12*	.52	.20	.14**	.54	.40	.13	.31	.21	.08
Sexual Orientation	.28	.26	.05	.37	.28	.07	1.25	.62	.20*	.24	.30	.04
Religion	-.02	.05	-.03	.08	.05	.10	.12	.09	.14	.07	.05	.08
Political views	.14	.05	.15**	-.03	.05	-.03	.03	.10	.36	-.01	.06	-.01
Frequency of SNS Use	.01	.07	.01	.10	.07	.10	-.01	.16	-.01	-.03	.08	-.03
Number of SNSs Used	-.05	.09	-.03	-.07	.12	-.03	-.05	.31	-.02	-.01	.12	-.01
Privacy Concern on SNSs	.29	.06	.25***	.31	.07	.28***	.07	.13	.06	.26	.07	.22***
R^2 change		.11			.09			.05			.06	

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
F for change in R^2		5.239***			3.37***			1.53			42.66**	
Model 2: Heuristic Effects on Perceived Risk about Disclosure on SNSs												
Affect Heuristic	-.39	.08	-.29***	-.57	.09	-.38***	-.55	.18	-.36**	-.37	.08	-.28***
Bubble Heuristic	.21	.05	.21***	.18	.04	.22***	.18	.11	.16	.21	.05	.25***
Homophily Heuristic	-.04	.07	-.03	-.06	.07	-.05	-.08	.13	-.08	-.03	.07	-.02
Bandwagon Heuristic	-.01	.08	-.01	.02	.08	.01	.08	.14	.07	.01	.08	.01
Hyperbolic Discounting	.08	.06	.08	.18	.07	.19*	-.16	.13	-.17	.14	.06	.15*
Ephemerality Heuristic	.15	.06	.17**	.11	.06	.14†	.22	.12	.25†	No ephemeral features available on Twitter		
R^2 change		.11			.20			.14			.12	
F for change in R^2		9.90***			13.28***			3.62**			9.21***	
N		356			257			84			278	

Note. ***p <.001. **p < .01. *p < .05. †p < .10.

Facebook

On Facebook, overall the six predictors explained a significant amount variance in Facebook users' perceived risk about disclosure on Facebook. As predicted by H1b, Facebook users' perceived risk about disclosure on Facebook was negatively associated with how positive they feel about Facebook. However, the remaining hypotheses that predicted the other heuristics' effect on perceived risk about disclosure on SNSs were not supported on Facebook. Although H3b and H7b predicted users' perceived risk about disclosure to be negatively associated with the bubble heuristic and ephemerality heuristic, users' perceived risk about disclosure on Facebook was positively associated with the bubble heuristic and the ephemerality heuristic measures. Also, Facebook users' perceived risk about disclosure was not significantly related to the homophily heuristic, bandwagon heuristic, or hyperbolic discounting measures.

Instagram

The six predictors explained a significant amount of variance in Instagram users' perceived risk about disclosure on Instagram overall. As predicted by H1b, Instagram users' perceived risk about disclosure was negatively associated with the affect heuristic, such that users felt less risk about disclosure the more positively they felt about Instagram. On the other hand, the other hypotheses that predicted the various heuristics' effects on perceived risk about disclosure on SNSs were not supported on Instagram. Although H3b and H6b predicted users' perceived risk about disclosure would be negatively associated with the bubble heuristic and hyperbolic discounting, users' perceived risk about disclosure on Instagram was positively associated with the bubble heuristic and hyperbolic discounting measures. Moreover, users' perceived risk about disclosure was not significantly predicted

by the homophily heuristic or bandwagon heuristic measures, and results for the ephemerality heuristic were marginal (p = .06).

Snapchat

On Snapchat, the six predictors also explained a significant amount of variance on Snapchat users' perceived risk about disclosure on Snapchat overall. As with the other platforms, H1b was supported on Snapchat as well. Snapchat users' perceived risk about disclosure on Instagram was negatively associated with the extent to which users feel positively about Snapchat. On the other hand, perceived risk about disclosure on Snapchat was not significantly related to any of the other heuristics: bubble heuristic, homophily heuristic, bandwagon heuristic, or hyperbolic discounting. Again, results for the ephemerality heuristic were marginal (p = .06).

Twitter

The five predictors explained a significant amount of variance in Twitter users' perceived risk about disclosure on Twitter. As with the other SNS platforms, H1b was supported on Twitter; more positive feelings about Twitter were associated with lower perceived risk about disclosure on Twitter. However, none of the other hypotheses about heuristic effects on SNS users' perceived risk about disclosure in Twitter were supported. While H3b and H6b predicted that perceived risk about disclosure would be negatively associated with the bubble heuristic and hyperbolic discounting, Twitter users' perceived risk about disclosure was positively associated with the bubble heuristic and hyperbolic discounting measures. Also, Twitter users' perceived risk about disclosure on Twitter was not significantly related to the homophily heuristic or bandwagon heuristic measures.

Effect of Heuristics on the Restrictiveness of Privacy Settings

H2c and H5c were proposed to study how the availability heuristic and bandwagon heuristic, which are two heuristics that were identified as "privacy" (versus "disclosure") heuristics, are related to the restrictiveness of SNS users' privacy settings. To address H5c, which asked how the bandwagon heuristic is related to the restrictiveness of users' privacy settings on SNSs, hierarchical regression analyses were performed by first entering the control variables (age, sex, education level, ethnicity, race, sexual orientation, religious views, political views, frequency of SNS use, number of SNSs used, and privacy concern on SNSs), and then entering the measure for bandwagon heuristic as a predictor variable to examine how it is related to the restrictiveness of their privacy settings (see Table 19). The bandwagon heuristic did not explain a significant amount of variance in the restrictiveness of their privacy settings on any of the four SNS platforms. H5c was thus not supported on every SNS platform, as adding the bandwagon heuristic into the model decreased the adjusted R^2 value, which suggests that the predictor improved the model by less than expected by chance. H2c was addressed separately, as described below.

Table 19

Bandwagon Heuristic and Restrictiveness of Privacy Settings on SNSs

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
Model 1: Control Variables												
Constant	2.40	.63	.00	2.34	.82	.00	2.48	1.26	.00	2.39	.72	.00
Age	-.01	.01	-.11*	-.01	.01	-.05	.02	.01	.12	-.01	.01	-.08
Sex	.12	.15	.04	.07	.17	.02	-.42	.26	-.16	.02	.17	.01
Education Level	.04	.04	.05	.05	.05	.06	.07	.08	-.08	.02	.05	.03
Ethnicity	.60	.25	.13*	.57	.29	.12†	.73	.36	.20*	.62	.30	.12*
Race	.09	.17	.03	.07	.20	.02	.43	.28	.14	.02	.19	.01
Sexual Orientation	.43	.23	.09†	.36	.26	.08	.74	.42	.17†	.42	.26	.10
Religion	.03	.04	.05	.03	.05	.05	.06	.07	.10	.04	.05	.06
Political views	.03	.04	.05	.04	.05	.05	.09	.07	.13	.06	.05	.08
Frequency of SNS Use	-.01	.06	-.01	.06	.07	.07	-.08	.10	-.10	-.01	.07	-.02
Number of SNSs Used	.00	.08	.00	.01	.12	.00	-.27	.23	-.12	.00	.10	.00
Privacy Concern on SNSs	.35	.05	.37***	.33	.06	.34***	.42	.09	.47***	.36	.06	.37***
R^2 change		.11			.11			.20			.10	

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
F for change in R^2	4.86***			3.07***			3.23***			3.85***		
Model 2: Effect of Bandwagon Heuristic on Restrictiveness of Privacy Settings on SNSs												
Bandwagon Heuristic	.10	.07	.18***	.02	.08	.02	.07	.10	.10	.07	.07	.08
R^2 change	-.0031			-.0032			-.0046			-.0065		
F for change in R^2	2.22 (p = .14)			.09 (p = .76)			.49 (p = .49)			.95 (p = .33)		
N	349			261			90			280		

Note. ***p <.001. **p < .01. *p < .05. †p < .10.

Results for the Availability Heuristic. As described in the previous chapter, the availability heuristic was measured by having participants indicate the perceived severity of any past negative privacy experience they had on the different SNSs. Due to this measurement approach, the perceived severity of participants' past negative privacy experience was measured only for a subset of the sample that includes participants who reported having had a negative privacy-related experience on any of the SNSs. Only 69 participants on Facebook, 22 on Instagram, 7 on Snapchat, and 17 on Twitter answered the question that measured the availability heuristic. Because of the resulting sample sizes available to study the availability heuristic, the hypotheses about the availability heuristic (H2a-c) were tested separately (i.e., without entering the availability heuristic measure as a predictor variable in the hierarchical regression analyses described above). Including availability heuristic in the hierarchical regression analyses above would have made the overall sample size for the analyses too small to test these regression models with several predictors.[4]

Therefore, to test H2a-c on Facebook, partial correlations between the perceived severity of past negative privacy experiences on Facebook and (1) amount of disclosure, (2)

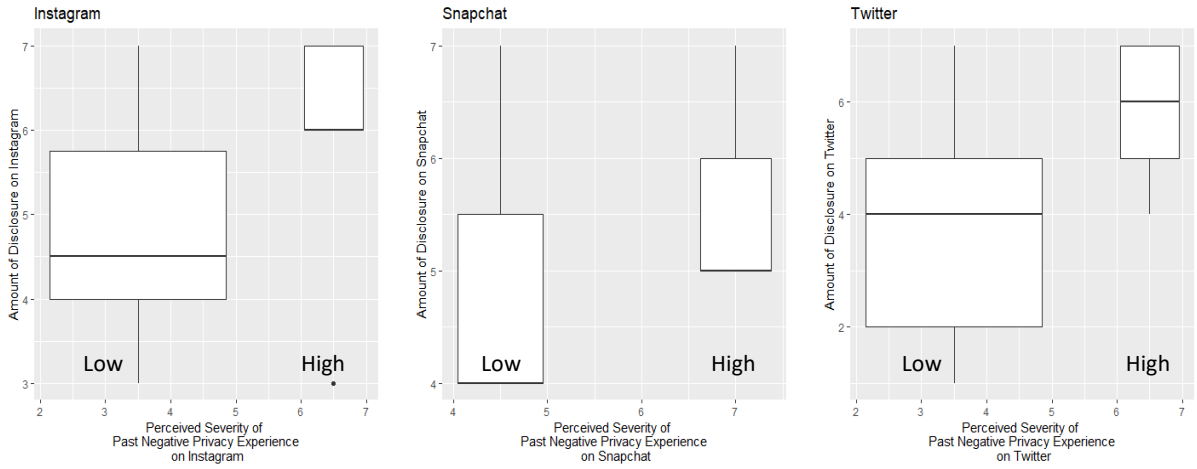
[4] To address the issue with small sample sizes available to study the role of availability heuristic on different SNSs, the measures for the availability heuristic on each SNS can be transformed into a dichotomous variable, where any case of past negative privacy experience would be coded as "1" (regardless of the participants' perceived severity of their experiences), and the rest as "0," to include the full sample. However, when this dichotomous variable is entered into regression analyses on the amount of disclosure on SNSs, the perceived risk about disclosure, and the restrictiveness of privacy settings, this measure is not significantly related to the amount of disclosure or perceived risk about disclosure on any of the SNSs. This dichotomous variable is positively associated with the restrictiveness of privacy settings on Facebook, but it is not significantly associated with the restrictiveness of privacy settings on any other SNS platforms. It is important to consider the perceived severity of past negative experiences to understand the role of availability heuristic on SNSs, as simply having had negative privacy experiences do not seem to influence SNS users' risk perceptions and decisions.

restrictiveness of privacy settings, and (3) perceived risk about disclosure on Facebook were computed. The perceived severity of past negative privacy experience on Facebook was not significantly related to the amount users disclose (r = .22, p = .09) and the restrictiveness of their privacy settings (r = .09, p = .51), but it was positively correlated with the perceived risk about disclosure (r = .33, p = .01) on Facebook.

For the remaining three platforms, partial correlations were not computed, as those measures would not be meaningful when dealing with such small sample sizes. An alternative approach was thus taken to test H2a-c on Instagram, Snapchat, and Twitter, whereby Figures 5-7 help explore whether there are patterns in the data that reflect relationships predicted in the hypotheses (but again, these patterns could not be properly tested on these platforms, so this is just a descriptive analysis). Contrary to what H2a predicted, Figure 5 shows that people who have had a more severe negative privacy experience in the past share more information than those who reported having had a less severe negative privacy experience. Consistent with what H2c predicted, Figure 6 shows that people who reported having had a more severe negative privacy experience have more restrictive privacy settings than those who reported to have had a less severe negative privacy experience in the past. Lastly, Figure 7 shows that people who have had more severe negative privacy experiences perceive greater risk about disclosure than those have had less severe experiences on Instagram and Twitter, but no clear relationship can be determined about Snapchat users due to the extremely small sample size. One plausible explanation of these figures may be that people who disclose a lot were more likely to have more severe negative privacy experiences and that having had those severe experiences would have led these users to select more restrictive privacy settings and continue to feel more risk about disclosure after such experiences.

Figure 5

Amount of Disclosure by Perceived Severity of Past Negative Privacy Experience (High-Low)



Note. The boxplot on the left reflects the amount of disclosure by participants who reported to have experienced a negative event that is less severe (labeled as "Low"), and the boxplot on the right reflects the amount of disclosure by those who reported having had a more severe negative privacy event (labeled as "High").

Figure 6

Restrictiveness of Privacy Settings by Perceived Severity of Past Negative Privacy Experience (High-Low)

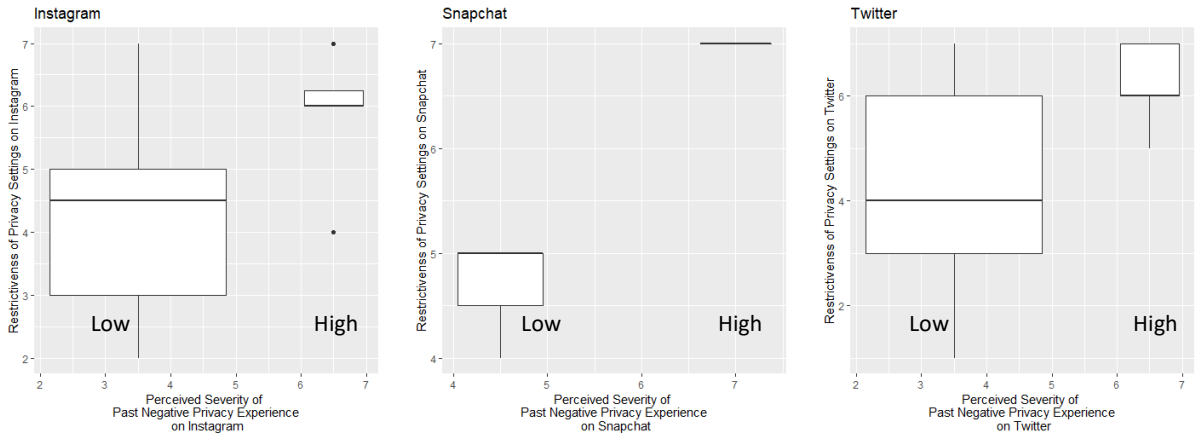
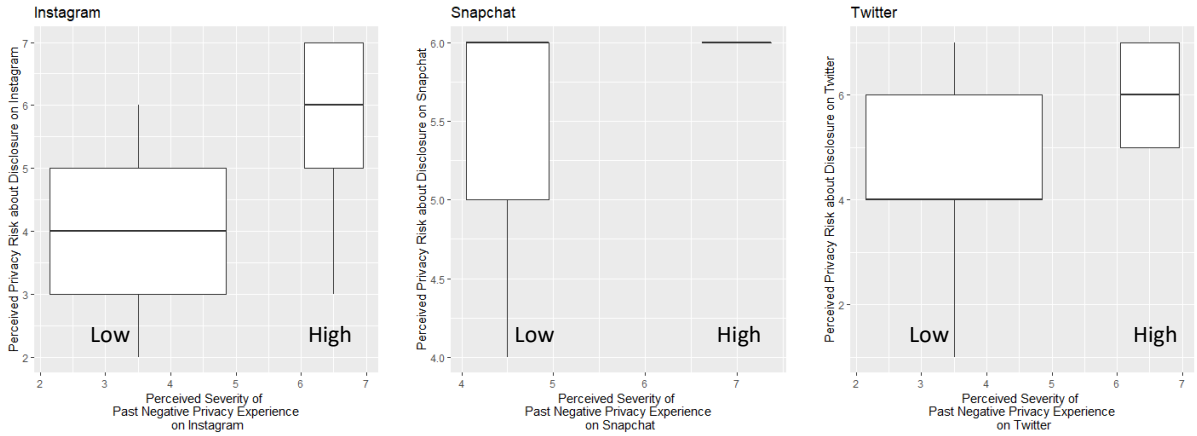


Figure 7

Perceived Risk about Disclosure by Perceived Severity of Past Negative Privacy Experience (High-Low)



Summary

The results described in this chapter offer insight into how the heuristics are related to SNS users' disclosure and privacy-protecting behavior and attempt to help explain the mechanism by which the heuristics may influence SNS users' decision-making processes by understanding their perceived risk about disclosure. Although the results provide a clear picture into how the heuristics are related to SNS users' amount of disclosure, the picture is fuzzier about the underlying mechanism that explains how heuristics influence the amount of disclosure on SNSs (see Tables 20 and 21 for summary of results). While the hypotheses about SNS users' perceived risk about disclosure were posed to understand how users' risk perception might be affected by the heuristics, and thus then potentially influence users' decisions about disclosure, in many cases, users' decisions about disclosure were not aligned with their self-reported perceived risk. These results could suggest that heuristic effects influence users' decisions too quickly to raise or lower SNS users' perceived risk about disclosure to inform their final decisions. As demonstrated by Gigerenzer and colleagues

(1999), people often use mere recognition or a single reason that can be based on the first, not the best, cue that they see in their environment to make decisions, and so relying on cognitive heuristics may not allow time for a risk analysis. It would be difficult, however, to empirically document whether any sort of risk analysis takes place when people rely on cognitive heuristics because people's psychological decision-making processes cannot be measured at the same time as their actions. For example, methods like think aloud studies would embed rationality into the testing environment, as they require participants to explain their actions in the moment, and this process would likely compel participants to provide reasonings (e.g., perceived risk) that match their decisions. Nonetheless, it would be valuable to continue exploring whether the speed of heuristic processes is too quick to allow for risk analyses—perhaps by collecting additional empirical evidence that helps researchers make better inferences about people's risk perceptions during heuristic-based decision making.

Yet, looking at the results for the effects of heuristics on the amount of disclosure suggest that relying on cognitive heuristics may have negative implications for users' *actual* privacy risk on SNSs. Hyperbolic discounting and the ephemerality heuristic, which were predicted to increase the amount of disclosure on SNSs, were indeed positively associated with the amount of disclosure across all SNSs examined in this study. Moreover, the homophily heuristic, which was also predicted to increase the amount of disclosure, was also positively associated with a greater amount of disclosure across three out of the four SNSs examined. While the positive relationship between the perceived similarity to social network connections on Snapchat and the amount of disclosure on Snapchat was not significant, the *p*-value was approaching significance ($p = .08$), and this p-value may have been affected by the relatively small sample size for Snapchat users ($n = 84$).

These findings suggest that three cognitive heuristics (homophily heuristic, hyperbolic discounting, and ephemerality heuristic) could increase the amount of disclosure across multiple SNS platforms. However, while the availability heuristic triggered by a past negative privacy experience was the only heuristic (aside from negative affect) that was predicted to decrease the amount of disclosure on SNSs, and thus help users protect their privacy, the results did not support this hypothesis (H2a) on any of the SNS platforms. These findings, together, suggest that SNS users should be wary of the effects of at least some kinds of heuristics on their privacy decision making. Facebook users, in particular, may be most susceptible to heuristics when they make decisions about disclosure, as the amount of disclosure was positively associated with five out of the seven heuristics examined in Study 2B. The findings about Facebook users should be further investigated to understand why Facebook users are particularly more prone to be affected by cognitive heuristics compared to users of other SNSs.

The hypotheses that predicted negative relationships between heuristics and perceived risk about disclosure on SNSs were posed based on a logic that people would disclose more information as a result of lowered perceived risk due to heuristic effects. However, only the affect heuristic was negatively associated with the perceived risk about disclosure across four SNSs. Otherwise, most other heuristics (bubble heuristic, homophily heuristic, bandwagon heuristic, hyperbolic discounting, and ephemerality heuristic) were not negatively associated with perceived risk about disclosure. Interestingly, people's perceived risk about disclosure was generally positively associated with the ephemerality heuristic; there was a significant positive relationship between perceived risk about disclosure and ephemerality on Facebook, as well as marginally significant positive relationships between these two variables on Instagram and Snapchat.

These findings may help understand the role of the homophily heuristic, hyperbolic discounting, and the ephemerality heuristic because they suggest that these heuristics could increase the amount of disclosure, without affecting SNS users' risk perception, and thus have theoretical implications for using the privacy calculus framework to understand SNS users' decision-making processes. While the privacy calculus model assumes that people's decisions are a result their analysis of risks and benefits associated with their decisions, the current findings suggest that decisions that rely on cognitive heuristics may not involve such a risk analysis.

H2c and H5c were proposed to understand how the availability heuristic and bandwagon heuristic operate to affect privacy-related behaviors (i.e., privacy protection behaviors other than disclosure). The restrictiveness of SNS users' privacy settings was not associated with the bandwagon heuristic, and its relationship to the availability heuristic could not be considered conclusive due to the limited sample size available to study the role of the availability heuristic as noted earlier. Future studies employing a larger sample will be needed to test the influence of the availability heuristic on SNS users' decisions about their privacy in terms of the restrictiveness of users' privacy settings.

Table 20

Summary of Results from Study 2B

Dependent Variables		Hypotheses and Research Questions		Facebook	Instagram	Snapchat	Twitter
Amount of Disclosure	Hierarchical Regressions	H1a	Affect Heuristic	Supported	Not supported	Not supported	Not supported
		H3a	Bubble Heuristic	Not supported	Not supported	Not supported	Not supported
		H4a	Homophily Heuristic	Supported	Supported	Not supported	Supported
		H5a	Bandwagon Heuristic	Supported	Not supported	Not supported	Not supported
		H6a	Hyperbolic Discounting	Supported	Supported	Supported	Supported
		H7a	Ephemerality Heuristic	Supported	Supported	Supported	N/A
	Partial Correlation & Figures	H2a	Availability Heuristic	Not supported	Most likely not supported *(People with more severe experiences share more)*		
Perceived Risk about Disclosure	Hierarchical Regressions	H1b	Affect Heuristic	Supported	Supported	Supported	Supported
		H3b	Bubble Heuristic	Not supported	Not supported	Not supported	Not supported
		H4b	Homophily Heuristic	Not supported	Not supported	Not supported	Not supported
		H5b	Bandwagon Heuristic	Not supported	Not supported	Not supported	Not supported
		H6b	Hyperbolic Discounting	Not supported	Not supported	Not supported	Not supported
		H7b	Ephemerality Heuristic	Not supported	Not supported	Not supported	N/A
	Partial Correlation & Figures	H2b	Availability Heuristic	Supported	Difficult to tell (see Figures 5-7)		
Restrictiveness of Privacy Settings	Hierarchical Regressions	H5c	Bandwagon Heuristic	Not supported	Not supported	Not supported	Not supported
	Partial Correlation & Figures	H2c	Availability Heuristic	Not supported	Could be supported with more data *(People who have had more severe negative experiences have more restrictive privacy settings)*		

Note. Optimistic Bias (RQ1 and RQ2) and Inequity Aversion (RQ3 and RQ4) were not addressed in the data analyses for Study 2B.

Table 21

Summary of Results from Studies 2A and 2B

Hypotheses and Research Questions		Study 2A	Study 2B			
			Facebook	Instagram	Snapchat	Twitter
H1a	The affect heuristic, as reflected in the degree to which users feel affectively positive about a specific SNS, is positively associated with their amount of disclosure on that SNS.	Supported	Supported	Not supported	Not supported	Not supported
H1b	The affect heuristic, as reflected in the degree to which users feel affectively positive about a specific SNS is negatively associated with their perceived risk about disclosure on that SNS.	Supported	Supported	Supported	Supported	Supported
H2a	The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is negatively associated with the amount of disclosure.	Supported	Not supported	N/A	N/A	N/A
H2b	The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is positively associated with the perceived risk about disclosure on SNSs.	Supported	Supported	N/A	N/A	N/A
H2c	The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is positively associated with the restrictiveness of their privacy settings.	Supported	Not supported	N/A	N/A	N/A
RQ1	Is users' optimistic bias, as reflected in the perceived likelihood of having a negative privacy experience on SNSs compared to others, related to the amount of	Not positively	N/A	N/A	N/A	N/A

Hypotheses and Research Questions		Study 2A	Study 2B			
			Facebook	Instagram	Snapchat	Twitter
	information users disclose on SNSs?	related				
RQ2	Is users' optimistic bias, as reflected in the perceived likelihood of having a negative privacy experience on SNSs compared to others, related to the restrictiveness of users' privacy settings on SNSs?	Not negatively related	N/A	N/A	N/A	N/A
H3a	The bubble heuristic, as reflected in the restrictiveness of users' privacy settings, is positively associated with their amount of disclosure on SNSs.	Supported	Not supported	Not supported	Not supported	Not supported
H3b	The bubble heuristic, as reflected in the restrictiveness of users' privacy settings, is negatively associated with their perceived risk about disclosure on SNSs.	Supported	Not supported	Not supported	Not supported	Not supported
H4a	The homophily heuristic, as reflected in users' perceived similarity to their social network connections, is positively associated with their amount of disclosure on SNSs.	Supported	Supported	Supported	Not supported	Supported
H4b	The homophily heuristic, as reflected in users' perceived similarity to their social network connections, is negatively associated with their perceived risk about disclosure on SNSs.	Supported	Not supported	Not supported	Not supported	Not supported
H5a	The bandwagon heuristic, which is reflected in the extent to which users pay attention to others' posts on SNSs, is positively associated with their amount of disclosure on SNSs.	Partially supported	Supported	Not supported	Not supported	Not supported
H5b	The bandwagon heuristic, which is reflected in the extent to which users pay attention to others' posts on	Partially	Not	Not	Not	Not

Hypotheses and Research Questions		Study 2A	Study 2B			
			Facebook	Instagram	Snapchat	Twitter
	SNSs, is negatively associated with their perceived risk about disclosure on SNSs.	supported	supported	supported	supported	supported
H5c	The bandwagon heuristic, which is reflected in the extent to which users pay attention others' privacy settings, is positively associated with to the restrictiveness of their own privacy settings.	Not supported	Not supported	Not supported	Not supported	Not supported
RQ3	Is inequity aversion, as reflected in the degree of users' perceived benefit compared to other users, related to their amount of their disclosure on SNSs?	Not positively related	N/A	N/A	N/A	N/A
RQ4	Is inequity aversion, as reflected in the degree of users' perceived benefit compared to other users, related to their perceived risk about disclosure on SNSs?	Not negatively related	N/A	N/A	N/A	N/A
H6a	Hyperbolic discounting, as reflected in the degree to which users make decisions about disclosure on an impulse on SNSs, is positively associated with their amount of disclosure on SNSs.	Partially supported	Supported	Supported	Supported	Supported
H6b	Hyperbolic discounting, as reflected in the degree to which users make decisions about disclosure on an impulse on SNSs, is negatively associated with their perceived risk about disclosure on SNSs.	Not supported	Not supported	Not supported	Not supported	Not supported
H7a	The ephemerality heuristic, as reflected in the extent to which users use ephemeral features on SNS, is positively associated with the amount of their overall disclosure on SNSs.	Supported	Supported	Supported	Supported	N/A

Hypotheses and Research Questions		Study 2A	Study 2B			
			Facebook	Instagram	Snapchat	Twitter
H7b	The ephemerality heuristic, as reflected in the extent to which users use ephemeral features on SNS, is negatively associated with their perceived risk about disclosure on SNSs.	Supported	Not supported	Not supported	Not supported	N/A

Additional Analyses

Effect of Cognitive Heuristics on the Amount of Disclosure about Sensitive Topics on SNSs

Because the results concerning the effects of heuristics on the amount of disclosure suggest that relying on cognitive heuristics may have negative implications for SNS users' privacy risk, further analyses were performed to assess whether the heuristics also influence people's decisions to share not just more, but more *sensitive* information. If true, this would worsen their privacy risk. Hierarchical regression analyses similar to those that were conducted to test H1a, H3a, H4a, H5a, H6a, and H7a were performed with the same predictors but this time the amount of disclosure for the topics that were rated by participants to be sensitive to discuss on SNSs served as the dependent variable. Factor analyses showed that five items that measured the amount of information users share about the five most sensitive topics (contact information, deep feelings and emotions, romantic relationships, photos of them, and negative things that happened to them) formed a unidimensional scale and had high reliability in all four SNS platforms: Facebook (Cronbach's α = .88), Instagram (Cronbach's α = .88), Snapchat (Cronbach's α = .85), and Twitter (Cronbach's α = .88). Therefore, amount of disclosure about sensitive topics was measured as the average of these five items in each SNS platform.

The analyses revealed interesting insights into the effect of heuristics on SNS users' decisions about disclosure. Overall, the six predictor variables explained a significant amount of variance in SNS users' disclosure about sensitive topics on Facebook, Instagram, and Snapchat, and the five predictor variables (excluding ephemerality) explained a significant amount of variance in Twitter users' disclosure about sensitive topics overall. Three control variables were significantly associated with the amount of disclosure about sensitive topics

across all SNSs as follows: Older SNS users were less likely to share sensitive information compared to younger users, and SNS users who reported to be religious were more likely to share sensitive information compared to other users who reported to be less religious. Also, users' general concern about privacy on SNSs was negatively associated with the amount of disclosure about sensitive topics across all SNSs. Consistent with the findings for how the heuristics affect the amount of disclosure in general discussed earlier, hyperbolic discounting was positively associated with the amount of disclosure about sensitive topics across all four SNSs. Similarly, the ephemerality heuristic was positively associated with the amount of disclosure about sensitive topics on Facebook and Instagram. There was a positive association between the ephemerality heuristic and the amount of disclosure about sensitive topics on Snapchat, with the p-value approaching significance ($p = .07$). On the other hand, while the homophily heuristic was positively associated with the amount of disclosure in general across all four SNSs (including a marginally significant relationship on Snapchat), as predicted by the hypothesis, this was not the case for amount of disclosure about sensitive topics on any SNSs.

These additional findings suggest that hyperbolic discounting and the ephemerality heuristic might have serious negative implications for SNS users' privacy risk. These two heuristics could lead people to share *not just more information about themselves but more information about sensitive topics on SNSs* in a way that may not align with their perceived risk about disclosure. See Table 22 for full regression results for the amount of disclosure about sensitive topics on SNSs.

Table 22

Cognitive Heuristics and Amount of Disclosure about Sensitive Topics on SNSs

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
Model 1: Control Variables												
Constant	1.81	.46	.00	.79	.62	.00	2.66	1.27	.00	.39	.60	.00
Age	-.02	.00	-.14***	-.02	.01	-.11**	-.03	.01	-.15*	-.02	.01	-.13**
Sex	.02	.09	.01	.00	.12	.00	-.06	.23	-.02	-.03	.13	-.01
Education Level	.04	.03	.05	.08	.14	.08*	.05	.07	.05	.11	.04	.12**
Ethnicity	.12	.16	.03	.11	.20	.02	.20	.30	.05	.21	.23	.04
Race	-.07	.11	-.02	-.20	.13	-.58	.26	.25	.07	-.02	.14	.00
Sexual Orientation	-.02	.15	.00	-.01	.18	.00	.13	.38	.02	.10	.20	.02
Religion	.06	.03	.09*	.08	.13	.11*	.11	.06	.15†	.10	.04	.15**
Political views	.05	.03	.06	.08	.14	.09*	.03	.06	.03	.09	.04	.11*
Frequency of SNS Use	.02	.04	.02	.06	.05	.06	.03	.10	.04	-.02	.05	-.03
Number of SNSs Used	.03	.05	.02	.08	.08	.04	-.13	.19	-.05	.15	.08	.08
Privacy Concern on SNSs	-.18	.04	-.18***	-.11	.04	-.10*	-.23	.08	-.23**	-.18	.05	-.17***
R^2 change		.48			.50			.49			.41	

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
F for change in R^2		31.26***			25.35***			9.72***			19.53***	
Model 2: Heuristic Effects on the Amount of Disclosure about Sensitive Topics on SNSs												
Affect Heuristic	.04	.05	.03	.04	.06	.03	-.02	.11	-.02	.05	.05	.04
Bubble Heuristic	-.05	.03	-.06†	.02	.03	.03	-.08	.07	-.08	-.02	.04	-.03
Homophily Heuristic	.09	.04	.09*	.02	.04	.03	.11	.08	.12	.13	.04	.13**
Bandwagon Heuristic	.04	.04	.05	-.01	.05	-.01	.10	.09	.11	.04	.05	.04
Hyperbolic Discounting	.28	.04	.33***	.36	.05	.40***	.25	.08	.31**	.32	.04	.38***
Ephemerality Heuristic	.19	.03	.25***	.17	.04	.23***	.13	.07	.17†	No ephemeral features available on Twitter		
R^2 change		.18			.17			.12			.13	
F for change in R^2		31.39***			15.91***			5.38***			16.76***	
N		345			255			82			276	

Note. ***p <.001. **p < .01. *p < .05. †p < .10.

Effect of Cognitive Heuristics on Perceived Comfort and Safety about Disclosure on SNSs

Although the participants from Study 1 used the words "risky," "safe," and "comfortable" in similar contexts to explain how they think cognitive heuristics may have influenced their decisions about disclosure and/or privacy, factor analysis of three items that measured participants' perceived risk, comfort, and safety about disclosure did not load well on the same parent factor, as noted in Chapter 8. To better understand the relationship between SNS users' perceived "risk" about disclosure, through the dialectic lens of their perceived comfort and safety about disclosure, another set of hierarchical regression analyses was performed. As with the previous regression analyses, control variables (age, sex, education level, ethnicity, race, sexual orientation, religious views, political views, frequency of SNS use, number of SNSs used, and privacy concern on SNSs) were entered into the model first, and then the six predictors were entered to examine if and how they relate to participants' perceived comfort and safety about disclosure. The dependent variables for these analyses were created by averaging the two items that measured participants' perceived comfort and safety about disclosure on each of the four SNSs, as discussed in Chapter 8.

Overall, the affect heuristic was positively associated with participants' perceived comfort and safety about disclosure on all four SNSs, and the homophily heuristic was positively associated with their perceived comfort and safety about disclosure on three out of four SNSs examined. The relationship between homophily heuristic and participants' perceived comfort and safety about disclosure on Snapchat was marginal, but the p-value may have been impacted by the relatively smaller sample size that was available to study Snapchat users. See Table 23 for full regression results.

Table 23

Cognitive Heuristics and Perceived Comfort and Safety about Disclosure on SNSs

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
Model 1: Control Variables												
Constant	1.89	.58	.00	1.44	.81	.00	.39	1.57	.00	2.77	.69	.00
Age	.00	.01	-.01	.00	.01	-.02	.01	.02	.07	-.01	.01	-.06
Sex	.09	.12	.03	.04	.15	-.01	.45	.29	.15	-.06	.15	-.02
Education Level	.04	.04	.04	.02	.05	.02	.12	.09	.12	.01	.04	.01
Ethnicity	.17	.21	.03	.26	.25	.05	.21	.37	.05	.04	.27	.01
Race	-.03	.14	-.08	-.23	.17	-.07	-.25	.31	-.07	.04	.16	.01
Sexual Orientation	.06	.20	.01	.04	.23	.00	-1.05	.47	-.20*	.26	.23	.05
Religion	-.02	.03	-.02	-.05	.04	-.08	-.08	.07	-.11	-.04	.04	-.05
Political views	.00	.04	.00	.10	.05	.12*	.03	.08	.04	.05	.05	.06
Frequency of SNS Use	.05	.05	.06	.00	.06	.00	-.07	.12	-.08	.00	.06	.00
Number of SNSs Used	.09	.06	.06	.06	.10	.03	.12	.24	.05	.11	.09	.06
Privacy Concern on SNSs	-.27	.05	-.24***	-.19	.06	-.18**	-.23	.10	-.23*	-.27	.05	-.27***
R^2 change		.34			.20			.21			.21	

	Facebook			Instagram			Snapchat			Twitter		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
F for change in R^2		18.81***			7.44***			3.46***			8.23***	
Model 2: Heuristic Effects on Perceived Comfort and Safety about Disclosure on SNSs												
Affect Heuristic	.45	.06	.36***	.56	.08	.40***	.63	.13	.49***	.42	.06	.37***
Bubble Heuristic	-.13	.04	-.14***	-.10	.04	-.13**	.14	.09	.14	-.07	.04	-.10†
Homophily Heuristic	.17	.05	.15***	.21	.06	.21***	.16	.10	.18†	.13	.05	.14*
Bandwagon Heuristic	.08	.06	.08	.05	.07	.05	.02	.11	.02	.01	.06	.02
Hyperbolic Discounting	.19	.05	.20***	.05	.06	.06	.13	.10	.16	.08	.05	.10†
Ephemerality Heuristic	-.08	.04	-.10*	.03	.05	.04	.05	.09	.07	No ephemeral features available on Twitter		
R^2 change		.18			.19			.17			.14	
F for change in R^2		24.64***			14.81***			5.08***			13.61***	
N		356			259			84			277	

Note. ***p <.001. **p < .01. *p < .05. †p < .10.

Facebook

The six predictors explained a significant amount of variance in participants' perceived comfort and safety about disclosure on Facebook. The affect heuristic, homophily heuristic, and hyperbolic discounting were positively associated with participants' perceived comfort and safety about disclosure on Facebook. On the other hand the bubble heuristic and the ephemerality heuristic were negatively associated with this dependent variable, while the bandwagon heuristic was not significantly related to participants' comfort and safety perception.

As expected, the relationships between participants' perceived comfort and safety about disclosure on Facebook and the affect heuristic, bubble heuristic, and ephemerality heuristic are in the opposite direction from those between the same heuristics and participants' perceived risk about disclosure on Facebook. However, it is interesting to note that there are significant positive relationships between participants' perceived comfort and safety about disclosure on Facebook and the homophily heuristic and hyperbolic discounting, while these two heuristics are not significantly related to their perceived risk about disclosure on the same platform. This result suggests that perceived risk and perceived comfort and safety about disclosure are not always inversely related, as first suggested by data from the participants in Study 1.

Instagram

The six predictor variables explained a significant amount of variance in participants' perceived comfort and safety about disclosure on Instagram. Similar to the results on Facebook, perceived comfort and safety about disclosure on Instagram was positively associated with the affect heuristic and homophily heuristic, and it was negatively associated with the bubble heuristic. On the other hand, users' perceived comfort and safety about

disclosure on Instagram was not significantly related to the bandwagon heuristic, hyperbolic discounting, or the ephemerality heuristic.

The relationships between participants' perceived comfort and safety about disclosure on Instagram and the affect and bubble heuristics were in the opposite direction from those between the same heuristics and participants' perceived risk about disclosure on Instagram. However, the homophily heuristic was positively associated with the perceived comfort and safety about disclosure, while it was not significantly associated with the perceived risk about disclosure. Similarly, hyperbolic discounting was positively associated with the perceived risk about disclosure on Instagram, but it was not significantly associated with the perceived comfort and safety about disclosure on the same platform. These results also show that SNS users' perceived comfort and safety about disclosure is not always inversely related to their perceived risk about disclosure.

Snapchat

On Snapchat, the six predictors explained a significant amount of variance in participants' perceived comfort and safety about disclosure. As with two other SNSs, perceived comfort and safety about disclosure was positively associated with the affect heuristic, but it was not significantly related to any other heuristics on Snapchat (bubble heuristic, homophily heuristic, bandwagon heuristic, hyperbolic discounting, and ephemerality heuristic). These results are consistent with the results from the regression analyses on perceived risk about disclosure on Snapchat, as participants' perceived comfort and safety about disclosure was negatively associated with the affect heuristic, but it was not significantly associated with any other heuristics for this SNS platform.

Twitter

On Twitter, the five predictors explained a significant amount of variance in participants' perceived comfort and safety about disclosure. For Twitter, perceived comfort and safety about disclosure was positively associated with the affect heuristic and homophily heuristic, but it was not significantly associated with any other cognitive heuristics (bubble heuristic, bandwagon heuristic, and ephemerality heuristic.

It is interesting to compare this result to the results of the regression analysis on perceived risk about disclosure on Twitter discussed earlier in this chapter. As expected, the affect heuristic was positively associated with perceived comfort and safety about disclosure, while it was negatively associated with the perceived risk about disclosure on Twitter. However, the other cognitive heuristics had different relationships with the perceived comfort and safety than they do with perceived risk about disclosure on Twitter. While the bubble heuristic and hyperbolic discounting were positively associated with perceived risk, they were not significantly related to perceived comfort and safety about disclosure. Similarly, while the homophily heuristic was positively associated with perceived comfort and safety, it was not significantly associated with perceived risk about disclosure. As with the regression results on other SNS platforms, these results about Twitter users also show that people's perceived risk and perceived comfort and safety about disclosure are not necessarily inversely related, and so perhaps should be examined separately in future research.

As described earlier in this chapter, participants' perceived risk may not be very helpful for explaining how SNS users' decisions are influenced by cognitive heuristics. The relationships between cognitive heuristics and participants' perceived risk about disclosure are not consistent with the relationships between cognitive heuristics and their actual disclosure decisions as predicted in the hypotheses. Additional analyses of heuristic effects

on participants' perceived comfort and safety about disclosure on SNSs were conducted to offer an alternative way to assess perceived risk and examine its relationship to cognitive heuristics on SNSs.

The focus group discussions suggested that people are hesitant to talk about risk directly. Indeed, measuring participants' perceived risk by directly asking them to indicate their perception of risk may make people appear or feel more vulnerable, and as such, people might be unwilling to admit such vulnerability in the context of privacy because it makes them look weak or stupid for using SNSs. Thus, measuring users' perceived "comfort" and/or "safety," which are words with more positive connotations, may be more effective in providing additional insights into how SNS users' decisions about disclosure are influenced by cognitive heuristics. The data in Study 2B support this assumption in some ways. For example, the homophily heuristic had positive associations with the amount of disclosure on every SNS (including a marginally positive relationship observed on Snapchat), but it was not significantly related to participants' perceived risk on any SNSs. Table 24 shows that the effect of the homophily heuristic on disclosure decisions may be explained better by participants' perceived comfort and safety about disclosure on SNSs, as this heuristic was positively correlated to users' perceived comfort and safety about disclosure and their reported amount of disclosure on every SNS. This example illustrates not only that people's perceived comfort and safety about disclosure is not always inversely related to their perceived risk about disclosure, as detailed above, but also that perceived comfort and safety might be a better explanatory factor for understanding how SNS users' decisions are influenced by heuristic effects.

Table 24

Relationships between Cognitive Heuristics and (1) the Amount of Disclosure, (2) Perceived Risk about Disclosure, and (3) Perceived Comfort and Safety about Disclosure on SNSs

		Facebook	Instagram	Snapchat	Twitter
Affect Heuristic	Disclosure	Positive	-	-	Positive†
	Risk	Negative	Negative	Negative	Negative
	Comfort/Safety	Positive	Positive	Positive	Positive
Bubble Heuristic	Disclosure	Positive	-	-	-
	Risk	Positive	Positive	-	Positive
	Comfort/Safety	Negative	-	-	Negative†
Homophily Heuristic	Disclosure	Positive	Positive	Positive†	Positive
	Risk	-	-	-	-
	Comfort/Safety	Positive	Positive	Positive†	Positive
Bandwagon Heuristic	Disclosure	Positive	-	-	-
	Risk	-	-	-	-
	Comfort/Safety	-	-	-	-
Hyperbolic Discounting	Disclosure	Positive	Positive	Positive	Positive
	Risk	-	-	-	-
	Comfort/Safety	Positive	-	-	Positive†
Ephemerality Heuristic	Disclosure	Positive	Positive	Positive	n/a
	Risk	Positive	Positive†	Positive†	n/a
	Comfort/Safety	Positive	-	-	n/a

Note. All values indicate the direction of beta coefficients in hierarchical regression analyses reported in Tables 17, 18, 22.

† indicates marginally significant relationships.

Table 24 combines results from analyses of relationships between cognitive heuristics and the amount of disclosure, participants' perceived risk about disclosure, and their perceived comfort and safety about disclosure to (1) present two different approaches taken to understand the underlying mechanism for heuristic processes, and (2) demonstrate that perceived comfort and safety about disclosure is a better explanatory factor than perceived

risk for understanding heuristic effects in the present study. There are several cases where cognitive heuristics' relationships with perceived comfort and safety are consistent with their relationships with amount of disclosure, while these cognitive heuristics' relationships with perceived risk are *not* consistent with SNS users' disclosure decisions. However, cases that demonstrate a reverse or opposite pattern do not exist. In other words, there are no cases where cognitive heuristics' relationships with perceived risk are consistent with their relationships with amount of disclosure when these heuristics' relationships with the perceived comfort and safety are not already aligned with users' disclosure amount. These patterns show that findings about perceived risk mostly confirm or support findings about perceived comfort and safety on SNSs in terms of understanding heuristic effects on users' decisions, but do not add more to understanding heuristic processes. This comparison of the degree of alignment with the predicted heuristic effects on the amount of disclosure seem to add support to the notion that expected benefits have more predictive power than costs (i.e., privacy concerns) when predicting self-disclosure on Facebook (Dienlin & Metzger, 2016). Continued investigation about the role of perceived benefits, rather than costs, would to be valuable for gaining a better understanding of heuristic effects on SNS users' decisions about disclosure and privacy.

Lastly, as shown in Table 24, neither perceived risk nor perceived comfort and safety about disclosure can explain all effects of cognitive heuristics on SNS users' decisions about disclosure. Thus, while measuring perceived comfort and safety adds more insight into understanding heuristic processes compared to measuring perceived risk, it is not enough to understand all heuristic effects. As discussed earlier in this chapter, measuring psychological and subconscious processes that explain heuristic effects is challenging, and thus more

efforts should be invested in finding a reliable way to measure psychological mechanisms underlying heuristic effects in future research.

Chapter 10: Discussion and Conclusion

With three studies, this dissertation presents a mixed-method analysis of the effects of nine cognitive heuristics that are theorized to impact SNS users' privacy-related perceptions and behaviors. Using different approaches helped address the limitations of each methodological approach and resulted in findings that complement each other and provided a more nuanced understanding of how these cognitive heuristics relate to SNS users' privacy-related perceptions and behaviors. This chapter will summarize the findings for each heuristic from the three studies and will discuss both theoretical and practical implications of the findings along with future directions for continued investigation of cognitive heuristics and their possible influence on SNS users' disclosure and privacy decisions.

The Role of Cognitive Heuristics in Understanding Disclosure and Privacy on SNSs

The reasoning for the mixed methodological approach taken in this dissertation is that, because the effect of cognitive heuristics is invisible and largely subconscious, some heuristic effects may be captured better with quantitative data, while others may manifest themselves more clearly in qualitative data. This section will summarize the results across all three studies in this project, for each of the nine heuristics.

Affect Heuristic

Both the qualitative (Study 1) and quantitative findings (Studies 2A and 2B) show that the affect heuristic, which refers to using positive and negative emotions to guide decisions, influences SNS users to perceive less risk and feel safer and more comfortable about disclosure. Yet, at the same time, despite its effect on SNS users' risk perceptions about disclosure, the affect heuristic does not appear to prompt SNS users to actually disclose more information about themselves when using social media platforms. While Study 2B showed that the affect heuristic could lead SNS users to share more information on

Facebook, that was the only platform in which a relationship was found. Moreover, as the affect heuristic is also not significantly related to the amount of disclosure about sensitive topics on SNSs, it may seem like relying on the affect heuristic may not pose much threat to users' privacy on SNSs.

However, it is still important to consider the possibility of indirect effect of the affect heuristic on the amount of disclosure on SNSs. As illustrated by findings from Yu and colleagues (2015), the affect heuristic might indirectly affect people's disclosure decisions, such that it positively influences motivators of disclosure, which then affects actual disclosure on SNSs. Motivators that Yu and colleagues have identified include expression (i.e., relief of psychological distress through self-disclosure), social acceptance, reciprocity, and self-presentation. As explained in the previous chapter, SNS users' perceived risk might not be able to explain the effect of affect heuristic well, but considering the findings by Yu and colleagues, examining the role of users' perceived benefit may be a better way to understand how the affect heuristic impacts users' decision-making processes. As Yu and colleagues studied the effect of affect heuristic on SNSs using a sample of college students in Taiwan, future studies should investigate the role of SNS users' perceived benefit to understand whether and how it influences their decisions about both disclosure and privacy using a larger and more representative sample of SNS users.

Availability Heuristic

Although prior research has examined the effect of past negative privacy experience on people's future SNS use (Debatin et al., 2009; Litt, 2013; Litt & Hargittai, 2014), this dissertation used the concept of the availability heuristic to explain why those past experiences influence SNS users' future decisions. Consistent with prior studies, participants in Study 1 relayed many anecdotes about the effects of their past negative privacy

experiences on their risk perceptions and decisions about disclosure and privacy on SNSs, but this study also provided participants' explanations about how those past experiences influenced their future decisions on SNSs. These explanations were aligned with the logic behind the availability heuristic, as described by Tversky and Kahneman (1974), which is that past experiences can bias people's probability judgment about a particular event based on its familiarity, recency, and/or cognitive salience. In this project, it was observed that participants who were familiar with the possibility of negative privacy-related event—those who had heard of others' experiences with negative privacy-related events that were particularly severe (and thus remained salient in their minds) or had experienced a negative privacy-related event themselves—reported being more aware of privacy risks on SNSs and more cautious about the way they share information or select their privacy settings on SNSs.

Findings from Study 2A are consistent with the qualitative findings from Study 1 and show SNS users' strong agreement with the effect of these negative privacy experiences on their risk perceptions and decisions on SNSs. Although it was studied with a limited sample size, the general pattern in relationships between the availability heuristic and participants' risk perception and disclosure decisions also support the hypotheses about availability heuristic. All three studies in this dissertation illustrate that availability heuristic does play a role in people's decision-making processes about disclosure and privacy.

Results from Study 2B further suggest a possible future direction for continued investigation of the role of availability heuristic in SNS users' decision-making processes about disclosure and privacy. Consistent with Tversky and Kahneman's (1974) explanation about how the availability heuristic influences people's judgments as a function of cognitive salience, results from Study 2B suggests that, in the context of understanding people's decisions about disclosure and privacy on SNSs, the effect of the availability heuristic may

be predicted by the perceived severity of SNS users' negative privacy experiences. Findings from Study 2B about the relationship between perceived severity of past negative privacy experiences and SNS users' risk perceptions and decisions cannot be considered conclusive due to limited sample size that was available in this study. Also, further analyses show that the effect of availability heuristic cannot be properly examined by measuring this heuristic as a dichotomous variable, so researchers should account for the variance in perceived severity of SNS users' negative privacy experiences to better understand this heuristic effect on SNSs.

Optimistic Bias

Despite the evidence of optimistic bias in a variety of domains, including the SNS context (Acquisti & Gross, 2006; Baek et al., 2014; Campbell et al., 2007; Cho et al., 2010; Debatin et al., 2009; Dillard et al., 2006; Helweg-Larsen & Shepperd, 2001; Metzger & Suh, 2017; Radcliffe & Klein, 2002; Shepperd et al., 2003; Wei et al., 2007; Weinstein, 1980), none of the studies in this dissertation project provide evidence for optimistic bias among SNS users, and there was no evidence to support the hypotheses about its possible effects on SNS users' privacy-related risk perceptions or disclosure decisions. In short, neither the qualitative nor the quantitative data in this dissertation produced findings that support the effect of optimistic bias on SNS users' decisions about disclosure in a way that aligns with prior research on the effect of optimistic bias in other risk-related domains. The findings from this project suggest that optimistic bias about privacy risk on SNSs, if it exists, does not influence users to engage in riskier behaviors due to overconfidence. To investigate further, future studies could employ an experimental design to examine causal directions between optimistic bias and SNS users' privacy-related behaviors and assess whether optimistic bias is a result of SNS users' restrictive privacy management strategies rather due to the human cognitive tendency towards self-enhancement.

Bubble Heuristic

Study 1 provided numerous anecdotes about the effects of the bubble heuristic on SNS users, as many participants reported to not only feel safer and more comfortable about sharing information when they have tighter privacy settings or have carefully curated their audience by using more creative strategies like creating "finstas," but also, and likely as a result, share a greater amount of information that includes both mundane and sensitive content. Moreover, participants in Study 2A with a larger and more representative sample of SNS users showed strongest agreement with the effect of bubble heuristic compared to the other heuristics studied.

However, despite these participants' reported agreement that having privacy settings available leads them to feel less risk and share more information on SNSs, these same relationships between the restrictiveness of participants' privacy settings (which was assumed to trigger the bubble heuristic), and SNS users' risk perception and disclosure were not evident in Study 2B. Instead, the restrictiveness of participants' privacy settings on SNSs was positively associated with their perceived risk on three out of four SNSs, and it was negatively associated with the amount of their disclosure on Facebook. These mixed findings about the bubble heuristic across the three studies might be a result of the measurement approach taken in Study 2B. A sense of security that comes from an online enclosure (e.g., using SNSs with privacy settings) may not be readily apparent to SNS users unless they see statements like the ones in Study 2A that clearly describe the effect of the bubble heuristic reflected in their privacy settings.

If this explanation is correct, it is important to increase SNS users' awareness of their susceptibility to the bubble heuristic, as it seems to lead them to perceive less risk and share more information on SNSs (at least on Facebook), thereby exposing them to more privacy

risk. Research investigating ways to design and implement "privacy nudges" might be useful to find solutions to help users become more mindful of their susceptibility to the bubble heuristic (or other heuristics too). Nudges refer to small, simple changes in the decision environment to lead people to make more optimal decisions without restricting their freedom too much (Thaler & Sunstein, 2008). An example of *privacy nudges* are short messages that appear on-screen to remind users to adjust their privacy settings. They are considered a soft paternalistic approach to make users become more aware of privacy risks and guide them to make more informed choices about their privacy management (Acquisti, 2012; Acquisti et al., 2017; Dogruel, 2019; Solove, 2013). In general, educative nudges (e.g., disclosure requirements, reminders, warnings, etc.) can increase people's knowledge and help them become more aware of their decision environment (Sunstein, 2016).

Privacy nudges can help people become less susceptible to relying on cognitive heuristics that are associated with negative consequences and address the issue of information asymmetry when people make decisions about privacy (Acquisti et al., 2017). In the context of managing SNS users' susceptibility to the bubble heuristic, refining information-based nudges (e.g., a picture of few randomly selected users that can see one's post and an additional text, such as "X, Y, Z, and 500 others can see this post") would be useful for reminding people about the size and composition of their audience (Schöbel, Barev, Janson, Hupfeld, & Leimeister, 2020). Future research could also explore the effectiveness and viability of developing privacy nudges that also inform people about the invisible audience (e.g., marketers, advertisers, government officials, etc.), as well as other heuristics.

Homophily Heuristic

Both qualitative and quantitative data provide strong support for the hypothesized effects of the homophily heuristic on SNS users' risk perceptions and disclosure decisions. Many focus group participants in the first study expressed how they feel less comfortable and refrain from sharing information when they feel dissimilar to their friends and/or followers, which is consistent with the homophily heuristic. Moreover, participants in the second study reported significant agreement with statements about how their perceived similarity or dissimilarity to their social network connections affected their perceived risk and amount of disclosure on SNSs in ways that are consistent with predictions based on the homophily heuristic. In addition, the third study found that perceived similarity to one's social media contacts was positively associated with the amount of information that person disclosed on three out of four SNSs examined—and had a marginally significant positive relationship with the disclosure on the fourth. Moreover, perceived homophily was also significantly associated with the amount of disclosure about sensitive topics on Facebook and Twitter, suggesting that SNS users should be wary of their susceptibility to this heuristic effect. Increasing disclosure about both sensitive and general topics based on perceived similarity to SNS users' visible audience (e.g., friends and/or followers) might lead them to neglect or deter them from thinking about the flow of their information to invisible audiences (e.g., advertisers, marketers, government officials, etc.) and expose them to unknown or unpredictable privacy risks (Stutzman et al., 2013).

As explained in the previous chapter, results from Study 2B also illuminate an underlying mechanism that could explain the effect of the homophily heuristic on SNSs user behavior. While the homophily heuristic was not related to participants' perceived risk about disclosure on any of the SNSs, its relationship to participants' perceived comfort and safety about disclosure mirrored the results about its relationship to the amount of disclosure on

SNSs. In other words, the homophily heuristic was positively associated with participants' perceived comfort and safety about disclosure on Facebook, Instagram, and Twitter, and it had a marginally significant positive relationship with the perceived comfort and safety about disclosure on Snapchat. These results show that the homophily heuristic, reflected in people's perceived similarity to their social network connections, may be raising people's perceived comfort and safety about disclosure (instead of decreasing their perceived risk), thereby leading them to share more information. Given these results about the effect of homophily heuristic on SNS users' attitudes and decisions about disclosure, future research could employ mediational analyses to gain a deeper understanding about the process by which the homophily heuristic influences SNS users' disclosure.

Bandwagon Heuristic

Study 1 provided numerous anecdotes about the effect of the bandwagon heuristic on SNS users' decision-making processes about disclosure and privacy. Participants in the focus group interviews reported feeling more comfortable about posting specific content (e.g., holiday photos, social media trends, etc.) or using specific features (e.g., polls, stickers, privacy settings, etc.) when they see others doing the same. However, the results from Study 2A revealed that these anecdotes likely illustrate the experience of only younger SNS users, who comprised the sample for the first study. When controlling for age, among other demographic variables, in the hierarchical regression analyses conducted in Study 2B, the bandwagon heuristic was positively associated with amount of disclosure on Facebook, but not on other SNSs. Also, it was not significantly related to any of the attitudinal measures (e.g., perceived risk and perceived comfort and safety about disclosure) on any of the SNSs.

While prior literature and thematic analyses of the focus group interview transcripts suggested that the level of users' attention to others' sharing behaviors on SNSs could trigger

the bandwagon heuristic, the findings concerning the bandwagon heuristic in Study 2B indicate that future research may need to employ a more specific measure to test the effect of this heuristic. Spottswood and Hancock (2017) found evidence of the effect of bandwagon heuristic in their experiment that manipulated the bandwagon heuristic through an explicit cue that showed the proportion of users who had shared their email address in a fictitious SNS to test whether that cue would lead participants to share their email address as well. Thus, researchers should identify an explicit and specific cue on existing SNSs if they hope to find additional evidence to support the bandwagon heuristic's effects on SNS users' decisions about disclosure and privacy outside of an experimental setting.

Inequity Aversion

Like optimistic bias, inequity aversion, which is people's tendency to resist unfair outcomes, is also a robust phenomenon that influences people's behaviors in various domains that involve social comparison (Acquisti & Grossklags, 2007; Fehr & Schmidt, 1999). Moreover, some prior research about SNSs suggests that inequity aversion may play a role in SNS users' decision-making processes (Acquisti & Grossklags, 2007; Buglass et al., 2017; Przybylski et al., 2013). However, the studies in this dissertation project did not provide evidence to suggest that inequity aversion influences SNS users' risk perceptions or disclosure. Both in the focus group interviews and the survey-based studies, participants reported that they do not feel much inequity aversion in their SNS use, and do not believe that inequity aversion influences their risk perceptions or behaviors. As discussed in Chapters 4 and 7, it is possible that the hypothesized behavioral consequences of inequity aversion (e.g., sharing content to get as much social benefit as other users on SNSs) are too similar to the effect of bandwagon heuristic on SNS users' disclosure decisions to distinguish the effect of two cognitive heuristics. Despite the lack of findings for inequity aversion in this

dissertation project, media coverage and popular accounts about the competitive nature of information sharing on SNSs (see Herman, 2019; Rodriguez, 2019) may warrant further examination of the role of inequity aversion in SNS users' decision-making processes. It is possible that effects of inequity aversion could be captured through another methodological approach, or that the effect of inequity aversion is limited to only a specific segment of SNS users (e.g., those involved with influencer marketing efforts on SNSs).

Hyperbolic Discounting

Hyperbolic discounting describes people's tendency to place greater weight on proximate benefits while discounting distal risks. In the context of SNSs, hyperbolic discounting about privacy risks refers to users sharing information for immediate gratification despite their awareness of temporally distant risks. Most likely due to social desirability biases, few focus group participants in Study 1 admitted that hyperbolic discounting affected their privacy decision making on SNSs, although several shared experiences of making rash decisions while they were intoxicated, perhaps to lift the possible shame associated with making regrettable decisions. And despite social desirability pressures, some participants in Study 1 shared anecdotes about strong or intense emotions leading them make impulsive decisions to disclose despite being aware of the privacy risk associated with sharing those posts. These anecdotes were useful for creating measures for hyperbolic discounting for the subsequent survey studies, which were less susceptible to social desirability biases. Still, in Study 2A overall, participants did not show much agreement with statements that described the effect of hyperbolic discounting on their privacy decision making. However, when measuring the effect of hyperbolic discounting by examining the correlational relationships between participants' tendency to make impulsive decisions and their risk perceptions and decisions about disclosure on SNSs in Study 2B,

findings supported the hypothesized behavioral implications of hyperbolic discounting on SNSs. In sum, Study 2B showed that hyperbolic discounting, as reflected in participants' tendency to act on an impulse and/or regret their decision as a result, was positively associated with the amount they disclose about both general topics and sensitive topics on all four SNSs.

Interestingly, however, hyperbolic discounting was positively associated with participants' perceived risk about disclosure on a few of the SNSs (Instagram and Twitter), and at the same time, it was also positively associated with their perceived comfort and safety on Facebook (and had a marginally significant positive relationship with the perceived comfort and safety about disclosure on Twitter). These findings make it difficult to understand how hyperbolic discounting influences users' disclosure decisions on SNSs, as it seems to paradoxically raise both users' perceived risk as well as their perceived comfort and safety. These findings highlight the complexity of studying the effect of cognitive heuristics, which are invisible and subconscious. The current findings about the relationships between hyperbolic discounting and SNS users' risk perception and disclosure decisions might suggest that heuristics effect SNS users incredibly quickly, and that they might lead SNS users to act in a way that does not properly align with their risk perceptions because they influence behavior before SNS users can engage in any kind of rational risk analysis.

Ephemerality Heuristic

Evidence for the ephemerality heuristic was observed in both the qualitative and quantitative data. In Study 1, focus group participants were able to provide anecdotes that clearly differentiate how making decisions by relying on this heuristic (e.g., using Stories), is different from deciding to share information in a more careful manner (e.g., sharing permanent posts). Similarly, participants in Study 2A reported agreement with statements

describing the effect of the ephemerality heuristic, while Study 2B showed that the frequency of using ephemeral features is positively associated with the amount of SNS users' disclosure on all of the SNSs that offer ephemeral features. Also, using ephemeral features was positively associated with the amount of disclosure about sensitive topics on Facebook and Instagram, and it had a marginally significant positive relationship with the amount of disclosure about sensitive topics on Snapchat. The findings from Study 2B about the relationships between ephemerality heuristic and disclosure decisions across the SNSs studied illustrate that ephemerality heuristic has a consistent positive influence on how much information SNS users share.

Again, though, and similar to findings about hyperbolic discounting, the ephemerality heuristic does not align well with participants' risk perceptions about disclosure. In contrast to what was hypothesized, the ephemerality heuristic was positively associated with perceived risk about disclosure and negatively associated with perceived comfort and safety about disclosure on Facebook, and it was not significantly associated with these attitudinal measures on any other SNSs. These findings add more support to the idea that heuristic effects are perhaps too quick to influence risk perceptions to inform people's disclosure decisions, and thus should not be evaluated the same way rational decisions are understood. While popular theoretical approaches, such as the privacy calculus model, lead researchers to view SNS users' decisions as a result of risk-benefit analysis, decisions relying on cognitive heuristics may involve a different process and/or underlying mechanism that should be investigated further in future research.

Theoretical and Practical Implications and Future Directions

This dissertation project began with the goal of understanding the effects of cognitive heuristics on SNS users' privacy decisions. If empirical evidence is found that heuristics

guide such decisions, this would suggest that people's decision-making processes about privacy in SNSs are not fully rational, contrary to the assumptions of the privacy calculus model, which is one of the very few theoretical frameworks that have been advanced to explain SNS users' privacy behaviors. As discussed in the early chapters of this dissertation, such evidence was found for several of the cognitive heuristics that were tested in the three studies. While such empirical findings of the effects of cognitive heuristics on SNS users' decisions about disclosure and privacy do not necessarily "disprove" the privacy calculus model, they illuminate that researchers should consider the impact of less rational processes operating to affect SNS users' decision-making processes, in addition to the role of rational risk-benefit analyses. The results of this dissertation project support Acquisti and colleagues' (2015) assertion that assuming SNS users' decision-making processes can be both rational (as implied in many classic economic theories) and not fully rational can offer a better understanding of their behaviors that do not seem to align with their reported risk perceptions and concerns (i.e., the privacy paradox) (Barnes, 2006; Norberg, Horne, & Horne, 2007). The privacy paradox is exemplified in SNS users' disclosure even when they feel the risks are high (Dienlin & Metzger, 2016; Taddicken, 2014).

As highlighted by the increasing number of large-scale privacy scandals on SNSs in recent years, users continue to experience privacy breaches and violations despite many SNS platforms' efforts to be more transparent about their data use policies and to offer more privacy settings to give users greater control over their information. Findings from this dissertation suggest that SNS users' continued experience of negative privacy-related events may be partially explained by their reliance on cognitive heuristics because they are not capable of performing a thorough privacy calculus to correctly estimate the net benefit associated with every instance of disclosure on SNSs. While some scholars may argue that

relying on cognitive heuristics is efficient, and that it can even be effective for making quick decisions (Gigerenzer et al., 1999), some findings from this project seem to show that relying on cognitive heuristics on SNSs, which is a uniquely complex communication environment, has negative implications for users' privacy management. For this reason, it is critical for researchers to expand their assumptions about the level of rationality in SNS users' privacy decision making and to continue to investigate the role of cognitive heuristics with the ultimate goal of helping SNS users make more informed decisions without falling prey to disclosure and/or privacy heuristics that have negative repercussions for their privacy when using SNSs. Although this project identified several cognitive heuristics that appear to influence SNS users' decisions about disclosure and privacy, a continued research effort is needed to establish a more comprehensive list of disclosure and privacy heuristics and improve people's awareness and understanding of their possible effects on their decision-making processes.

As mentioned earlier, research on privacy nudges may help people make more informed decisions about disclosure and privacy by raising their awareness about privacy risks in their specific decision environment (e.g., specific SNSs). As tools to help people deal with the "hurdles" in privacy decision making (e.g., cognitive biases, bounded rationality, information asymmetry, incomplete information, etc.), privacy nudges can help users by increasing knowledge, visually highlighting relevant user interfaces to reduce cognitive load, providing more privacy-protecting default settings, delaying the timing of users' decisions, etc. (see Acquisti et al., 2017 for an overview of recent research on privacy nudges in computer science, usability, persuasive technoloiges, and behavioral decisions).

Because the way cognitive heuristics operate in people's minds are invisible and subconscious, a mixed methods approach is useful to study how cognitive heuristics

influence SNS users' decision-making processes, as triangulation across methods helps instill greater confidence in phenomenon like cognitive heuristics that are elusive to direct observation. As described earlier in this chapter, some heuristic effects are better captured using qualitative methods, while others are better measured with a quantitative approach. Stated otherwise, understanding heuristics benefits from using both qualitative and quantitative methods that could lead to complementary findings.

Moreover, when using multiple methodological approaches, it is important to understand how these approaches lead to results that complement each other, but also why results from each approach may be distinct from one another. Carefully examining how results may be determined by each method and then comparing the results across studies could help explain seemingly conflicting results about cognitive heuristics in this dissertation. For example, many participants in Study 1 shared numerous anecdotes about how they felt more comfortable about sharing specific types of contents (e.g., holiday photos) on SNSs when they noticed that others were posting similar types of content. However, in Study 2A, results showed little agreement with the effect of bandwagon heuristic on sharing specific type of content. Thus, these results appear to contradict each other. To understand the discrepancy, it is important to consider the specific goal of each method in terms of addressing the research questions. The aim of the focus group interviews conducted for Study was to find whether there is *any* evidence of cognitive heuristics' influence on people's SNS use. As such, *any* mention of cognitive heuristics was counted as evidence of heuristic processing. On the other hand, the goal of Study 2A was to test the extent of agreement with the effects of cognitive heuristics on SNS users' decisions about disclosure and privacy in a broader sample, and thus results will only appear as significant if there is relatively wide-scale agreement with each heuristic effect. Therefore, the results about the effect of the

bandwagon heuristic in Study 2A showing low agreement does not mean the bandwagon heuristic does not influence this type of decision at all. As shown by qualitative data in Study 1, the bandwagon heuristic does and can influence some SNS users, but not *most* users.

As another example, it may be the case that the availability heuristic affects people's disclosure and privacy decisions, but only for a small subsample of people who have had a negative privacy experience. If the entire sample is included in the analysis, then any significant relationships would be washed out by the nonsignificant relationships between the variables amongst the majority of participants who have *not* experienced a negative privacy event in the past. In any case, these examples show that the conflicting results of Study 1 and 2A do not necessarily weaken the argument that heuristics may play an important role when SNS users decide what to disclose and how to protect their privacy when using social media platforms.

The complexity of studying heuristic effects is challenging, and while this project took multiple methodological approaches to gain an in-depth understanding about the role of nine cognitive heuristics, there were some methodological challenges (explained earlier) that should be rectified in future research. The current project would have benefitted from larger and more representative samples and perhaps more specific measurement approaches to studying cognitive heuristics. But most importantly, due to a lack of clear findings about the underlying mechanism to explain how cognitive heuristics influence SNS users' decisions (i.e., risk and comfort/safety perceptions), it is difficult to view the current findings as conclusive or to confidently claim that users' decisions are indeed *caused* by each specific cognitive heuristic examined in this project. Because cognitive heuristics can be triggered by extremely simple and seemingly inconsequential cues (e.g., a smiley face can trigger the affect heuristic, and in the studies presented in this dissertation, the affect heuristic was

observed to be associated with increased disclosure on some SNSs), in a context that contains thousands of potential cues, SNS users can be influenced by multiple heuristics at once. For example, a user's increased disclosure about sensitive topics on Stories (an ephemeral feature) may be a result of ephemerality heuristic, but it is difficult to rule out other cognitive heuristics as possible contributing factors to this user's disclosure decisions. In this case, this user may have felt comfortable sharing information because he or she was sharing using Stories as opposed to permanent parts of the profile. But at the same time, this user may have also discounted the distal risk to gain immediate responses from his or her friends and followers to a Story that shows him or her engaging in a cool or fun activity (i.e., hyperbolic discounting). If this were the case, this user's decision would be a result of both ephemerality heuristic and hyperbolic discounting, but it is difficult to detangle the effects of these two heuristics or account for their interaction effects.

Understanding and distinguishing different heuristics and their effects, and identifying the cues that trigger specific heuristics, could be helpful for finding technological solutions for reducing any negative consequences associated with relying on those heuristics (e.g., removing those cues). Therefore, future research should consider employing experimental designs that manipulate possible heuristic cues in the user interface to understand their relationships to specific cognitive heuristics and/or their behavioral consequences on SNSs. As demonstrated by findings from Kehr and colleagues (2015), a simple smiley face is enough to trigger the affect heuristic. Using this logic, future research could explore manipulating heuristic cues associated with cognitive heuristics that were found to be associated with negative consequences in this dissertation. For example, these studies could test the effect of having a timer on the screen to indicate the post's ephemerality to test the effect of ephemerality heuristic on users' disclosure amount, or the

effect of seeing an expected number of likes (which would highlight immediate gratification) on the pre-posting screen to test the effect of hyperbolic discounting on users' disclosure decisions. Future research that uncovers the effect of visual heuristic cues like the ones described here using experimental research designs would deepen the understanding of heuristics effects on SNSs, offer grounds to understand causality, and also inform research on privacy nudges since it could be used to help determine the most effective nudges to discourage people from relying on cognitive heuristics that are associated with negative consequences for their privacy on SNSs.

In general, then, while the findings from this dissertation answer the question of *whether,* and to some degree, *to what extent* cognitive heuristics influence SNS users' decisions about disclosure and privacy, more research is needed to investigate and understand *how* and *in what combinations* these heuristics influence users' decisions. This effort will be crucial for finding solutions to help people become less susceptible to cognitive heuristics and make more informed decisions that they are less likely to regret or put them at risk.

Overall, this project advances scholars' growing discussion about how people's privacy-related decisions in online contexts are influenced by cognitive heuristics (Acquisti, 2012; Acquisti et al., 2015; Acquisti & Grossklags, 2004, 2005; Carey & Burkell, 2009; Gambino et al., 2016; Kim et al., 2018; Sundar et al., 2016, 2019). It also contributes to the literature by offering empirical evidence of cognitive heuristic effects on disclosure and privacy-related decisions in the specific context of SNSs. Indeed, the studies in this project may be one of the first studies to have empirically tested the effect of hyperbolic discounting on people's privacy-related decisions online, which has been long discussed as a possibility since it was initially hypothesized by Acquisti and Grossklags in 2004. This dissertation not

only employed multiple methodological approaches, but it made further efforts to gain a more contextualized and in-depth understanding of the effects of heuristics by studying more than one SNS platform, and thus avoids making claims about SNS users' behaviors that are limited to only one SNS platform. The findings from this project should serve as a strong basis for future research to continue investigating the role of cognitive heuristics as they relate to disclosure and privacy-related decisions on SNSs. This line of research not only challenges scholars' popular and widely-accepted assumptions about human rationality to expand their theoretical framework, but it could also help reduce the likelihood that people experience negative privacy-related events on SNSs that cause them to feel powerless in a dynamically complex communication environment and empower SNS users to make more informed decisions.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on Electronic Commerce*, 21-29. https://doi.org/10.1145/988772.988777

Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. In J. Bus, M. Crompton, M. Hilderbrandt, & G. Metakides (Eds.), *Digital enlightenment yearbook 2012* (pp. 193-197). IOS Press. https://doi.org/10.3233/978-1-61499-057-4-193

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys, 50*(3), 1-41. https://doi.org/10.1145/3054926

Acquisti, A., Brandimarte, L., & Lowenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(409), 509–514.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *PET 2006: Privacy enhancing technologies* (pp. 36–58). Springer.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In L. J. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 1–15). Springer. https://doi.org/10.1007/1-4020-8090-5_13

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. De Capitani di Vimercati

(Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 363–379). Auerbach Publications.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215

Ainslie, G., & Monterosso, J. (2003). Hyperbolic discounting as a factor in addiction. A critical analysis. In R. E. Vuchinich & N. Heather (Eds.), *Choice, behavioural economics and addiction* (pp. 35-69). https://doi.org/10.1016/B978-008044056-9/50043-9

Alhakami, A. S., & Slovic, P. (1994). A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis*, *14*(6), 1085–1096. https://doi.org/10.1111/j.1539-6924.1994.tb00080.x

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company.

Anderson, M., & Quinn, D. (2019, August 8). *46% of U.S. social media users say they are "worn out" by political posts and discussions*. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/08/08/46-of-u-s-social-media-users-say-they-are-worn-out-by-political-posts-and-discussions/

Asch, S. E. (1951). Effects of group pressure upon the modification and distortion of judgments. In H. Guetzkow (Ed.), *Groups, leadership and men; research in human relations* (pp. 177–190). Carnegie Press.

Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological Monographs: General and Applied*, *70*(9), 1–70. https://doi.org/10.1037/h0093718

Baddeley, M. (2011, June 14-15). Information secruity: Lessons from behavioural economics [Paper presentation]. The 10th Workshop on the Economics of Information Security, Fairfax, VA, United States.

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56. https://doi.org/10.1016/j.chb.2013.10.010

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Barrett, B. (2018, December 14). *Facebook exposed 6.8 million users' photos to cap off a terrible 2018.* WIRED. https://www.wired.com/story/facebook-photo-api-bug-millions-users-exposed/

BBC News. (2018, March 21). *Facebook data row: Cambridge Analytica academic a "scapegoat."* BBC. https://www.bbc.com/news/uk-43480978

Bellur, S., & Sundar, S. S. (2014). How can we tell when a heuristic has been used? Design and analysis strategies for capturing the operation of heuristics. *Communication Methods and Measures*, *8*(2), 116–137. https://doi.org/10.1080/19312458.2014.903390

Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the invisible audience in social networks. *Proceedings of the 2013 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI'13)*, 21-30. https://doi.org/10.1145/2470654.247065

boyd, d. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and cuture on social network sites* (pp. 39–58). Routledge.

boyd, d. (2014). *It's complicated: The social lives of networked teens* (1st ed.). Yale

University Press.

Bracetti, A. (2012, May 10). *25 Facebook posts that have gotten people fired*. Complex. https://www.complex.com/pop-culture/2012/05/25-facebook-posts-that-have-gotten-people-fired/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. https://doi.org/10.1111/j.1460-2466.1978.tb01621.x

Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. M. (2017). Motivators of online vulnerability: The impact of social network site use and FOMO. *Computers in Human Behavior*, *66*, 248–255. https://doi.org/10.1016/j.chb.2016.09.055

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273–1284. https://doi.org/10.1016/j.chb.2004.12.005

Carey, R., & Burkell, J. (2009). A heuristics approach to understanding privacy-protecting behaviors in digital social environments. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 65–82). Oxford University Press.

Chaiken, S. (1987). The heuristic model of persuasion. In M. P. Zanna, J. M. Olson, & C. P. Herman (Eds.), *Social influence: The Ontario symposium* (pp. 3–39). Lawrence Erlbaum Associates, Inc.

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*, 1859–1872.

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC

relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21–40). Peter Lang.

Child, J. T., Petronio, S., Agyeman-Budu, E. A., & Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior*, *27*(5), 2017–2027. https://doi.org/10.1016/j.chb.2011.05.009

Cho, H., & Filippova, A. (2016). Networked privacy management in Facebook: A mixed-methods and multinational study. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW '16)*, 503–514. https://doi.org/10.1145/2818048.2819996

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Clark, A. E., & Oswald, A. J. (1996). Satisfaction and comparison income. *Journal of Public Economics*, *61*(3), 359–381. https://doi.org/10.1016/0047-2727(95)01564-7

Cohen, D. (2018, June 5). *Infographic: What happens on the internet in a single minute*. AdWeek. https://www.adweek.com/digital/infographic-what-happens-on-the-internet-in-a-single-minute/

Collins, N. L., & Miller, L. C. (1994). Self-Disclosure and liking : A meta-analytic review. *Psychological Bulletin*, *116*(3), 457–475. https://doi.org/10.1037/0033-2909.116.3.457

Cook, K. S., & Rice, E. (2003). Social exchange theory. In J. Delamater (Ed.), *Handbook of Social Psychology* (pp. 53–76). https://doi.org/10.1007/978-94-007-6772-0

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

https://doi.org/10.1287/orsc.10.1.104

Culnan, M. J., & Bies, J. R. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342. https://doi.org/10.1111/1540-4560.00067

Dance, G. J. X., La Forgia, M., & Confessore, N. (2018, December 30). *As Facebook raised a privacy well, it carved an opening for giant techs*. The New York Times. https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html

Davies, H. (2015, December 11). *Ted Cruz using firm that harvested data on millions of unwitting Facebook users.* The Guardian. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Devenow, A., & Welch, I. (1996). Rational herding in financial economics. *European Economic Review*, *40*(3–5), 603–615. https://doi.org/10.1016/0014-2921(95)00073-9

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dillard, A. J., McCaul, K. D., & Klein, W. M. P. (2006). Unrealistic optimism in smokers: implications for smoking myth endorsement and self-protective motivation. *Journal of Health Communication*, *11*(S1), 93–102. https://doi.org/10.1080/10810730600637343

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce

transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.l060.0080

Dogruel, L. (2019). Privacy nudges as policy interventions: Comparing US and German media users' evaluation of information privacy nudges. *Information Communication and Society*, *22*(8), 1080–1095. https://doi.org/10.1080/1369118X.2017.1403642

Ellison, N., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy Online* (pp. 19–32). https://doi.org/10.1007/978-3-642-21521-6

Fehr, E., & Schmidt, K. M. (1999). A theory of fairness, competition, and cooperation. *The Quarterly Journal of Economics*, *114*(3), 817–868. https://www.jstor.org/stable/2586885

Fiandt, K., Pullen, C., & Walker, S. (1999). Actual and perceived risk for chronic illness in rural older women. *Clinical Excellence for Nurse Practitioners*, *3*(2), 105–115. https://www.ncbi.nlm.nih.gov/pubmed/10646399

Fischoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, *9*(2), 127–152. https://doi.org/10.1007/BF00143739

Gambino, A., Kim, J., Sundar, S. S., Ge, J., & Rosson, M. B. (2016). User disbelief in privacy paradox: Heuristics that determine disclosure. *Proceedings of the 2016 CHI Conference Etxtended Abstracts on Human Factors in Computing Systems*, 2837–2843. https://doi.org/10.1145/2851581.2892413

Gao, X., Yang, Y., Fu, H., Lindqvist, J., & Wang, Y. (2014). Private browsing: An inquiry on usability and privacy protection. *Proceedings of the 13th Workshop on Privacy in the*

Electronic Society, 97–106. https://doi.org/10.1145/2665943.2665953

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. *Annual Review of Psychology*, *62*, 451–482. https://doi.org/10.1146/annurev-psych-120709-145346

Gigerenzer, G., Todd, P. M., & The ABC Research Group (1999). *Simple heuristics that make us smart*. Oxford University Press.

Guest, G., MacQueen, K., & Namey, E. (2014). Planning and preparing the analysis. *Applied Thematic Analysis* (pp. 21-48). SAGE. https://doi.org/10.4135/9781483384436.n2

Halper, K. (2015, July 13). *A brief history of people getting fired for social media stupidity.* The Rolling Stone. https://www.rollingstone.com/culture/culture-lists/a-brief-history-of-people-getting-fired-for-social-media-stupidity-73456/

Harding, X. (2018, March 22). *"Who cares, I have nothing to hide" - Why the popular response to onine privcy is so flawed.* Mic. https://www.mic.com/articles/188563/who-cares-i-have-nothing-to-hide-why-the-popular-response-to-online-privacy-is-so-flawed

Heider, F. (1946). Attitudes and cognitive organization. *Journal of Psychology*, *21*(1), 107–112. https://doi.org/10.1080/00223980.1946.9917275

Helweg-Larsen, M., & Shepperd, J. A. (2001). Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Review*, *5*(1), 74–95. https://doi.org/10.1207/S15327957PSPR0501_5

Herman, J. (2019, May 31). *What if Instagram got rid of likes?* The New York Times. https://www.nytimes.com/2019/05/31/style/are-likes-and-followers-the-problem-with-social-media.html

Hitlin, P., & Rainie, L. (2019). *Facebook Algorithms and Personal Data*. Pew Research Center. http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/

Homans, G. C. (1961). *Social behavior: Its elementary forms.* Harcourt, Brace & World.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. https://doi.org/10.1080/15252019.2010.10722168

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud!: Privacy concerns for consumer cloud storage. *Proceedings of the 7th Symposium on Usable Privacy and Security*, 13-20. https://doi.org/10.1145/2078827.2078845

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, *58*(9), 697–720. https://doi.org/10.1037/0003-066X.58.9.697

Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment* (pp. 49–81). https://doi.org/10.1017/cbo9780511808098.004

Kang, C., & Frenkel, S. (2018, April 4). *Facebook says Cambridge Analytical harvested data of up to 87 million users*. The New York Times. https://nyti.ms/2EjnUyB

Karjanen, D. (2010). The crash of 2008 and what it means: The new paradigm for financial markets. *Contemporary Sociology: A Journal of Reviews*, *39*(6), 744–746. https://doi.org/10.1177/0094306110386886ss

Kehr, F., Kowatsch, T., Wentzel, D., & 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), 607–635. https://doi.org/10.1111/isj.12062

Kim, J., Gambino, A., Sundar, S. S., Rosson, M. B., Aritajati, C., Ge, J., & Fanning, C. (2018). Interface cues to promote disclosure and build community: An experimental test of crowd and connectivity cues in an online sexual health forum. *Proceedings of the ACM on Human-Computer Interaction*. https://doi.org/10.1145/3274359

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). “When I am on wi-fi, I am fearless”: Privacy concerns & practices in everyday wi-fi use. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1993–2002. https://doi.org/10.1145/1518701.1519004

Klausner, A. (2018, October 31). *Nurse fired for blackface Beyoncé costume.* New York Post. https://nypost.com/2018/10/31/nurse-fired-for-blackface-beyonce-costume/

Knobloch-Westerwick, S., Sharma, N., Hansen, D. L., & Alter, S. (2005). Impact of popularity indications on readers’ selective exposure to online news. *Journal of Broadcasting & Electronic Media*, *49*(3), 296-313. https://doi.org/10.1207/s15506878jobem4903_3

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kossinets, G., & Watts, D. J. (2009). Origins of homophily in an evolving social network. *American Journal of Sociology*, *115*(2), 405–450. https://doi.org/10.1086/599247

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/ *10.1057/JIT.2010.6*

Krasnova, H., Veltri, N. F., & 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), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Laibson, D. (1997). Golden Eggs and Hyperbolic Discounting. *The Quarterly Journal of Economics*, *112*(2), 443–478. https://doi.org/10.1162/003355397555253

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lazarsfeld, P. F., & Merton, R. K. (1964). Friendship as social process: A substantive and methodological analysis. In M. Berger, T. Abel, & C. H. Page (Eds.), *Freedom and control in modern society*. Van Nostrand.

Lee, J. Y., & Sundar, S. S. (2013). To tweet or to retweet? That is the question for health professionals on twitter. *Health Communication*, *28*(5), 509–524. https://doi.org/10.1080/10410236.2012.700391

Lewin, K. (1947). Frontiers in group dynmaics: II. Channels of group life, social planning and action research. *Human Relations*, *1*(2), 143–153. https://doi.org/10.1177/001872674700100201

Lewin, K. (1948). *Resolving social conflicts: Selected papers on group dynamics [1935-1946]*. Harper & Row.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, *14*(1), 79–100. https://doi.org/10.1111/j.1083-6101.2008.01432.x

Li, H., Sarathy, R., & 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), 434–445. https://doi.org/10.1016/j.dss.2011.01.017

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, *29*(4), 1649–1656. https://doi.org/10.1016/j.chb.2013.01.049

Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior*, *36*, 520–529. https://doi.org/10.1016/j.chb.2014.04.027

Loewenstein, G. F., Thompson, L., & Bazerman, M. H. (1989). Social utility and decision making in interpersonal contexts. *Journal of Personality and Social Psychology*, *57*(3), 426–441. https://doi.org/10.1037/0022-3514.57.3.426

Madden, M. (2012). *Privacy management on social media sites*. Pew Research Center. https://www.pewresearch.org/internet/2012/02/24/privacy-management-on-social-media-sites/

Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Madden, M., Rainie, L., Zickuhr, K., Duggan, M., & Smith, A. (2014). *Public perceptions of privacy and security in the post-Snowden era*. Pew Research Center. https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.l040.0032

Manjoo, F. (2019, April). *It's time to panic about privacy*. The New York Times. https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html

Marwick, A., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context

collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Marwick, A., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

McCroskey, J. C., Richmond, V. P., & Daly, J. A. (1975). The development of a measure of perceived homophily in interpersonal communication. *Human Communication Research 1*(4), 323-332. https://doi.org/10.1111/j.1468-2958.1975.tb00281.x

McGuire, W. J. (1968). Theory of the structure of human thought. In R. P. Abelson, A. Eliot, W. J. McGuire, T. M. Newcomb, M. J. Rosenberg, & P. H. Tannenbaum (Eds.), *Theories of cognitive consistency; a sourcebook* (pp. 140–162). Rand McNally.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology*, *27*(1), 415–444. https://doi.org/10.1146/annurev.soc.27.1.415

Menand, L. (2018, June 18). *Why do we care so much about privacy?* The New Yorker. https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy

Metzger, M. J., & Suh, J. J. (2017). Comparative optimism about privacy risks on Facebook. *Journal of Communication*, *67*(2), 203–232. https://doi.org/10.1111/jcom.12290

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, *66*(4), 839–857. https://doi.org/10.1002/asi

Neubaum, G., & Krämer, N. C. (2017). Monitoring the opinion of the crowd: Psychological

mechanisms underlying public opinion perceptions on social media. *Media Psychology*, *20*(3), 502–531. https://doi.org/10.1080/15213269.2016.1211539

Newell, A., & Simon, H. A. (1972). *Human problem solving*. Prentice-Hall.

Nisbett, R. E., & Wilson, T. D. (1977). Telling more than we can know: Verbal reports on mental processes. *Psychological Review*, *84*(3), 231–259. https://doi.org/10.1037/0033-295X.84.3.231

Noelle-Neumann, E. (1984). *The spiral of silence: Public opinion, our social skin*. University of Chicago Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Notopoulos, K. (2019, April 10). *Facebook Showed Me My Data Is Everywhere And I Have Absolutely No Control Over It.* BuzzFeed News. https://www.buzzfeednews.com/article/katienotopoulos/facebook-advertisers-data-brokers-car-dealerships

O'Donoghue, T., & Rabin, M. (2000). The economics of immediate gratification. *Journal of Behavioral Decision Making*, *13*(2), 233–250. https://doi.org/10.1002/(SICI)1099-0771(200004/06)13:2<233::AID-BDM325>3.0.CO;2-U

Payne, J. W. (1976). Task complexity and contingent processing in decision making: An information search and protocol analysis. *Organizational Behavior and Human Performance*, *16*(2), 366–387. https://doi.org/10.1016/0030-5073(76)90022-2

Perrin, A. (2018). *Americans are changing their relationship with Facebook.* Pew Research Center. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Perrin, A., & Anderson, M. (2019). *Share of U.S. adults using social media, including Facebook, is mostly unchanged sicne 2018*. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/

Peters, E., & Slovic, P. (1996). The Role of Affect and Worldviews as Orienting Dispositions in the Perception and Acceptance of Nuclear Power1. *Journal of Applied Social Psychology*, *26*(16), 1427–1453. https://doi.org/10.1111/j.1559-1816.1996.tb00079.x

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, *1*(4), 311–335. https://doi.org/10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Phelan, C., Arbor, A., & Resnick, P. (2016). It's creepy, but it doesn't bother me. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5372–5384. https://doi.org/10.1145/2858036.2858388

Przybylski, A. K., Murayama, K., Dehaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, *29*(4), 1841–1848. https://doi.org/10.1016/j.chb.2013.02.014

Rachlin, H., Brown, J., & Cross, D. (2000). Discounting in judgments of delay and probability. *Journal of Behavioral Decision Making*, *13*(2), 145–159. https://doi.org/10.1002/(SICI)1099-0771(200004/06)13:2<145::AID-BDM320>3.0.CO;2-4

Radcliffe, N. M., & Klein, W. M. P. (2002). Dispositional, unrealistic, and comparative optimism: Differential relations with the knowledge and processing of risk information

and beliefs about personal risk. *Personality and Social Psychology Bulletin*, *28*(6), 836–846. https://doi.org/10.1177/0146167202289012

Rainie, L. (2018). *Americans' complicated feelings about social media in an era of privacy concerns*. Pew Research Center. https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Read, D., & Loewenstein, G. (2000). Time and decision: Introduction to the special issue. *Journal of Behavioral Decision Making*, *13*(2), 141–144. https://doi.org/10.1002/(sici)1099-0771(200004/06)13:2<141::aid-bdm347>3.3.co;2-l

Rodriguez, S. (2019, December 6). *Facebook has a theory that hiding "likes" will increase post volume, and Instagram is testing that theory*. CNBC. https://www.cnbc.com/2019/12/06/instagram-hiding-likes-could-increase-post-volume.html

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). *How Trump Consultants Explotied the Facebook Data of Millions*. The New York Times. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Rosson, M. B., & Ge, J. (2016). To disclose or note: Scenario-based design of privacy heuristics [Workshop]. CHI 2016 Workshop: Bridging the Gab between Privacy by Design and Privacy in Practice, San Jose, CA, United States.

Rubinstein, A. (2003). "Economics and psychology"? The case of hyperbolic discounting. *International Economic Review*, *44*(4), 1207–1216. https://www.jstor.org/stable/3663648

Schöbel, S., Barev, T., Janson, A., Hupfeld, F., & Leimeister, J. M. (2020). Understanding user preferences of digital privacy nudges - A best-worst scaling approach. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, *3*, 3918–3927. https://doi.org/10.24251/hicss.2020.479

Shah, A. K., & Oppenheimer, D. M. (2008). Heuristics made easy: An effort-reduction framework. *Psychological Bulletin*, *134*(2), 207–222. https://doi.org/10.1037/0033-2909.134.2.207

Shepperd, J. a., Helweg-Larsen, M., & Ortega, L. (2003). Are comparative risk judgments consistent across time and events? *Personality and Social Psychology Bulletin*, *29*(9), 1169–1180. https://doi.org/10.1177/0146167203254598

Shi, P., Xu, H., & Chen, Y. (2013). Using contextual integrity to examine interpersonal information boundary on social network sites. *Proceedings of the 2013 ACM SIGCHI Conference on Human Factors in Computing Systems*, 35-38. https://doi.org/10.1145/2470654.2470660

Shibchurn, J., & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic-extrinsic motivation perspective. *Computers in Human Behavior*, *44*, 103–117. https://doi.org/10.1016/j.chb.2014.10.059

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99–118. http://www.jstor.org/stable/1884852

Simon, H. A. (1979). Rational decision making in business organizations. *The American Economic Review*, *69*(4), 493–513. https://www.jstor.org/stable/1808698

Simon, H. A. (1982). *Models of bounded rationality*. MIT Press.

Simon, H. A. (1990). Invariants of huamn behavior. *Annual Review of Psychology1*, *41*, 1–19. https://doi.org/10.1146/annurev.ps.41.020190.000245

Simon, H. A. (1997). Bounded rationality. In *Models of bounded rationality: Emperically grounded economic reason* (Vol. 3, pp. 291–294). The MIT Press.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings. *Risk Analysis*, *24*(2), 311–322. https://doi.org/10.1111/j.0272-4332.2004.00433.x

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333–1352. https://doi.org/10.1016/j.ejor.2005.04.006

Smith, A., & Anderson, M. (2018). *Social media use in 2018*. Pew Research Center. http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880–1903. https://ssrn.com/abstract=2171018

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, *22*, 55–70. https://doi.org/10.1111/JCC4.12182

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41. https://ssrn.com/abstract=3305329

Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292.

https://doi.org/10.1016/j.chb.2015.06.006

Sundar, S. S. (2008). The MAIN model: A heuristic approach to understanding technology effects on credibility. In M. J. Metzger & A. J. Flanagin (Eds.), *Digital media, youth, and credibility* (pp. 73–100). The MIT Press.

Sundar, S. S., Gambino, A., Kim, J., & Rosson, M. B. (2016). Six ways to enact privacy by design: Cognitive heuristics that predict users' online information disclosure [workshop]. *CHI 2016 Workshop: Bridging the Gap between Privacy by Design and Privacy in Practice*, San Jose, CA, United States.

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox: do cognitive heuristics hold the key? *CHI EA '13: CHI '13 Extended Abstracts on Human Factors in Computing Systems*, 811–816. https://doi.org/10.1145/2468356.2468501

Sundar, S. S., Kim, J., & Rosson, M. B. (2019). The role of interface cues in online privacy: Cognitive heuristics that predict information disclosure [Paper presentation]. *International Communication Association*. Washington, D.C., United States.

Sundar, S. S., Knoblock-Westerwick, S., & Hastall, M. R. (2007). News cues: Information scent and cognitive heuristics. *Journal of the American Society for Information and Technology*, *58*(3), 366–378. https://doi.org/10.1002/asi

Sunstein, C. R. (2016). People prefer system 2 nudges (kind of). *Duke Law Journal*, *66*(1), 121–168. https://doi.org/10.2139/ssrn.2731868

Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science*, *12*(2), 257–285. https://doi.org/10.1016/0364-0213(88)90023-7

Sweller, J., Van Merrienboer, J. J. G., & Paas, F. G. W. C. (1998). Cognitive Architecture and Instructional Design. *Educational Psychology Review*, *10*(3), 251–296.

https://doi.org/10.1023/A:1022193728205

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), 248–273. https://doi.org/10.1111/jcc4.12052

Tajfel, H., & Turner, J. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Eds.), *Social Psychology of Intergroup Relations* (pp. 33–47). Brooks/Cole Publishing.

Thaler, R. H. (1981). Some empirical evidence on dynamic inconsistency. *Economics Letters*, *8*(3), 201–207. https://doi.org/10.1016/0165-1765(81)90067-7

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media and Society*, *3*(1). https://doi.org/10.1177/2056305116688035

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, *5*(2), 207–232. https://doi.org/10.1016/0010-0285(73)90033-9

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice : A reference-dependent model. *The Quarterly Journal of Economics*, *106*(4), 1039–1061. https://doi.org/10.2307/2937956

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative

representation of uncertainty. *Journal of Risk and Uncertainty*, *5*, 297–323. https://doi.org/10.15358/0340-1650-2006-6-331

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, *22*(2), 157–174. https://doi.org/10.1016/j.jsis.2013.01.003

Warzel, C. (2019, April 16). *Privacy Is Too Big to Understand*. The New York Times. https://www.nytimes.com/2019/04/16/opinion/privacy-technology.html

Wei, R., Lo, V.-H., & Lu, H.-Y. (2007). Reconsidering the relationship between the third-person perception and optimistic bias. *Communication Research*, *34*(6), 665–684. https://doi.org/10.1177/0093650207307903

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, *39*(5), 806–820. https://doi.org/10.1037/a0020997

Westin, A. (1967). *Privacy and freedom*. Atheneum.

Wilson, D. W. (2015). *Overcoming information privacy concerns: Learning from three disclosure contexts* [Doctoral dissertation, University of Arizona]. University Libraries, University of Arizona.

Wilson, D. W., & Valacich, J. (2012, December 16-19). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus [Paper presentation].

International Conference on Information Systems, Orlando, FL, United States.

Winkielman, P., Zajonc, R. B., & Schwarz, N. (1997). Subliminal affective priming resists attributional interventions. *Cognition and Emotion*, *11*(4), 433–465. https://doi.org/10.1080/026999397379872

Yu, J., Hu, P. J. H., & Cheng, T. H. (2015). Role of affect in self-disclosure on social network websites: A tets of two competing models. *Journal of Management Information Systems*, *32*(2), 239–277. https://doi.org/10.1080/07421222.2015.1063305

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

Appendix

Appendix A

Focus Group Interview Protocol

Introduction

Welcome to our study. This study is about privacy on social network sites, such as Facebook, Instagram, and Snapchat or others that you might use. My name is _____ and I will be leading a group discussion today about this topic. I will be asking questions about how you think about, and deal with, privacy on social network sites.

Specifically, we are looking to learn about the "mental shortcuts" people use to make choices about privacy when they use social network sites. These mental shortcuts are also known as *cognitive heuristics*. Some examples of cognitive heuristics outside the realm of privacy include things like: people tend to feel that something that is expensive is high quality; something that is said by an expert is true and unbiased; or people tend to assume that something that is popular is good.

General

1. Which social network sites (SNSs) do you use?
2. How often do you use these SNSs?

Affect Heuristic

3. How much do you like using social network sites, such as Facebook, Instagram, Snapchat, etc.? Are there some that you like better or worse? Why?
4. To what extent do you think that people's *opinion* (that is, how much they like) Facebook, Instagram, or Snapchat affects *how much information* they post on them?
    a. [In other words, do you think how much people like (Facebook/Instagram/Snapchat) ever plays into how much information they disclose about themselves on those SNSs?]
    b. Can you give an example or describe a time where your own positive feelings about an SNS influenced your decision to post information on it?

Availability Heuristic

5. Have you ever had a bad experience concerning privacy, or has a friend ever had a bad privacy experience, as a result of posting information on (Facebook/Instagram/Snapchat)? This might include things like:
   a. … been really embarrassed by something on Facebook being seen by the wrong people?
   b. … had a stalker as a result of using Facebook?
   c. … lost a friendship as a result of using Facebook because some private information was revealed?
   d. … or other things.
6. Do you feel that this experience affected the things you do to protect privacy on (Facebook/Instagram/Snapchat) after it happened? For example, do you share less information as a result of it? Do you have stricter privacy settings? Anything else? Please give an example if you can.

Optimistic Bias

7. Who do you think is more likely to have a bad privacy experience as a result of using (Facebook/Instagram/Snapchat), you or an average user?
   a. Please explain why you feel the way you do about this.
   b. Do you think you are more cautious in what you do, post, or select the privacy settings than the average person?

Bubble Heuristic

8. When you think about (Facebook/Instagram/Snapchat), which one/ones feel "safer" to you in terms of posting information about yourself?
   a. Do you think this sense of (relative) safety of one versus another affects how much people disclose on the site, or whether they disclose more sensitive types of information on one versus another of these sites?
9. To what extent do you feel using social network site's privacy settings (such as limiting who can see your posts, etc.) factor into people's decision to share information? Does using those settings make you feel that the site is a safe place to post information?
   a. Do you think that affects how much information people disclose on these SNSs?
   b. Give an example or time this happened to you if you can.
   c. How would you feel if there were no privacy settings?
10. Have you ever created a "finsta"? If yes, do you post more information there or more sensitive information there? Why? Does it feel safer to post there? Why?

Homophily Heuristic

11. To what extent do you feel that your friends/followers on (Facebook/Instagram/Snapchat) are similar to you, and in what ways are they similar (same age; race; hometown, school; or job; same political views, etc.)?
    a. What about the people you interact with most on SNSs—how similar do you feel they are to you?
12. On (Facebook/Instagram/Snapchat), does it feel safer to express your opinions when you think your friends/followers are similar to you—for example when they have similar opinions or life experiences as your own? If yes, why does it feel safer?
    a. Can you give an example of a time that you might have posted *more* information because you believed your friends/followers had similar opinions or views as yours?
    b. Can you give me an example of a time that you *held back* posting something online because you weren't sure if your friends/followers would agree? Why did you decide not to post? How did you feel when you were making the decision to hold back your opinion, photo, comment, etc.?
    c. If this isn't something that applies to you personally, do you think it's something that other people consider or do? [Have you heard of anyone doing this? Provide an example if you can.]

Bandwagon Heuristic

13. To what extent do you think people post about certain topics or post certain types of pictures because other people are posting those things? Can you give an example? Why do you think people do this? Has this happened to you?
14. Do you ever notice or hear about other people's privacy settings? If so, does this affect what you do to protect your privacy on (Facebook/Instagram/Snapchat)? Can you give any examples?

Inequity Aversion

15. To what extent do you feel that fear of missing out (missing out socially) motivates people to post or disclose information on social media? Can you give an example from your own experience or from something you heard from a friend?
16. To what extent do you post on SNSs to get as much response (likes, retweets, etc.) as other people? Can you give an example?

Hyperbolic Discounting

17. Have you ever posted something even though you knew you might regret it later? Why did you post it [did you want the immediate gratification] when you knew it could have negative repercussions?
    a. Why do you think you posted the information in that moment? Were you hesitant to post that information in the moment?
    b. Can anyone think of any other examples when this happened to them or someone you know?

c. [Ask about *emotional* posts specifically.]

Ephemerality Heuristic

18. To what extent does it feel "safer" or less risky to post on (Instagram Stories/ Snapchat/ Facebook Stories) when you know your post will disappear in 24 hours? Why do you feel this way?
    a. Do you think that this temporal aspect affects how <u>much</u> information you disclose on social media? What about the <u>types</u> of information you post (e.g., how personal or sensitive the information you post is)?
    b. Please give an example if you can.

Appendix B

Summary of Hypotheses and Research Questions for Study 2

Heuristic	Disclosure/ Privacy	Hypotheses and Research Questions	
Affect Heuristic	Disclosure Heuristic	H1a	The affect heuristic, as reflected in the degree to which users feel affectively positive about a specific SNS, is positively associated with their amount of disclosure on that SNS.
		H1b	The affect heuristic, as reflected in the degree to which users feel affectively positive about a specific SNS is negatively associated with their perceived risk about disclosure on that SNS.
Availability Heuristic	Both Disclosure and Privacy Heuristic	H2a	The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is negatively associated with the amount of disclosure.
		H2b	The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is positively associated with the perceived risk about disclosure on SNSs.
		H2c	The availability heuristic, as reflected in the perceived severity of a past negative privacy experience on SNSs, is positively associated with the restrictiveness of their privacy settings.

Heuristic	Disclosure/ Privacy	Hypotheses and Research Questions	
Optimistic Bias	Unknown	RQ1	Is users' optimistic bias, as reflected in the perceived likelihood of having a negative privacy experience on SNSs compared to others, related to the amount of information users disclose on SNSs?
		RQ2	Is users' optimistic bias, as reflected in the perceived likelihood of having a negative privacy experience on SNSs compared to others, related to the restrictiveness of users' privacy settings on SNSs?
Bubble Heuristic	Disclosure Heuristic	H3a	The bubble heuristic, as reflected in the restrictiveness of users' privacy settings, is positively associated with their amount of disclosure on SNSs.
		H3b	The bubble heuristic, as reflected in the restrictiveness of users' privacy settings, is negatively associated with their perceived risk about disclosure on SNSs.
Homophily Heuristic	Disclosure Heuristic	H4a	The homophily heuristic, as reflected in users' perceived similarity to their social network connections, is positively associated with their amount of disclosure on SNSs.
		H4b	The homophily heuristic, as reflected in users' perceived similarity to their social network connections, is negatively associated with their perceived risk about disclosure on SNSs.
Bandwagon Heuristic	Both Disclosure and Privacy Heuristic	H5a	The bandwagon heuristic, which is reflected in the extent to which users pay attention to others' posts on SNSs, is positively associated with their amount of disclosure on SNSs.
		H5b	The bandwagon heuristic, which is reflected in the extent to which users pay attention to others' posts on SNSs, is negatively associated with their perceived risk about disclosure on SNSs.
		H5c	The bandwagon heuristic, which is reflected in the extent to which users pay attention others' privacy settings, is positively associated with to the restrictiveness of their own privacy settings.

Heuristic	Disclosure/ Privacy	Hypotheses and Research Questions	
Inequity Aversion	Unknown	RQ3	Is inequity aversion, as reflected in the degree of users' perceived benefit compared to other users, related to their amount of disclosure on SNSs?
		RQ4	Is inequity aversion, as reflected in the degree of users' perceived benefit compared to other users, related to their perceived risk about disclosure on SNSs?
Hyperbolic Discounting	Disclosure Heuristic	H6a	Hyperbolic discounting, as reflected in the degree to which users make decisions about disclosure on an impulse on SNSs, is positively associated with their amount of disclosure on SNSs.
		H6b	Hyperbolic discounting, as reflected in the degree to which users make decisions about disclosure on an impulse on SNSs, is negatively associated with their perceived risk about disclosure on SNSs.
Ephemerality Heuristic	Disclosure Heuristic	H7a	The ephemerality heuristic, as reflected in the extent to which users use ephemeral features on SNS, is positively associated with the amount of their overall disclosure on SNSs.
		H7b	The ephemerality heuristic, as reflected in the extent to which users use ephemeral features on SNS, is negatively associated with their perceived risk about disclosure on SNSs.

Appendix C

Summary of Measures for Study 2A

Variable	Items
Affect Heuristic	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree”)
	The more I like a particular social media platform (e.g., its features), the more information I share on that platform.

Variable	Items
	The more I dislike a particular social media platform (e.g., its features), the less comfortable I feel about sharing my information on that platform. The more I like a particular social media platform (e.g., its features), the less risk I feel when sharing my information on that platform. How good or bad I feel about a particular social media company affects how much information I tend to share on its platform. How good or bad I feel about a particular social media company affects how comfortable I feel about sharing information on its platform. How good or bad I feel about a particular social media company affects how much risk I feel when sharing information about myself on its platform.
Availability Heuristic	Have you ever had a negative experience concerning privacy as a result of using a social media platform? (1 = "Yes", 0 = "No") As a result of this experience, to what extent did you… (1 = "Not at all", 7 = "A whole lot") ...reduce the amount of information you share on social media? ...reduce your use of social media? ...feel less comfortable sharing information about yourself on social media? ...change your account settings in ways to better protect your privacy? ...become more protective of your privacy when using social media? Have you ever heard of others (e.g., friends, acquaintances, or people in media coverage) having a negative experience concerning privacy as a result of using a social media platform? (1 = "Yes", 0 = "No") If yes, as a result of this experience, to what extent did you… ...reduce the amount of information you share on social media? ...reduce your use of social media? ...feel less comfortable sharing information about yourself on social media? ...change your account settings in ways to better protect your privacy? ...become more protective of your privacy when using social media?

Variable	Items
Optimistic Bias	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree”) I do not select restrictive privacy settings on social media because I feel like other people are more likely to have a negative privacy experience than I am. Because I feel I am less likely to have a negative privacy experience on social media than most people, I feel comfortable sharing my information there. I share more of my information on social media because I feel less likely to have a negative privacy experience than others.
Bubble Heuristic	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree”) Having privacy settings available makes me feel more comfortable about sharing information on social media. To feel comfortable about sharing certain information on social media, I tightly control who can see my posts. Using the privacy settings on social media to restrict who can see my profile or posts makes sharing information feel less risky. The privacy settings a platform offers users is a big factor in how much information I share on social media.
Homophily Heuristic	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree”) I share more posts with my friends and followers on social media who are more similar to me (in age, political opinions, background, etc.) When I feel more similar to my friends and followers on social media, I feel more comfortable posting information. The more similar my friends and followers on social media are to me, the less risk I feel about posting things on those platforms. I am less likely to post my feelings or opinions when I think my social media connections (e.g., friends and followers) will disagree with me.
Bandwagon Heuristic	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree”) When I see my friends or followers post about something personal or sensitive on social media, I feel more

Variable	Items
	comfortable about posting something similar myself.
	If I see my friends or followers post about something on social media (e.g., holiday photos, etc.), I am more likely to post something similar myself.
	If my friends change their privacy settings to be more or less private, I am more likely to do it too.
	If my friends and followers use specific social media features (e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.), I am more likely to use them too.
	When my friends and followers use specific social media features (e.g., Stories, stickers, GIFs, hashtags, poll features, recommendation features, etc.), it feels safer for me to use them too.
	If I were to hear about my friends using a new social media platform, I would probably feel more comfortable about trying that platform myself.
Inequity Aversion	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree")
	I feel motivated to post on social media when I see others getting more benefits than me (e.g., getting more likes, more attention, invitations, etc.).
	I feel motivated to get more friends/followers because I want to get as much benefit as I see other people getting (e.g., likes, attention, invitations, etc.).
	I feel motivated to use social media more often when I see others getting more benefits than me (e.g., getting more likes, more attention, invitations, etc.)
	Seeing others benefit (e.g., getting more likes, more attention, etc.) more than I do from posting information on social media makes me feel less concerned about the privacy risks of using social media.
	When I experience fear of missing out (FOMO), I feel motivated to engage in an experience I can post about on social media so I feel less left out.
Hyperbolic Discounting	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree")
	I posted something on social media "in the heat of the moment," which I later regretted.
	When debating whether to post some information, I sometimes feel the immediate benefits of posting outweigh the risks I might experience later.
	I sometimes post or share things on social media without thinking about the consequences.
	I tend to post things on social media in the spur of the moment to express my feelings, even if I know I might

Variable	Items
	regret it later. I resist the urge to act “on impulse” when posting things on social media (reverse coded).
Ephemerality Heuristic	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree") I am inclined to post more information on social media platforms where the content disappears after a short period of time (e.g., 24 hours). I am more comfortable posting on social media platforms where content disappears within 24 hours. I post more Stories than permanent posts because I feel like there is less risk in posting content that disappears within 24 hours.

Appendix D

Summary of Measures for Study 2B

Variable	Items
Dependent Variables	
Amount of Disclosure	How much information do you share on the following social media platforms: [Facebook/Instagram/Snapchat/Twitter]? (1 = "None", 7 = "A great deal")
Sensitive Disclosure	How much information do you share about the following topics on the following social media platforms: [Facebook/Instagram/Snapchat/Twitter]? (1 = "Not at all", 7 = "A great deal") Please rate the following topics in terms of how sensitive you feel each type of information is. (1 = "Not sensitive at all", 7 = "Extremely sensitive") • Political opinions and preferences

Variable	Items
	• Deep feelings and emotions • Negative things that happened to you • Controversial social issues or news topics • Photos of you • Photos of things you like (e.g., hobbies, interests, etc.) • News (e.g., local, national, international, etc.) • Contact information (e.g., cell phone number, mailing address, etc.) • Positive things that happened to you • Romantic Relationships
Restrictiveness of Privacy Settings	How public or private are your privacy settings on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = “Public”, 7 = “Very private”)
Perceived Risk about Disclosure	How risky do you feel about posting information on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = "Not risky at all", 7 = "Very risky") How comfortable do you feel about posting information on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = "Very uncomfortable", 7 = "Very comfortable") How safe do you feel posting information on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = "Not safe at all", 7 = "Very safe")
Privacy Management Strategies	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree") I have restricted who can view my posts on social media. I have customized the privacy setting of individual posts to restrict who can view my posts on social media. I have limited people from searching my profile on social media. I have restricted or blocked accounts on social media.

Variable	Items
	I have restricted who can directly contact or message me on social media.
Heuristics	
Affect Heuristic	When I think about [Facebook/Instagram/Snapchat/Twitter], I feel: (1 = "Bad", 7 = "Good", 1 = "Positive", 7 = Negative [reverse coded], 1 = "Happy", 7 = "Sad" [reverse coded], 1 = "Fearful", 7 = "Unafraid", 1 = "Angry", 7 = "Pleased", 1 = "Respect", 7 = "Disgust" [reverse coded], 1 = "Disliking", 7 = "Liking", 1 = "Trust", 7 = "Suspicion" [reverse coded])
Availability Heuristic	Have you ever had a negative experience concerning privacy as a result of using social media platforms, such as Facebook, Instagram, Snapchat, and Twitter? (1 = "Yes", 0 = "No") How severe was that negative experience on [Facebook/Instagram/Snapchat/Twitter]? (1 = "Not severe at all", 7 = "Very severe")
Optimistic Bias	Who would you say is more likely to have a negative privacy experience as a result of using the following social media platform(s) [Facebook/Instagram/Snapchat/Twitter], you or an average user? (1 = "I am more likely", 7 = "An average user is more likely")
Homophily Heuristic	People may be similar to one another in terms of their age, background, political views, or other things. How similar or dissimilar do you feel to your connections (e.g., friends, followers, etc.) on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = "Not similar at all", 7 = "Very similar")
Bandwagon Heuristic	To what extent do you pay attention to what others post on the following social media platform(s) [Facebook/Instagram/Snapchat/Twitter]? (1 = "Not at all", 7 = "Very much") To what extent do you enjoy following social media trends (e.g., holiday photos, ice bucket challenge, etc.) on the following social media platform(s)? (1 = "Not at all", 7 = "Very much")
Inequity	Compared to other users, do you think you get more or less benefit (e.g., popularity, attention, likes, etc.) on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = "I get more benefit", 7 =

Variable	Items
Aversion	"Other users get more benefit")
Hyperbolic Discounting	Looking back on your experience using [Facebook/Instagram/Snapchat/Twitter], to what extend have you shared something… (1 = "Never", 9 = "Many times") …in the heat of the moment ...because you had to express or release my emotions (e.g., happiness, sadness, anger, etc.)? ...and then regretted your decision later? ...on an impulse?
Ephemerality Heuristic	How frequently do you share Stories that disappear in 24 hours on the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]? (1 = "Never", 7 = "Very often")
Control Variables	
Age	What is your age?
Sex	What is your sex?
Ethnicity	What is your ethnicity?
Race	What is your race?
Sexual orientation	How would you describe your sexual orientation?
Education level	What is the highest level of education you have completed?
Religious views	What is your present religion, if any? How religious are you?

Variable	Items
Political views	What is your political party affiliation? How would you describe your political views?
Frequency of SNS Use	How frequently do you use the following social media platform(s): [Facebook/Instagram/Snapchat/Twitter]?
Number of SNSs used	Which of these social media platforms do you use: [Facebook/Instagram/Snapchat/Twitter]? (please select all that you use)
Privacy Concern on SNSs	To what extent do you agree with the following statements? (1 = "Strongly disagree", 7 = "Strongly agree) Compared with other topics, privacy in social media is not very important to me. I do not feel especially concerned about my privacy in social media. The danger to people's privacy when they use social media has been overblown.