12-2019

Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings

Hichang CHO

Sungjong ROH
Singapore Management University, sroh@smu.edu.sg

Byungho PARK

Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings

Hichang Choa , Sungjong Roh , Byungho Park

Abstract

Privacy research has debated whether privacy decision-making is determined by users' stable preferences (i.e., individual traits), privacy calculus (i.e., cost-benefit analysis), or "responses on the spot" that vary across contexts. This study focuses on two factors—default setting as a contextual factor and regulatory focus as an individual difference factor—and examines the degree to which these factors affect social media users' decisionmaking when using privacy preference settings in a fictitious social networking site. The results, based on two experimental studies (study 1, n = 414; study 2, n = 213), show that default settings significantly affect users' privacy preferences, such that users choose the defaults or alternatives proximal to them. Study 2 shows that regulatory focus also affects privacy decisions, such that users with a strong promotion focus select options favoring a higher social networking utility, perceiving lesser cognitive efforts and more confidence in decisions. Finally, we find a significant interaction effect between default setting and regulatory focus on perceived effort and confidence, suggesting that the default effect is contingent on users' goal orientations (operationalized as regulatory focus). We discuss the implications for research and practice

Keywords: Privacy Default effect Regulatory focus Social media

1. Introduction

Though new information and communication technologies (ICTs) enable innovative and effective ways of socializing with others, working together, and transacting services and products online, many people are concerned about information privacy risks because the personal information they disclose online while engaging in these activities can be easily collected, shared, and/or misused by third parties, including businesses, governments, and even their own friends. The recent Facebook and Cambridge Analytica privacy scandal that resulted in more than 87 million Facebook users' data being compromised is one of many examples of privacy risks (BBC News, 2018). More recently, Facebook reported that a software bug changed privacy settings of up to 14 million Facebook users, making their private posts available to the public (New York Times, 2018a). As privacy risks are increasingly prevalent and unpredictable, information privacy is a key factor influencing users' communication behavior (Dienlin & Metzger, 2016), technology acceptance (Shin, 2010a), and their relationship with media (Pew Research Center, 2018).

Previous privacy studies have assumed that, to maintain an optimal level of privacy, users engage in thoughtful assessments of risks and benefits based on privacy calculus and make rational choices (e.g., information disclosure/withholding, network size control) (Dienlin & Metzger, 2016; Lankton, McKnight, & Tripp, 2017). However, research has shown that users are "not always rational but paradoxical" (Park, Chung, & Shin, 2018, p. 1323). Further, recent studies have revealed that privacy decision-making is also influenced by heuristics and cognitive biases, such as decision frames (Acquisti, John, & Loewenstein, 2012) and hyperbolic discounting (Krasnova, Spiekermann, Kololeva, & Hildebrand, 2010). For instance, users' privacy preferences can easily be shifted by subtle changes in privacy default settings, such as opt-in versus opt-out (Johnson, Bellman, & Lohse, 2002). Although the options that are given to users are logically equivalent, when framed differently in default settings, the differences in privacy settings can cause marked reversals in revealed preferences (Baek, Bae, Jeong, Kim, & Rhee, 2014; Knijnenburg & Kobsa, 2014). These findings suggest that a user's privacy

decision-making is based on “responses on the spot” rather than on stable privacy preferences or a privacy calculus, highlighting the malleability of privacy decision-making and preferences.
In this study, we examine social media users' privacy decision-making using a novel approach through which we investigate the effect of privacy default settings (as a contextual factor) and individuals' goal orientations (i.e., regulatory focus as an individual trait) on users' construction of privacy preferences. While a significant default effect on users' preferences has been demonstrated elsewhere, previous studies also show that its effect may not equally influence all users’ behavior (Knijnenburg & Kobsa, 2014; Lai & Hui, 2006), suggesting that individual differences or contextual factors should be incorporated into a research model to gain a more complete understanding.

Specifically, an important gap in prior privacy studies is that most studies have investigated this topic neglecting motivational factors, especially, users' goals. Privacy decision-making inherently involves a tradeoff between multiple goals and competing considerations, such as self-promotion, social need fulfilment, privacy protection, and security (Vishwanath, Xu, & Ngoh, 2018). It has been suggested that goals are a key component of decision-making (Payne, Bettman, & Johnson, 1993; Higgins, 1997, 2011), and that individuals' goal orientations and goal pursuit strategies are determined by a distinctive self-regulations system called regulatory focus (Higgins, 1997). Therefore, this study examines regulatory focus as an important individual trait that can affect users' judgments and decisions when individuals construct their preferences using preference settings. For instance, individuals’ preference for stability (e.g., maintaining privacy defaults) versus change (e.g., choosing alternative, non-default options) can be explained by the distinction between prevention focus and promotion focus to the extent that the former is associated with a preference for stability/status quo (for prevention/safety), whereas the latter is associated with openness to change (for promotion/gain) (Chernev, 2004; Crowe & Higgins, 1997). Whether people with a distinct regulatory focus construe privacy as a different goal (privacy as a desirable end-state [i.e., promotion] versus privacy for safety and security [i.e., prevention]) and construct their preferences differently is also a theoretical question that has yet to be empirically investigated.

In spite of the rational connections between regulatory focus, default effect, and privacy decision-making, little empirical research has been conducted to investigate the role of regulatory focus in relation to privacy (see Craciun, 2018; Lwin, Wirtz, & Stanaland, 2016; Mosteller & Poddar, 2017; for exceptions). As such, this study aims to conduct one of the first studies to empirically examine these relationships in the social media context. Drawing on previous literature on default effects (e.g., Johnson et al., 2002; Knijnenburg & Kobsa, 2014) and regulatory focus (e.g., Higgins, 1997, 2011), we formulated research hypotheses and tested them in two studies in which we (a) examine the baseline model focusing on the main effect of default settings on privacy decision-making (study 1); (b) test the replicability/robustness of the default effect (study 2); and (c) examine the main effect and the moderating effect of regulatory focus in the context of privacy decision-making using preference settings (study 2). In doing so, we address the following broad research questions.
RQ1

To what extent is social media users' privacy decision-making influenced by default settings, regulatory focus, and the interaction between them?

This study aims to contribute to privacy studies by suggesting a theoretical approach to examining the effect of a contextual factor (default settings) and an individual factor (regulatory focus) and the interplay between them to understand complex mechanisms operating in privacy decision-making. The investigation of the potential interaction between default (contextual factor) and regulatory focus (individual factor) will enable us to specify boundary conditions under which different default settings have differing implications for social media users’ privacy decisions. In addition, its findings would be of practical value as they reveal the magnitude of default effects in different conditions and hint at optimal default settings for individuals with different traits like regulatory focus. To achieve these

aims, we conducted two empirical studies (Study 1 [n = 414]; Study 2 [n = 213]), and report and discuss the findings and their implications.

2. Literature review

2.1. Privacy decision-making and preference settings

Privacy decision-making is complex, as it involves not only a high degree of uncertainty but also complicated trade-offs between multiple, conflicting goals (Acquisti, Brandimarte, & Loewenstein, 2015). According to Altman (1975), privacy management is defined as an interpersonal boundary-control process that makes us open or close to others. This process is dialectic, dynamic, and bidirectional because people encounter with "the competing simultaneous needs to be both social (by disclosing information) and private (by withholding information)" (Dienlin & Metzger, 2016, p. 371). Therefore, people engage in dynamic and dialectic decision-making processes related to interpersonal boundary regulation and privacy management strategies (Petronio, 1991) through which they can keep the optimal level of balance between privacy and openness. Likewise, social media users negotiate privacy concerns and social capital needs when making privacy-related decisions (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011; Vishwanath et al., 2018). Because social media users want to have strict privacy control through information withholding but at the same time need to share their personal data for personalized content and services (Park et al., 2018), trade-off difficulty is inherent in privacy decision-making (Vishwanath et al., 2018). The increasing complexity involved in privacy management and protection also leads to feelings of resignation and lack of control (Choi, Park, & Jung, 2018).

In social media contexts, privacy settings are a primary technological mechanism through which users can articulate their desired levels of social connections, information disclosure, and privacy (Ellison et al., 2011; Lankton et al., 2017). For instance, with the privacy settings embedded in Facebook, users can set their profiles to "Only Me," "Friends except ___," "Friends," and "Public" to control the visibility, searchability, and access to their personal information and content. Though seemingly a simple choice, this type of decision context involves trade-off difficulty and decisional complexity. Because the attainment of one goal (e.g., strict privacy control achieved by limiting access to close friends) blocks the attainment of other goals (e.g., high social networking utility with wider audiences), an individual must make explicit trade-offs between the conflicting goals. Similarly, use of privacy settings involves deciding between stability (i.e., preserving defaults/status quo) and change (choosing alternative options). In addition, privacy decision-making involves a high degree of uncertainty because the outcome of each choice is not entirely clear to many online users, and neither option clearly dominates the other (Acquisti et al., 2015).

Ideally, users can overcome such trade-off difficulties by putting forth extra effort to make the best and the most rational decision. However, studies have shown that, when faced with trade-offs and uncertainties, people often prefer effort-saving to accuracy (Lee & Benbasat, 2011). A possible reason is that the benefit of saving their cognitive load is temporarily near and easily observable than accuracy (Lee & Benbasat, 2011). As a result, users are likely to construct their preferences using various decisional shortcuts and contextual factors, such as privacy defaults, especially when they have unclear preferences or are not motivated to engage in effortful deliberation (Huh, Vosgerau, & Morewedge, 2014). In fact, research shows that although users are well aware of the privacy risks in social media use, most of them keep the default privacy settings that allow the public to access their online profiles and shared content (Gross & Acquisti, 2005), though a recent study showed that about 40 percent of U.S. Facebook users modified their privacy settings after the Cambridge Analytica privacy scandal (Pew Research Center, 2018).

2.2. Default effect

Default is defined as "the choice alternative a consumer receives if he/she does not explicitly specify otherwise" (Brown & Krishna, 2004, p. 529). Facebook's privacy settings, for instance, have been set to make users' profile information shared-by-default, making it available to the public unless users choose otherwise.

Powerful default effects have been well-demonstrated in various decision-making contexts. Many people do not change default settings on software (Mackay, 1991). Similarly, users of smartphone apps are more likely to retain more expensive privacy features when the privacy premium features are presented as defaults rather than as additional options (Dogruela, Joekelb, & Vitak, 2017). Privacy studies also have found that merely framing the question as opt-out instead of opt-in changes users' preferences (Baek et al., 2014; Johnson et al., 2002). Similarly, users are more likely to disclose personal information in shared-by-default than in privacy-by-default (Knijnenburg & Kobsa, 2014).

Importantly, a default effect is observed even for a decision requiring a considerable amount of effort and accuracy, such as choosing auto insurance options (Johnson, Hershey, Meszaros, & Kunreuther, 1993) and participating in organ donations (Johnson & Goldstein, 2003). The findings suggest that default effects cannot occur merely due to individuals' inattentiveness or laziness, but should operate through multiple theoretical mechanisms.

2.2.1. Theoretical mechanisms of default effect

The default effect can be explained by several theoretical mechanisms. First, due to cognitive and physical laziness (i.e., inertia), people are reluctant to make an effort to change to the non-default option. However, as noted earlier, studies have shown that effort calculations alone cannot fully explain default effects. For instance, when choosing to preserve or abandon the default required the same number of mouse clicks, a default effect was still observed (Johnson et al., 2002; Johnson & Goldstein, 2003).

Second, defaults determine decisions through status-quo bias. People believe that defaults are an endowment. Once the defaults are given, they perceive giving it up as loss of a valuable object that they possessed. According to the loss aversion and endowment effect (Tversky & Kahneman. 1981), the cost of losses looms larger than the pleasure of the equivalent gain. Consequently, people choose to keep the endowed option (i.e., defaults) rather than choosing alternative options. The presentation of one option as the status quo increases its attractiveness, because it is perceived as a focus of evaluation (Dhar & Simonson, 1992), despite the default option was randomly assigned (Samuelson & Zeckhauser, 1988).

Third, people are less likely to choose the non-default option to avoid the feeling of regret (Baron & Ritov, 1994). According to the omission bias, an act (or its outcomes) is weighted more heavily than inaction (or its outcomes) (Baron & Ritov, 1994). People regret more when poor decisions or outcomes are due to their own action (i.e., commission) rather than of inaction (i.e., omission) due to perceived decision responsibility. This omission bias is distinct from the status-quo bias, as people prefer inaction even when keeping the status quo requires actions, and changing the status quo does not require any (Baron & Ritov, 1994).

Fourth, individuals also perceive that defaults have been implicitly recommended or endorsed as the best option by those who select them (McKenzie, Liersch, & Finkelstein, 2006). In addition, individuals perceive the default as an indication of descriptive norms (i.e., many people would choose the same thing), and they thus follow a heuristic of imitation (Henrich et al., 2001).

Taken together, the literature reviewed above suggests that default effects operate through multiple theoretical mechanisms that are likely to function simultaneously. Empirical studies have demonstrated a default effect on the making of various decisions including privacy preference (Baek et al., 2014; Johnson et al., 2002; Knijnenburg & Kobsa, 2014), though most studies focused on a

binary choice (default versus nondefault). Studies have shown that when defaults are predefined, people evaluate multiple, alternative (non-default) options based on the degree to which they deviate from the default or the initial, starting point (Herrmann et al., 2011; Park, Jun, & MacInnis, 2000). The literature reviewed above suggest that defaults are perceived as the status quo and serve as a focus of evaluation (i.e., the initial value) with which other available options are compared (Dhar & Simonson, 1992; Payne et al., 1993). Even when people choose non-default options to make their selection in accordance with their own preferences, the default nonetheless influences expressed preferences as people direct their decisions toward implicitly or explicitly expressed recommended or endowed options (McKenzie et al., 2006; Tversky & Kahneman. 1981). As such, people are likely to preserve defaults or choose options that are proximal to the defaults because they consider them an endowment (Johnson et al., 2002) and deviations from them a loss or risky choice (Tversky & Kahneman, 1981). Hence, we predict that the following baseline hypothesis:

H1

Privacy defaults will have an impact on privacy preferences such that people are likely to preserve the default or choose alternative options proximal to the defaults.

2.3. Regulatory focus

2.3.1. Regulatory focus, privacy preference, and default settings

Regulatory focus theory (Higgins, 1997, 2011) postulates that individuals have two essential, distinguishable self-regulatory orientations: promotion focus and prevention focus. A person who has a promotion focus is oriented towards maximizing positive outcomes such as goal attainment, aspirations, and hope. On the contrary, a prevention-focused individual is oriented towards avoiding pain or bad outcomes. Because both types of goal pursuits (nurturance/advancement and protection) are essential for survival, it is assumed that all people have both foci to a certain extent. However, individuals exhibit stable, and trait-like differences in the predominance of each (Higgins, 1997). A shift in regulatory focus can also be momentarily induced by situational features, such as task instructions or message frames (Higgins, 1997).

Little research has examined whether privacy preference is a function of regulatory focus (Craciun, 2018; Jin, 2012). Promotion focus is associated with a preference for advancement, gain/attainment, and preference for eagerness strategies, whereas prevention focus is related to loss prevention and vigilance strategies. As such, it can be posited that strong promotion-focused people are likely to prefer higher levels of accessibility/permeability to maximize social networking sites' (SNSs) utility, whereas strong prevention-focused individuals prefer high levels of privacy protection to avoid potential privacy risks/losses. In the context of e-health website use, strong prevention regulatory focus corresponds to greater self-concealment tendency, the tendency to conceal personal information from others (Jin, 2012). In social media, social networking and self-promotion are related to users' advancement or promotion-oriented goals, whereas privacy is generally associated with prevention-oriented or safety-related user goals (Lwin et al., 2016). Hence, we predict that:

H2

Regulatory focus will have an impact on users' privacy preferences. Specifically, promotion focus will lead to preferences favoring wider audience groups whereas prevention focus will lead to strict privacy management.

The default effect is conceptually related to deciding between stability and change because users need to choose between maintaining the status quo (i.e., default) and pursuing non-default, alternatives. According to the endowment effect and decision frames (Payne et al., 1993; Tversky & Kahneman, 1981), the defaults function as a background or given condition, and alternative options are considered a new action or object, which create an opportunity for change. Studies have suggested that regulatory focus can explain preferences for stability versus change (Chernev, 2004; Friedman & Förster, 2001; Liberman, Idson, Camacho, & Higgins, 1999; Pham & Higgins, 2005). Promotion-focused people employ an eagerness or risk-taking strategy because of their strong focus on maximizing

potential gains and opportunities. As such, promotion-focused individuals are willing to pursue alternative possibilities by responding rather than nonresponding (Liberman et al., 1999; Liberman, Molden, Idson, & Higgins, 2001).

In contrast, a vigilance strategy is a preferred mode for people with a strong prevention focus. Due to their strong focus on risk minimization, prevention-focused people tend to choose safety/stability over accomplishment/change. As a result, prevention-focused individuals are inclined to choose the status quo to avoid making mistakes or causing potential losses due to their acts (Herzenstein, Posavac, & Brakus, 2007; Pham & Higgins, 2005). Further, Friedman and Förster (2001) suggest that a strong prevention focus triggers the risk-averse, cautious information processing and search style, leading to perseverance on initially assessed materials (e.g., the starting point in defaults). In summary, a promotion focus is conceptually linked to commission bias (i.e., tendency to undertake actions), and a prevention focus to an omission bias (i.e., tendency *not* to undertake actions).
The literature reviewed above indicates that promotion-focused and prevention-focused individuals should adopt different goal-pursuit strategies when using privacy preference settings. Specifically, individuals with a strong prevention focus are likely to focus on loss prevention. As a result, the perceived losses due to the departure from the status quo should appear to be larger to prevention-oriented than to promotion-oriented individuals (Chernev, 2004). On the other hand, people who have a strong promotion focus are likely to focus on maximizing gains and are less sensitive to potential losses due to their acts.

Taken together, we predict that default effects (as predicted in H1) can be potentially moderated by regulatory focus such that default effects will be intensified for those with a strong prevention focus, because they are oriented towards stability, and reduced for promotion-focused individuals, who favor actions and change (Pham & Higgins, 2005). Hence, we predict that there is an interaction effect between default and regulatory focus. To the best of our knowledge, there has been only one study (Craciun, 2018) that examined whether regulatory focus moderates the effect of defaults (opt-in versus opt-out) on consumers' information sharing intentions: their willingness to share personal information with third party service providers in an e-commerce setting. The study demonstrated that the opt-out default (i.e., "do not disclose") led to a significant decrease in the propensity of information sharing for prevention-focused consumers, but not for promotion-focused consumers. Though the findings are insightful, it is still unclear whether the same findings can be observed in the context of social media in which context (SNSs versus e-commerce), recipients of information (friends versus retailers), and choice architecture (multiple options versus dichotomous choices) are different. Hence, we test the following hypothesis.

H3

The effect of default settings on preferences will be moderated by regulatory focus such that the default effect will be stronger for users with a strong prevention focus than for users with a strong promotion focus.

2.3.2. Attitudes, perceived efforts, and confidence

While H1-H3 focus on the effect of default settings and regulatory focus on behavioral outcomes, we also explore their effects on attitudinal and judgmental factors that are central to decision-making: attitudes towards the use of privacy settings, perceived effort in decision-making, and confidence. We focus on these three outcome factors for the following reasons. First, confidence in choice is defined as "beliefs about the goodness of one's judgments or choices" (Sniezek, 1992, p. 124). In a privacy decision context, it refers to the degree to which users believe that their privacy choices are in line with their desired state of privacy control and information sharing (Church, Anderson, Bonneau, & Stajano, 2009). Confidence is central to decision making as it determines if and how those judgments or choices are implemented by the decision makers themselves. For instance, overconfidence leads to complacency whereas a lack of confidence results in doubt: both inhibiting an individual from taking necessary actions.

Second, perceived cognitive effort is defined as the perceived amount of effort required to make a decision (Lee & Benbasat, 2011). In decision-making contexts, individuals want to achieve two primary (often conflicting) goals: increasing the accuracy of the decision and reducing cognitive effort (Bettman, Luce, & Payne, 1998). People generally prefer decision-support systems that are perceived to provide accurate recommendations and want to be confident in their choices (Lee & Benbasat, 2011). However, decision means can be valued less when they are perceived to incur high cognitive effort (e.g., Payne et al., 1993), particularly when a choice task involves uncertainty and trade-off difficulty (as in the case of privacy decision-making). For instance, social media users perceive that privacy settings are confusing and time-consuming, resulting in a lack of motivation to put effort to manage privacy using preference settings (Lipford, Besmer, & Watson, 2008). Therefore, perceived cognitive effort is another key factor determining decision-making processes (e.g., the choice heuristics and the effort expenditure) and the quality of decisions about privacy.

Third, because this study tests privacy decision-making using technological mechanisms (i.e., privacy preference settings), we examine attitudes towards privacy setting use as another key variable. According to regulatory focus theory (Higgins, 1997), people drive value not only from the outcomes of the choices they make, "but also from their subjective assessments of the process by which those choices are made" (Pham & Higgins, 2005, p. 37). As such, we focus on *attitudes towards privacy setting use* that is defined as individuals' assessment of favorableness of using default settings as a means of constructing their privacy preferences. Attitudes towards technology use are a key factor influencing technology acceptance as well as continued use (Venkatesh, Morris, Davis, & Davis, 2003), including social media (Shin, 2010b) and decision-support systems (Jiang, Muhanna, & Klein, 2000). Attitudes towards technology use also affect user experiences, such as users' overall satisfaction with health informatics services (Shin, Lee, & Hwang, 2017). Hence, we examine attitudes as an important variable in our study.

In short, previous studies have emphasized that judgmental factors are "just as important to the ultimate outcomes of the decision as the quality of decision itself" (Sniezek, 1992, p. 124). Therefore, we claim that this study's additional focus on these factors enables a more comprehensive understanding of affective (i.e., attitudes), cognitive (i.e., perceived effort and confidence) and behavioral (i.e., choice outcomes) aspects of privacy decision-making.

More importantly, the regulatory focus literature suggests that regulatory focus is a key factor influencing attitudes and judgments in decision-making (Higgins, 1997). Regulatory focus theory proposes that people with different goal orientations have different preferences for goal-pursuit strategies (Cesario, Grant, & Higgins, 2004; Cesario & Higgins, 2008). When decision means are compatible with their goal orientations (e.g., approach [or avoidance] means for people with a strong promotion [or prevention] focus), regulatory fit occurs. With regulatory fit, people find it easy to respond to decision task (Cesario et al., 2004), because it is compatible with how they naturally think and behave (Higgins, 1997), resulting in feelings of rightness, favorable attitudes, and confidence in judgments in decision-making (Cesario & Higgins, 2008; Chernev, 2009).

Likewise, we predict that regulatory focus will have an impact on users' attitudes and judgments when making privacy decisions using preference settings. As privacy preference settings provide users with an opportunity to pursue goal attainment (be the goal privacy or social networking), users with a strong promotion focus are likely to have a favorable user experience when equipped with a decision support system that enables them to construct and specify a desired level of privacy/social networking. Specifically, an actor with a strong promotion focus is more likely to use preference settings as *eager strategic means* that enables the achievement of positive outcomes (optimal privacy and/or networking levels; ensuring "hits") and prevent the absence of positive outcomes (commission

bias; the preference not to close off possible advancements). Most privacy preference settings on social media (e.g., Facebook) provide users with multiple options (e.g., only me, friends only, public) and let them choose their desired option. A strong promotion focus, when matched with appropriate goal pursuit means, such as preference settings, leads to a regulatory fit.

As reviewed above, individuals feel right about their decisions when decision frames are compatible with their goal orientations. A strong regulatory focus, when matched with appropriate goal pursuit means, also leads to high engagement in tasks and an increase in processing fluency (Lee & Aaker, 2004), decreasing perceived effort and increasing both confidence (Cesario et al., 2004) and feelings of rightness or correctness (Cesario & Higgins, 2008). Hence, we predict that:

H4

a-c: Promotion focus will have a positive impact on (a) attitudes towards privacy setting use, (b) perceived effort, and (c) confidence when using privacy settings.

On the other hand, a prevention-focused user is likely to use privacy settings as *vigilant strategic means*. Use of privacy settings involves the risks of a "false alarm" or commission error, because users need to choose between conflicting goals with uncertain outcomes (Aquisti et al., 2015). People with a strong prevention focus prefer fewer alternative choices/hypotheses (Liberman et al., 2001) because having fewer choices makes it easier for them to eliminate or avoid mistakes/mismatches (e.g., commission error: taking actions when they are not right). Due to a strong focus on safety and loss aversion related to their prevention focus, prevention-focused people can also be more concerned about the risks of making a wrong choice (Chernev, 2004; Crowe & Higgins, 1997; Pham & Higgins, 2005). Because privacy decision making involves trade-offs and uncertainties, individuals with a strong prevention focus are likely to believe that using privacy preference settings to define their preferences takes a relatively higher degree of effort and is less favorable (omission bias: avoid mistakes, do not choose wrong ones), and to be less confident about their choices. Taken together, we predict that a prevention focus will produce a relatively weaker positive (or negative) impact on user experiences:

H5

a-c: A strong prevention focus will have a negative impact on (a) attitudes towards privacy setting use, (b) perceived effort, and (c) confidence when using privacy settings.

3. Study 1

In Study 1, we examined a baseline hypothesis (H1): the default effect on privacy preferences. Specifically, users' privacy preferences were predicted to be malleable such that users are likely to choose strict privacy preserving options when privacy-by-default is used, and promotion-enhancing options (e.g., higher levels of access) when the option shared-by-default is provided, although the two settings present a logically equivalent set of options to users. Facebook preference settings are labelled as "privacy settings and tools." This labelling itself can be a source of priming or the framing effect. As a result, we created two labels for preference settings, "privacy preference settings" and "networking preference settings" because users can adjust the levels of privacy and social networking simultaneously when using preference settings. Similarly, we also created two different names for a fictitious SNS ("SocialNET" and "Square") (a) to rule out potential confounding effects due to name; and (b) to explore whether the predicted default effect can be replicated across different contexts. Thus, a 2 (default settings) × 2 (labels) × 2 (names) between-subject design was used, though the focus of Study 1 was the main effect of default settings on privacy decision-making.

3.1. Method

3.1.1. Sample and procedures

We recruited participants through Amazon's MTurk. A total of 414 individuals (188 women, 45.4%) participated in this study for $1.00 each. Eligibility criteria were set to include those who are above 18 years old and who access their SNS account (e.g., Facebook, Google+, Instagram) at least once every

two weeks. Qualtrics, a research software, was employed for the online experiment. At first, participants were told that they had decided to use a new SNS named "SocialNET" (or "Square") because many of their friends had migrated to this fast-growing SNS. The new SNS was described as having useful features and personalization services: For instance, they could easily migrate all their friends lists, their profile, and their old posts from their existing SNS accounts to "SocialNET" (or "Square"). Before using "SocialNET," they were asked to set their "privacy" (or "networking") preference settings to define their preferences through a series of questions, such as "Who can see your future posts on your personal page?", "Who can post on your personal page?", and "Who can see posts/photos tagged?" The question set was adapted from current Facebook privacy preference settings. The three questions are conceptually related to interpersonal privacy boundary regulations regarding accessibility control, permeability management, and linkages control, respectively (Jia & Xu, 2016).

Default settings were manipulated by altering the preference settings in each question (see Appendix A). Half the participants were randomly assigned to the privacy-by-default condition in which the default and the first option was "Only Me." If a participant wanted to change her preferences to allow access to more people, she could click the pull-down menu, and alternative options appeared in the order of "Close Friends," "Friends," Friends of Friends," and "Everyone." In the shared-by-default condition, the default was reversed: The default was "Everyone," followed by "Friends of Friends," "Friends," "Close Friends," and "Only Me." Note that we wanted to emulate current Facebook privacy settings.

Labeling was manipulated by changing the name of preference settings (privacy preference settings versus network preference settings) in the instructions and the heading shown in each question. Naming was manipulated by changing the name of the SNS ("SocialNET" versus "Square") in a similar way.[1]

The dependent variable was users' choices for each question/decision (e.g., "Friends" versus "Only Me"). The dependent variable in the shared-by-default condition was recoded so that all levels had the same meaning across the board (1 = only me, 2 = close friends, 3 = friends, 4 = friends of friends, 5 = everyone). The experiment took between five and 7 min.

3.2. Results

We tested the default effect on privacy decision-making (H1) using ordinal regression analyses, because the dependent variable was an ordinal-level, multi-categorical variable. An assumption check using the test of parallel lines showed that the location parameters (slope coefficients) were the same across response categories.

The results of ordinal regression analyses confirmed the significant default effects on users' choices (H1). Table 1 summarizes the results. As Table 1 shows, the main effect of default setting was significant across the board. However, the main effect of labeling and naming was not significant. Hence, H1 was supported. We also observed significant two-way interactions between the default and label on two questions. As Table 1 shows, the ordered log-odds (logit) regression coefficients were negative across the board (baseline/reference group: shared-by-default), indicating that participants in the privacy-by-default condition were *less* likely to choose higher levels/categories (i.e., options favoring wider access) than those in the shared-by-default group. The odds ratio indicates the extent to which people chose higher levels when using preference settings. For instance, for the first question ("who can see your future posts on your personal page?), the odds of those in the privacy-by-default group choosing higher levels of access decreased by about four fifths (.22). In other words, those in the *shared-by-default* group were nearly four times more likely to allow *higher* levels of access/permeability than those in the *privacy-by-default* group.

Note that the pseudo R^2 values were relatively low (ranging from 0.04 to 0.08). This is not too surprising, because there are other factors that influence users' preferences, many of which will be much more important predictors of user preferences than any subtle default effects. The low R^2 suggests that a research model with only default-related factors should be a poor model to predict the response patterns for any particular *individual user.* However, the low R^2 does not refute the finding that there is a statistically significant difference in the *average* user preference levels between different default settings.

We noticed that 87–89 percent of people chose the non-defaults in Study 1. We wanted to further examine whether the default effects could be observed from those who actively chose non-default options that varied in terms of their proximity to the status quo. To do this, we filtered out those who maintained the defaults (either "Only Me" or "Everyone") and tested the default effect (see Table 1.1 for the results). The effect size ranged from −1.06 to −1.59, and all of them remained statistically significant. Overall, it appears that the defaults also had an effect for those who chose non-defaults, by pulling their choices toward the default option. The results suggest that inertia or inattentiveness cannot be the sole reason for the default effect observed in this study, because people who chose alternatives were also influenced by the default setting (i.e., reference category).[2]

Table 1. Results of ordinal regression analyses predicting privacy preference levels (study 1).Results omitting those who chose default settings.

	Default (D)	**Label (L)**	**Name (N)**	**D × L**	**D × N**	**L × N**	**D × L × N**	**Pseudo R^2***
1. Who can see your future posts?	−1.53***	-.52	–.65	1.18*	1.10	.99	−1.28	.05
2. Who can see posts & photos tagged?	–.50	-.37	.18	.56	–.70	.49	.08	.04
3. Who can post on your personal page?	−1.75***	-.14	-.08	1.35*	.74	.09	-.94	.08

	Default	**Pseudo R^2***
1. Who can see your future post?	−1.59**	.06
2. Who can see posts and photos tagged?	−1.06*	.08
3. Who can post on your personal page?	−1.12***	.04

Notes.

1. Coefficients in the table are the ordered log-odds (logit) regression coefficients.

2. Pseudo R^2 is assessed by Nagelkerke measure.
3. Baseline (reference) groups are: Default (shared-by-default [1]), Label (privacy preference [1]), Name (Square [1]). SPSS chooses the last category as a reference category.

4. * <0.05, ** <0.01, *** <0.001.

* <0.05, ** <0.01, *** <0.001.

Overall, the findings confirm a strong default effect: Users' choices can be easily shifted by subtle changes of default settings, even though a logically equivalent set of options are presented to them. A limitation of Study 1, however, involves the small effect size observed in this study. What remains unclear, therefore, is whether the findings are replicable and robust. Given the recent controversies about the reproducibility of psychological findings (Open Science Collaboration, 2015), it is worthwhile to retest the robustness of the default effect found in study 1. In addition, study 1 focused on the main effect of default settings despite there might be other important individual factors that influence users' choices, and the default effect may be contingent upon them. Finally, Study 1 focused on behavioral outcomes, though judgmental factors are also crucial in a decision-making context. Thus, we conducted study 2 with three goals in mind: (a) to garner additional support for the default effect on privacy decision-making; (b) to further investigate the potential role of regulatory focus as an individual trait; and (c) to examine the default effect on additional outcome dimensions such as attitudes, perceived effort, and confidence.

4. Study 2

4.1. Method

4.1.1. Sample and procedures

We conducted Study 2, which is similar to Study 1 but has an additional focus on regulatory focus as a measured variable, and attitudes, perceived effort, and confidence as dependent variables. Similar to Study 1, default and labeling were included as independent, manipulated variables. Note that we used only one name ("SocialNET") in Study 2, because naming did not have any main or interaction effects in Study 1.

A total of 217 participants were recruited through Amazon's MTurk, at a cost of $.50 each. After omitting four unreliable responses using an attention-check question, the final data consist of 213 participants (90 women, 42.3%). We aimed to recruit at least 200 participants. This *N* was calculated using the "pwr2" package in R (Lu, Liu, & Koestler, 2017). This *N* is expected to provide 80% power for detecting an effect size of 0.20 for the two factors (here, default and label) with two levels in balanced design, assuming a type 1 error rate of 0.05. This effect size is based on results provided by Study 1, which had a small effect size. By assuming this conservative effect size, the required per-cell *n* for 80% power is 50, with 4 cells, requiring a total *N* of 200. The procedures were similar to those used in Study 1. After reading the instructions, participants defined their preferences through a series of questions using either privacy-by-default ("Only Me" first) or shared-by-default ("Everyone" first). After this, they answered questions assessing attitudes, confidence, perceived effort, and regulatory focus. The online experiment took between seven and 10 min.

4.1.2. Measures

Attitudes toward preference settings were assessed using a 3-item scale (M = 3.49; SD = 0.82;.α = 0.90) adapted from Igbaria, Livari, and Maragahh (1995). *Perceived effort* was assessed by a 4-item scale (M = 4.38; SD = 0.55; α = 0.88) and *confidence* in decision-making by a single item scale (M = 4.23; SD = 0.66), both adapted from Knijnenburg and Kobsa (2014). Scores of perceived effort were reversed to represent *lesser* cognitive effort so that all outcome variables could have positive valence in a decision context. Regulatory focus was measured by RFQ (Higgins et al., 2001). Promotion focus was assessed by a 5-item scale (M = 3.45; SD = 0.57; α = 0.69) and prevention focus by a 5-item scale (M = 3.44; SD = 0.67; α = 0.83). Privacy concern was measured by 8-item scale (M = 3.44; SD = 0.88; α = 0.91) adapted from Stewart and Segars (2002). The multiple-item scales were combined by using mean scores.

5. Results

5.1. Behavioral impact (H1-H3)

H1 and H2 predicted the main effects of default setting and regulatory focus on users' preferences, respectively, and H3 predicted an interaction effect between default setting and regulatory focus. To test these hypotheses, we conducted ordinal regression analyses. Regulatory focus theory assumes that promotion focus and prevention focus are not bipolar constructs because people can have high levels of both foci simultaneously (Higgins, 2011). However, using two regulatory foci simultaneously and testing interaction effects between multiple independent factors created many empty cells when conducting ordinal regression analyses. Hence, following Higgins et al. (2001), we created a dummy variable assessing relative regulatory focus by computing the difference in scores between promotion focus and prevention focus and using the median split for this variable (0 = relatively more prevention focused, 1 = relatively more promotion focused).

Table 2 summarizes the results of ordinal regression analyses. We observed a significant main effect of default settings on three choice questions. Similar to the results of Study 1, the baseline group was "shared-by-default" and the ordered log-odds (logit) regression coefficients were all negative, indicating that participants were significantly less likely to choose higher levels of access/permeability when using privacy-by-default. Hence, H1 was supported. The findings from Study 1 were replicated in Study 2.

Table 2. Results of ordinal regression analyses predicting privacy preference levels (study 2).

	Default (D)	**Label (L)**	**Regulatory Focus (RF)**	**D × L**	**D × RF**	**L × RF**	**Pseudo R^2***
Who can see your future posts?	−1.33**	–.44	−1.07*	.46	.46	1.13*	.09
Who can see posts & photos tagged?	−1.40**	–.04	.08	.35	.51	–.10	.08
Who can post on your personal page?	−1.31***	–.87	–.60	.42	.34	.41	.07

Notes.

1. Coefficients in the table are the ordered log-odds (logit) regression coefficients.

2. Pseudo R^2 is assessed by Nagelkerke measure.
3. Baseline (reference) groups: Default (shared-by-default), Label (privacy preference), Regulatory focus (Promotion focus).

4. * <0.05, ** <0.01, *** <0.001.

The main effect of regulatory focus on one choice item ("Who can see your future posts?") was significant. The baseline group was promotion focus and the coefficient was negative (−1.33, $p < .01$), indicating that individuals with a relatively higher prevention focus were less likely to choose higher levels of access/permeability. However, the effect of regulatory focus on the other two outcome variables was not significant. Hence, the results partially supported H2. Finally, the interaction effect between default and regulatory focus was not significant across the board. Therefore, H3 was not supported.

5.1.1. Impacts on attitudes and judgments (H4-H5)

We ran ordinary least square (OLS) regression analyses predicting the effect of promotion focus (H4) and prevention focus (H5) on three attitudinal or judgmental outcomes: (a) attitudes; (b) perceived effort; and (c) confidence. We included both foci—promotion focus and prevention focus—as

separate variables in our OLS regression models because we no longer must deal with empty cell problems observed in ordinal regression analyses. The results of preliminary analyses also showed that prevention focus had significant two-way interaction effects (prevention × default and prevention × label). As a result, in our final regression model, we report interaction effects involving prevention focus, though they were not predicted in our original hypotheses. On the other hand, promotion focus did not have any interaction effects. Because interaction terms involving promotion focus were neither hypothesized nor statistically significant, they were not added to the final model to avoid overfitting in regression analyses with an overly-complicated model. To examine interaction effects, we used the Process Macro in which interaction terms were created using a product indicator approach (Hayes, 2013).

The results (see Table 3 for details) showed that a promotion focus had a significant and positive effect on attitudes (b = 0.36, t = −3.72, p < .001), perceived (lesser) effort (b = 0.22, t = 3.55, p < .001), and confidence (b = 0.29, t = 3.74, p < .001). Hence, H4a, H4b, and H4c were all fully supported. The effect of a prevention focus on attitudes (b = −0.16, t = −1.98, p = .049), perceived (lesser) effort (b = 0.18, t = 3.38, p < .001), and confidence (b = 0.07, t = 1.03, p = .30) was less pronounced. In addition, the effect of prevention focus on attitudes, perceived effort, and confidence was also contingent on label and default. Hence, H5 was partially supported.

Table 3. Results of moderated regression analyses.

	Dependent Variables		
	Attitude	**Lesser Effort**	**Confidence**
	b (SE)	*b* (SE)	*b* (SE)
Default (D)	–.15 (.11)	–.13 (.07)	–.10 (.09)
Label (L)	–.09 (.11)	–.03 (.07)	.03 (.09)
Promotion focus (Pr)	.36 (.10)***	.22 (.06)***	.29 (.08)***
Prevention focus (Pv)	–.16 (.08)*	.18 (.05)***	.07 (.07)
D × L	.04 (.22)	–.10 (.14)	–.19 (.18)
D × Pv	–.05 (.16)	.27 (.11)*	.29 (.13)*
L × Pv	.38 (.16)*	–.09 (.10)	–.06 (.13)
D × L × Pv	.29 (.33)	.33 (.21)	.12 (.26)
% explained (R^2)	R^2 = .12	R^2 = .18	R^2 = .11

Notes.

1. Base group (Default = Privacy-by-default [0]; Label = networking preference [0]): The Process Macro, by default, chooses the smallest number as a reference category.

2. Variables for product terms were mean centered.

3. * <0.05, ** <0.01, *** <0.001.

We further probed the patterns of significant two-way interaction effects observed in Study 2 using techniques described by Aiken and West (1991) (see Appendix B for interaction plots). Note that the results are post-hoc findings. Fig. 1a describes the patterns of a two-way interaction between prevention focus and label. The analysis revealed that participants low in prevention focus (operationalized as $M - 1SD$) reported significantly greater positive attitudes when preference settings were labelled as "networking" relative to "privacy" ($b = -0.34$, $t = -2.21$, $p = .03$). In contrast, this effect was not observed among participants high in prevention focus ($M + 1SD$), $b = 0.17$, $t = 1.08$, $p = .28$. We also applied the Johnson–Neyman procedure (Bauer & Curran, 2005; Johnson & Fay, 1950; Johnson & Neyman, 1936) to identify the transition pointer between significance and non-significance of the conditional effect, which is denoted in Fig. 1 with a vertical line. The Johnson–Neyman point was −0.69 *SD*. Complementing this spotlight analysis, a simple-slopes analysis suggested that this interaction was mainly driven by judgments about "network" preference settings. While the prevention focus significantly predicted attitudes for the "networking" setting ($b = -0.36$, $t = -3.19$, $p < .001$), this relationship was not observed for the "privacy" setting ($t < 1$, $p = .86$). It appears that the potential match between reduced concern for prevention focus and a label (emphasizing promotion of a gain: social networking) led to a positive effect on attitudes.

The interaction between prevention focus and default setting on perceived effort and on confidence are shown in Fig. 1b and c, respectively. As Fig. 1b shows, participants low in prevention ($M - 1SD$) focus reported significantly less perceived effort when privacy-by-default ("Only Me" first) was employed, compared to shared-by-default ("Everyone" first), $b = -0.31$, $t = -3.04$, $p < .001$. Yet, such effect was not found among participants high in prevention focus ($M + 1SD$), $t < 1$, $p = .67$. The Johnson–Neyman point that differentiates between significance and non-significance of the conditional effect was −0.19 *SD*. A simple-slopes analysis further revealed that the interaction effect is driven by participants using shared-by-default settings. The prevention focus significantly predicted the perceived effort among participants who viewed the shared-by-default settings ($b = 0.30$, $t = 4.28$, $p < .001$), but not those who viewed the privacy-by-default settings ($t < 1$, $p = .73$). We observed a similar pattern for confidence (Fig. 1c). Participants low in prevention focus ($M - 1SD$) reported significantly greater confidence when privacy-by-default settings were employed, compared with when shared-by-default settings were given, $b = -0.30$, $t = -2.36$, $p = .02$. Again, this effect was not found among participants high in prevention focus ($M + 1SD$), $t < 1$, $p = .44$. The Johnson–Neyman point was −1.01 *SD.* A simple-slopes analysis showed that the interaction effect is primarily driven by participants using shared-by-default settings. The prevention focus predicted the confidence among participants who saw shared-by-default settings ($b = 0.20$, $t = 2.27$, $p = .02$), but not those who saw privacy-by-default settings ($b = -0.10$, $t = -0.95$, $p = .34$). We elaborate on the results in the following section.

In summary, in study 2, the default effect on users' preferences was replicated (H1). Regulatory focus also has a significant impact on a behavioral choice item (H2), and both a significant main effect and significant interaction effects on attitudes and judgmental outcomes (H3 & H4). The findings suggest that default effects are robust. In addition, users' goal/motivational orientations (i.e., regulatory focus) play an important role in shaping users' choice as well as their judgments.

6. Discussion

The aim of this study is to examine the ways in which social media users construct their privacy (networking) preferences, focusing on the effect of a contextual factor (default settings) and an individual difference factor (regulatory focus) and the interplay between them.

In both studies (study 1 and study 2), we found that default settings have a significant effect on users' preferences across different conditions. Specifically, in study 1, the results support H1, which predicts a significant default effect on users' privacy decision-making. When privacy-by-default was given ("Only Me" first), users' choices were more privacy-oriented (i.e., restricted access). Conversely, users were more likely to allow higher levels of access/permeability (i.e., wider audience group) when the default frame was reversed to shared-by-default ("Everyone" first). It is important to note that a majority of participants did not select the defaults, but their choices were still close to the defaults. In other words, the default effect was observed even for those who chose non-defaults. The findings can be explained by the endowment effect (Baron & Ritov, 1994; Tversky & Kahneman, 1981), or by a focus-of-comparison effect (Dhar & Simonson, 1992) that suggests that outcomes are not only evaluated on their absolute value but also on their deviation from a reference (an initial, starting) point (Sher & McKenzie, 2006). Because people have loss aversion, and because the default is perceived to be endowed or implicated recommended, options far from the default would be less preferred. Hence, people preferred options close to the default even when they opted for non-default options.

In study 2, the baseline, main effect of default is replicated, demonstrating the robustness of default effect on privacy decision-making. In addition to the main effect of default settings, study 2 examined regulatory focus. The results indicate that regulatory focus is an important motivational factor that researchers need to consider when examining users' privacy-related decision-making. Consistent with regulatory focus theory (Higgins, 1997, 2011) promotion focus and prevention focus have distinct relationships with decisional outcomes. Promotion focus has a significant impact on a single choice (behavioral) item. It also has a positive impact on attitudinal and judgmental outcomes, regardless of default settings. A possible reason for this is that promotion-focused individuals are likely to perceive preference settings use as an eager strategic means allowing them to define their desired states, be they social networking or privacy enhancement.

On the other hand, the effect of prevention focus is more complicated and contingent on decision frames. As noted earlier, the interaction effect between prevention focus and label is relatively easy to interpret: a congruence between a reduced prevention focus and the label emphasizing gains/advancements (i.e., social networking) can lead to positive attitudes.[3]

The two-way interaction effect between prevention focus and default on perceived effort and confidence warrants more careful interpretations. To recap, a prevention focus is positively associated with favorable user experiences in the shared-by-default condition but not in the privacy-by-default condition. Intuitively, one can expect the opposite pattern: higher levels of prevention focus should be positively associated with favorable judgmental outcomes upon using ***privacy***-by-default settings rather than shared-by-default settings due to its orientation towards safety. These seemingly counterintuitive findings can be explained by regulatory focus theory (Higgins, 1997) and the "focus-of-evaluation" effect (Dhar & Simonson, 1992; Sher & McKenzie, 2006). In the shared-by-default condition, the point of reference (the status quo, the initial point) for users was "Everyone." Given that most users chose alternative options departing from the default, the deviation from the default can be conceived of as increasing privacy protection in comparison with the reference ("Everyone," the lowest level of privacy protection). People with a strong prevention orientation focus on an undesired end-state and use vigilance strategies to move away from it (avoidance) (Pham & Higgins, 2005). Since individuals with a strong prevention focus are sensitive to security and safety, these acts (departure from shared-by-default, an undesirable initial point) appear to have a positive impact on users' judgments, as they chose stricter privacy options, abandoning the shared-by-default. The findings suggest that a deeper theoretical understanding of users—including their goal orientations and underlying processes involved in decision-making—would greatly facilitate researchers and practitioners in understanding users and their privacy decisions.

With regards to H3, we did not find support for the moderating effect of regulatory focus on the association between defaults and preference. In contrast, Craciun (2018) has demonstrated a significant moderating effect such that default effects are more pronounced for prevention-focused individuals than for promotion-focused ones. A possible reason for these different results would be that two studies are different in terms of context (e-commerce versus SNSs) and the nature of outcomes (monetary versus non-monetary rewards). Another potential explanation could be the lower power of this study because we tested several options whereas Craciun (2018) tested dichotomous options (disclose or non-disclose). Given that there is a dearth of privacy studies examining the role of regulatory focus, we suggest that it should be worthwhile to continue to explore the effect of regulatory focus on privacy-related attitudes and behavior across different contexts. We also suggest that future studies should revisit this research topic to specify the conditions under which regulatory focus plays varying roles in privacy decision-making.

We performed additional post-hoc tests to determine whether the default effect observed in this study is contingent on other motivational factors, such as issue involvement (operationalized as privacy concern). Heuristic information processing and cognitive biases have a weaker impact when decision makers are strongly involved in an issue at hand (Wang & Lee, 2006). As such, privacy concerns as a proxy of involvement can be a moderator of default effect (Park, June, & Macinnis, 2000). However, the results of preliminary analyses showed that privacy concern did not have any significant main or interaction effects on the outcome. Hence, we omit privacy concern from our final model. The nonsignificant main effect of privacy concern on privacy decision-making is unexpected. However, the results are not too surprising given that the association between privacy concern and privacy-related behavior has been found to be inconsistent in many previous studies (see Kokolakis, 2017 for a review on privacy paradox).

6.1. Implications for research

Overall, our findings suggest that simple alterations of the status quo and the order of the other options being presented shift users' choices, even though the two situations are logically equivalent. Previous studies have shown that when people are given a choice task, their preferences are often constructed rather than generated by stable preferences. In other words, "preferences do not come readily from a list in memory, nor are they generated by some invariant algorithm" such as expected value calculation (Wang & Lee, 2006, p. 29). Numerous studies have examined privacy decision-making using a rational-choice approach, such as privacy calculus (e.g., Dienlin & Metzger, 2016) and cognitive appraisals of threat and coping (e.g., Li, Juo, Zhang, & Xu, 2017). Our findings confirm that privacy decisions are *situated* in contexts and that privacy preference settings are an important contextual factor as they inherently involve decision frames.

One could argue that default effects are observed in this study because many participants simply did not change default settings and clicked the "next" button to complete a task. However, when we re-examined default effects on those who selected alternatives (nearly 90 percent of participants), a significant default effect was still observed to the extent that people chose options proximal to the default. Previous studies on privacy default effects operationalized privacy decisions as a binary choice (default versus non-default). As a result, users' choice of the non-default option was conceived of as the absence of the default effect. In this study, we employed a more granular approach by examining users' choices in multiple, alternative options. We find that default effects exist even when people actively seek out other options. The results suggest that inattentiveness or effort cannot alone explain the default effect for most people. It would be useful to study further theoretical mechanisms, such as reference-dependent choice, endowment effect, or the focus of evaluation (Dhar & Simonson, 1992; Tversky & Kahneman, 1981), to gain a complete understanding of privacy default effects.

In Study 2, we employed regulatory focus theory to specify conditions under which defaults have differing implications for users with different goal orientations. The results demonstrate the significant impact of regulatory focus on privacy decisions, particularly on judgmental factors. These relationships are also contingent on a degree of fit between default setting (or labels) and regulatory focus. Overall, the findings demonstrate that regulatory focus theory and its related concepts, such as regulatory fit (Higgins, 2011), provide a useful theoretical framework in which to examine the effects of users' goals and goal orientations in privacy decision-making.

Previous studies have examined regulatory focus in a variety of contexts, such as the effects of regulatory focus on attitude change and processing fluency (Aaker & Lee, 2001) and on behavioral intention to undertake an advocated action (Zhao & Pechmann, 2007). Though a few studies (Lwin et al., 2016; Mosteller & Poddar, 2017) have borrowed the concept of regulatory focus to suggest the difference between promotion-oriented privacy constructs (e.g., information disclosure) and prevention-oriented ones (e.g., privacy concerns and privacy protection), limited research has directly measured or manipulated regulatory focus to examine its impact on privacy decisions (see Craciun, 2018 for exception). A combination of default effects and regulatory focus, as demonstrated in this study, provides us with a powerful tool with which to examine the interplay between contextual factors and individual factors or to specify conditions under which these factors have a positive, negative, or nonsignificant effect on social media users. As such, we suggest that building a bridge between privacy research, default effect, and regulatory focus literature offers potential to give rise to useful approaches toward researching online privacy.

6.2. Practical implications

Besides the aforementioned implications for research and theory, the findings also have some useful practical implications. SNS providers offer new and updated privacy settings to give users better control of their information privacy. For instance, Facebook quickly introduced a refreshed privacy settings after the Cambridge Analytica Scandal (New York Times, 2018b). However, people seldom modify or manage privacy settings (Gross & Acquisti, 2005; Lipford et al., 2008**)**. Possible reasons for this under-utilization of privacy options include poor interface design, generalized trust in the online community, and a lack of motivation (Gross & Acquisti, 2005). Further, our findings show that the construction of privacy preferences are influenced by the inherent default effects, which may violate users' autonomy even when they are given choices through privacy settings. Studies have shown that social media users find the privacy settings confusing and time-consuming (Lipford et al., 2008) and that perceived difficulty leads people to use choice heuristics like default effects (Lee & Benbasat, 2011). As such, usability is an important factor that practitioners should consider when aiming to enhance users' willingness or ability to put forth the effort to manage their information privacy using privacy settings. Given the strong default effects on users' privacy decision-making, we suggest that practitioners and designers should test different privacy interfaces and management tools to figure out ways to empower or assist users: for instance, the pros and cons of providing more granular options for users; the effectiveness of feedback systems that allow users to check whether their decisions are in line with their actual (or implicit) privacy preferences; visualization systems displaying the impact of users' privacy preference settings on the visibility and searchability of their profiles; or a machine-learning approach that allows high-accuracy privacy settings using less user input than existing policy-specification tools.

6.3. Limitations and directions for future studies

There are several limitations of this study. First, though most hypotheses are supported in this study, overall effect sizes are relatively small. The robustness of the results should be further examined in subsequent studies. Second, research design is based on a hypothetical scenario. For some participants, this scenario-based experiment might be unrealistic, and their decision-making process could have been different in real-life contexts. Third, as mentioned earlier, there are at least several

theoretical mechanisms simultaneously involved in default effects. Specifying which process is more accountable for the observed effect would be necessary for future research. The use of process measures, such as verbal protocols or eye movement tracking measures, might be useful to improve our understanding of potential theoretical mechanisms, such as the focus-of-evaluation effect.

7. Conclusions

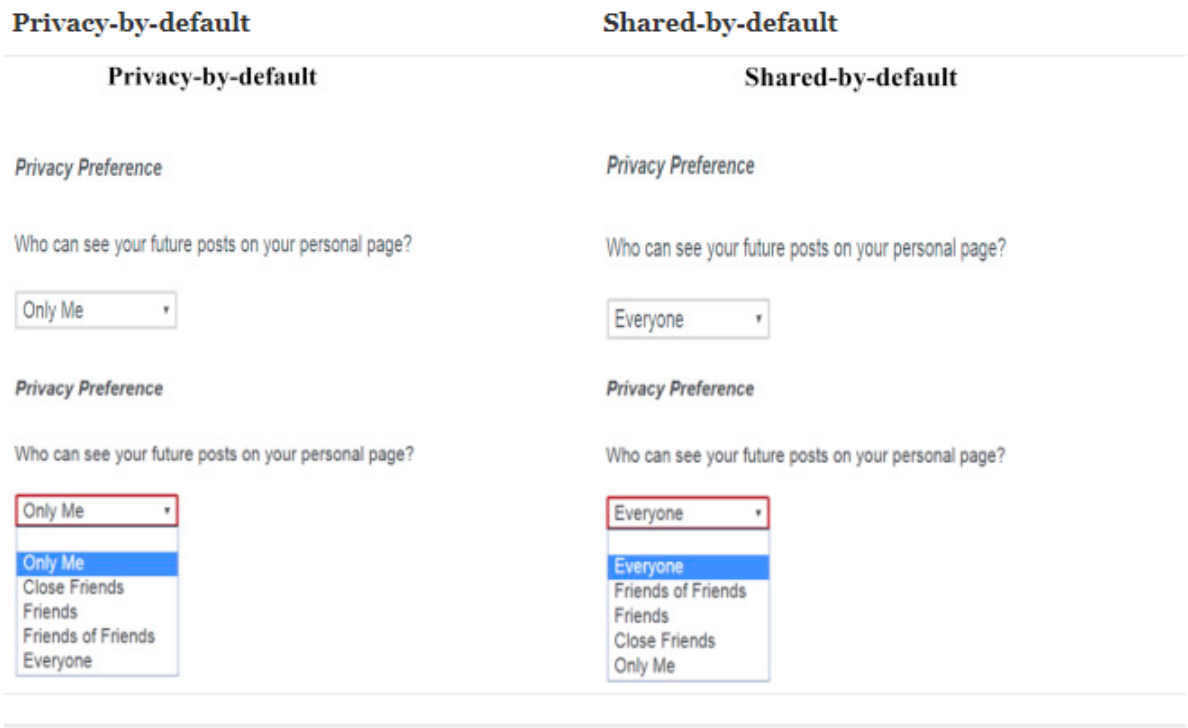
Despite the shortcomings of this research, we believe that our study offers valuable insights about users' judgments and decision-making related to privacy and social networking. Information privacy is a key factor influencing how media users determine their interpersonal boundaries (Jia & Xu, 2016) and level of self-disclosure (Dienlin & Metzger, 2016), and how they use of new communication technologies (Pew Research Center, 2018). In this study, we suggest a novel approach to examining privacy decision-making by combining default effect and regulatory focus theory, with which we specify the ways in which users' choices are influenced by both a contextual factor (default settings), an individual factor (goal orientation: regulatory focus), and an interaction between them. The implications of defaults cannot be ignored, because "even when consequence are benign, default manipulations can violate consumer autonomy" (Smith, Goldstein, & Johnson, 2013, p. 169). As such, we suggest that more theoretical and empirical investigations are needed to better understand why default effects exist in the context of privacy decision-making, or when the default effect can be intensified or reduced. We hope concerted research efforts to be continued so as to find powerful ways of understanding and assisting privacy decision-making in today's complex communication environment.

7.1. Notes

1. Note that we omitted manipulation checks because when "independent variable construct and its operationalizing are completely identical, a manipulation check would be unnecessary" (Mutz & Pemantle, 2015, p. 2). Manipulation checks are necessary when a study employs operations (e.g., a message) to manipulate a theoretical construct (information fluency) that cannot be manipulated directly. In our study, IVs (default and name) were directly manipulated, and they are identical to their operational definitions. Likewise, manipulation checks are omitted in most studies about default effects (e.g., Johnson et al., 2002; Lai & Hui, 2006) and reference points and omission bias (e.g., Baron & Ritov, 1994). Manipulation checks for labeling were done in a separate study, and the results showed that the manipulation was successful in that differences in perceived privacy/networking management in two different labeling conditions were significant ($t = 3.90$, $p < .001$; $t = 5.63$, $p < .001$).
2. As a post-hoc analysis, we explored in which condition users are more likely to choose the default options. We transformed the choice set answers (DV) into dichotomous variables (1 = default, 2 = non-default) and performed logistic analyses using three experimental conditions as IVs. The results showed that three factors had a nonsignificant effect on whether or not people choose the defaults, except for one choice question ("who can post on your personal page?"). For this question, people are more likely to choose the default option in the privacy-by-default condition than in the shared-by-default condition ($\beta = .-0.85$, $p < .01$). Other than that, the results suggest that the tendency for people to choose the defaults (due to inertia, laziness, or anchoring) is not affected by the label, name, or default settings. Note that the nonsignificant results are not contradictory to the main findings in study 1. That is, people choose the defaults (or alternatives proximal to them) in *both* default settings (privacy-by-default versus shared-by-default), resulting in marked reversals in their decision outcomes depending on how a set of choices are framed.
3.

Interestingly, such an interaction effect is not observed for promotion focus. A possible reason is that a strong positive effect of promotion focus favoring choice and change overrides a potential moderation effect.

Appendix A. Screenshots of default settings (Pull-down menu appears when a user clicks it)



Appendix B. Interaction plots for prevention focus, label, and default settings

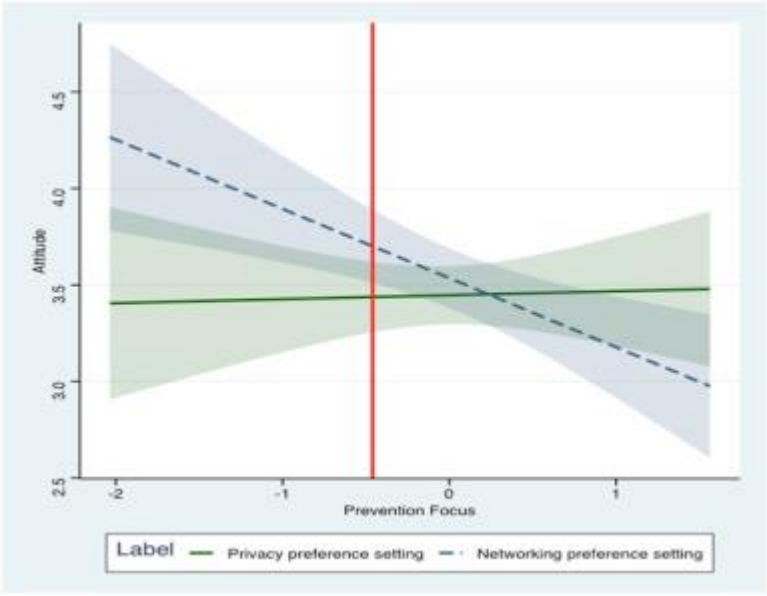


Fig. 1a. Attitude (Prevention × Label) Note: The shaded areas denote 95% confidence intervals. The vertical line marks the boundary between regions of significance and non-significance based on α = 5% .

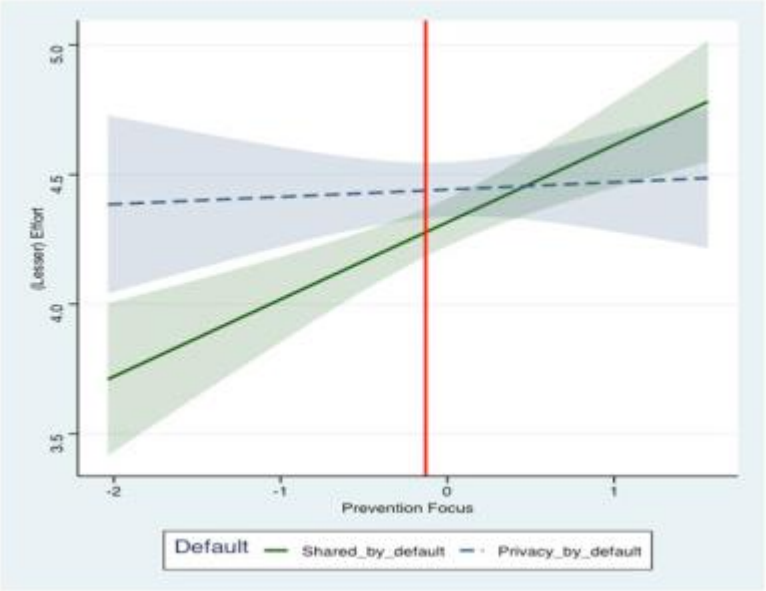


Fig. 1b. Perceived effort (Prevention × Default) Note: The shaded areas denote 95% confidence intervals. The vertical line marks the boundary between regions of significance and non-significance based on α = 5% .

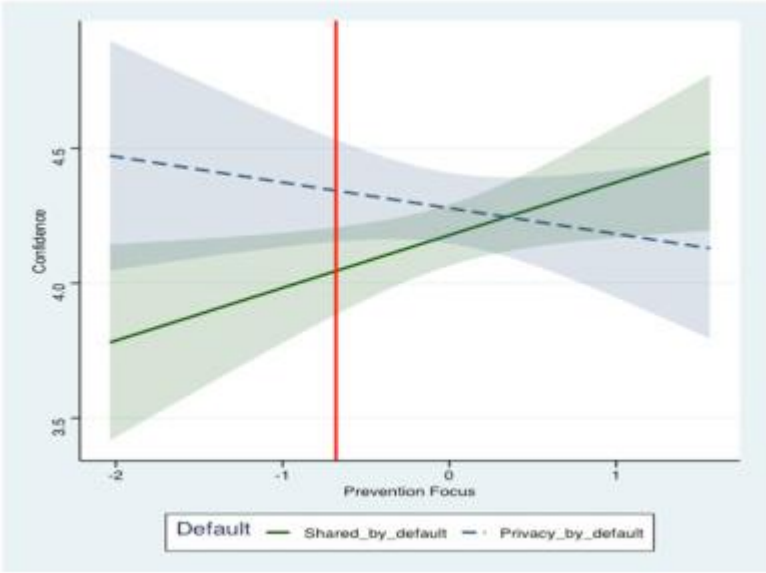


Fig. 1c. Confidence (Prevention × Default) Note: The shaded areas denote 95% confidence intervals. The vertical line marks the boundary between regions of significance and non-significance based on α = 5% .

Supplementary data to this article can be found online at https://doi.org/10.1016/j.chb.2019.07.001.