Telematics and Informatics 66 (2022) 101748

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

# Personal data concern, behavioral puzzle and uncertainty in the age of digital surveillance

Yong Jin Park [*]

*Howard University, School of Communications, United States*

ARTICLE INFO

*Keywords:*
Data privacy
Surveillance
Privacy concern
Personal information

ABSTRACT

Using U.S. national panel surveys conducted, this study organizes three-related analyses to examine puzzling responses to data concern. Each of three analyses shows that people have distinctive heuristic structures that are “hardwired” for quick judgements as they filter, interpret, and retain cues in their release of personal data. Analysis 1 examines a non-linear pattern of behavioral responses to varying intensity of concern. Analysis 2 investigates indirect relationships between concern and data surrender. Analysis 3 examines temporal incongruence as one’s protective action can be delayed over time. Findings across three analyses corroborate the insight that readily-accessible cognitive judgements help reduce the difficulty of estimating the likelihood of privacy gain and loss into a set of simple principles. This study concludes by cautiously warning the digital entrenchment of surveillance in that when a data consideration is reduced to a quick moment of choice, privacy can be over-released, surrendered over gratification, and eventually deferred to inaction.

## 1. Introduction

Will people ever take actions to protect their privacy? Acquisti et al. (2015) offered a compelling account:

> Privacy decision-making is only in part the result of a rational “calculus” of costs and benefits; it is also affected by misperceptions of those costs and benefits, as well as social norms, emotions, and heuristics. Any of these factors may affect behavior differently from how they affect attitudes. (p. 510).

This is a persuasive account in describing how a web of privacy-related emotion, concern, and uncertainty muzzle individual rationality related to information behavior. Complex functions of privacy attitudes, namely concern, have been explained in diverse streams of behavioral economic literature (Barth and De Jong, 2017; Brandimarte et al., 2013; Dienlin et al., 2019; Hargittai and Marwick, 2016; Masur and Trepte, 2021). However, empirical evidence is paradoxical at best as studies (Hoffmann et al., 2016; Paine et al., 2007) show that people take little action when they express concern about their personal information.

The present study is about this puzzle of privacy paradox, with the conceptual aim to highlight cognitive factors that influence behavioral decisions related to privacy protection and release. For this, this study suggests the three heuristics—(1) non-linearity, (2) indirect relationship, and (3) temporality—and tests the extent to which each of these heuristic principles explains the dichotomy between data privacy concern and behavior. Arguing from a purely rational perspective, economists have been testing somewhat

[*] Address: 525 Bryant St NW, Washington, DC 20059, United States
*E-mail address:* yongjinp@hotmail.com.

https://doi.org/10.1016/j.tele.2021.101748
Received 20 May 2021; Received in revised form 3 October 2021; Accepted 15 November 2021
Available online 26 November 2021

deterministic models of rational choice in guiding their behavioral calculation (Marcus et al., 2000). The puzzle found in behavioral function of privacy concern, however, suggests that the privilege of human rationality rarely runs its course, guided by bounded judgement toward uncertain future outcomes and events (Neuman, 2016; Tversky and Kahneman, 1974).

Recent studies in the field of information science (Dienlin and Metzger, 2016; Shin, 2020; Sundar, 2008) raised questions about the extent of rationality in explaining informational behavior as individuals pivot their judgement to simple sets of calculus rules. In the last few years, there has been also an enriched set of studies on this issue (Baruh et al., 2017; Gerber et al., 2018), looking at the role of dark patterns (Waldman, 2020) or cognitive heuristics (Gambino et al., 2016). In complex digital environments abound with constant influx of information, people face fundamental decisions in regards to whether they take systematic-central reasoning that requires deep consideration or heuristic peripheral-habitual processing of mental shortcuts that often guide decisions (Neuman et al., 2007). This study aims to fit into this great line of studies that explain the privacy paradox, but adding insights to this debate about how individual rationality, reliant upon heuristic principles, will hamper privacy-related decisions.

Analytical goal of this study is to capture a snapshot of public minds, providing a glimpse at how the omnipresence of digital citizenship is emerging from hyper-personal, mobile, and data-intensive environments. The use of three-wave online panel surveys (2014–2015) is warranted to gain insights on how public concern might channel into behavioral responses, manifest via personal data release and protection, to surveillance fear. Findings across each of three analyses corroborate the insight that readily-accessible cognitive judgements efficiently reduce the difficulty of estimating the likelihood of privacy gain and loss into a set of heuristic principles—recognized in this study as (1) non-linearity, (2) indirect relationship, and (3) temporality. The normative implication of these findings, however, is that inner workings of heuristics inhibit opportunities for fostering competent citizens, with their deleterious consequences on under-protection and over-disclosure of privacy as information decisions in digital landscapes depend ever more upon 'quick and easy' personal judgement.

## 2. Heuristics of mental personal-data shortcut

One might wonder how the expectation over the loss of privacy rarely factors into people's behavioral decision, especially when concern is explicitly expressed (Masur and Trepte, 2021). The apparent disregard for potential gain of privacy seems at odds with the image of a rational human being who is capable of making decisions regarding information release. Yet in explaining this oddity, we can draw upon heuristics—mental principles of assessing the likelihood of uncertain behavioral outcomes.

Heuristic is a psychological shortcut in which people reduce complex cost-benefit calculation to quick sets of mental judgements that are readily accessible in their cognition. It enables people to forego systematic reasoning of uncertain events, which can, not only exhaust their cognitive resources, but also be time-consuming. By assigning values to immediately available cues or convenience at moment, individuals' choices are optimized for minimizing the cognitive demand for active behavioral involvement (Acquisti et al., 2015; Neuman, 1991). The habitual reliance of heuristics, no matter how economizing (thus, rational) it may be, provides clues on (1) the function of privacy paradox, i.e. the extent to which privacy concern can (cannot) be translated into meaningful actions, and thus, (2) how to reverse its intuitive course of personal data-related action. In fact, social psychologists (Simon, 1955) applied heuristics in understanding human decision making in various domains. The traditional rational choice model of political behavior, for instance, has been challenged on the ground that there is no empirical support for attentive and thoughtful voters engaging in rational evaluations of costs and benefits that are congruent to their self-interest (Marcus et al., 2000). Instead, understandings of political decision have been qualified to suggest that a citizen's behavior is a product of bounded rationality, as the deliberate consideration for systematic choices and appropriate corrections are not general but specific cases.

The insight is equally applicable in understanding the puzzle of privacy. At best, the behavioral function of concern is largely inconsistent or even contradictory as people browse through quick guiding principles for their action. Simply put, it is unlikely for a person to invest time and energy to exercise deliberate ways of releasing personal information, when she continuously confronts similar issues in everyday routines. Keeping cognitive calculation at a minimum is not only attractive but also a rational option as no immediate harm or loss is discernible in recurring situations. In this vein, this study calls for qualifications understandings of privacy paradox, posing a new set of questions about underlying heuristic principles in explaining the dichotomy between privacy attitudes and behavior.

First, the thrust of any effect focused on discerning a linear relationship between concern and behavior. Statistical properties of linear slope (β), however, can throw away levels of variation, as each level of concern may not be linearly staked up against behavioral responses. The expectation that a unit increase in concern corresponds to a unit increase in behavior is a parsimonious account, but it does not tell whole stories as varying intensity of concern may trigger heuristics in a non-linear fashion. Second, in detecting behavioral congruence with privacy preference, the effect of concern has been presumed to be 'direct'. Nevertheless, behavioral response can be granulated or indirectly occur in multiple steps, as effect of concern is mediated through one's subjective evaluation of immediate benefits and gratification of her action. The overall process needs to be parceled out so that one can discern how heuristic norms intervene, as it might be that the links between concern and behavior are sequentially compounded. Third, the awe expressed over the behavioral incongruence is based on the expectation that both concern and behavior should correspond 'concurrently'. But can the effect be delayed temporally? A critical point of reevaluation here is whether privacy concern has a predictive, not concurrent, validity. People, relying on a quick habitual routine, might discount the need for immediate response to their concern. Instead, individuals' strategic decision can evolve gradually over time as they learn to adopt and engage in a slow but systematic reasoning.

## 3. Analysis 1: Non-linearity

Analysis 1 posits that it is characteristic of humans to defer systematic judgments when there is no overwhelming reason for immediate concern. From this, it is possible to project that the relationship between concern and behavior is non-linear, as it becomes a positive one only from a threshold point; as the concern increases, so do the accessible responses.

Social psychologists call it a floor or threshold effect at which the level of a decision to perform a certain task does not take off until it reaches a point of motivation (Frederick, 2005). Acquisti et al (2015) also raised an important insight about when people choose to be 'rationally ignorant' of uncertain events. According to them, ignorance can be rational if learning a new situation is estimated to be costlier, and more cumbersome than benefits of privacy. Here we can see how a threshold effect occurs at low concern (Neuman, 1990, 1991): a person remains perfectly rational in avoiding any actions related to their low privacy, but only up to a point of concern as efforts begin to make sense with increased concern. Reversely, this can be seen as a ceiling effect—a type of plateau where no action is triggered because people already pass a saturation point at which their concern no longer produces any differences.

Accordingly, Study 1 proposes to test the non-linearity of differential behavioral gains depending on levels of privacy concern. That is, there will be varying levels of covariation between privacy concern and behavior (H1)—a lower level of concern (H1a) is not associated with any privacy behavior, but with higher concern (H1b), privacy protection increases whereas privacy disclosure decreases.

### 3.1. Methods

For Analysis 1, a secondary analysis of the Knowledge Networks (KN) survey was performed. The data used in this study were publicly available and collected by the Pew Research to measure public attitudes toward government surveillance after Edward Snowden revelation in 2013 (Madden and Raine, 2015). A demographically balanced sample ($n$ = 607) was drawn from KN Panel participants who was recruited based on a combination of random digit dialing and address-based sampling. The response rate was 60.8% ($n$ = 935). A total of 607 respondents agreed to participate in each of three waves (2014–2015) of online panel surveys, with the completion rate of 64.9%. Study 1 analyzed those with mobile-based Internet access, using the first wave of the KN survey conducted on January 10–27, 2014. The publicly available dataset showed that 64% of the panel members ($n$ = 389) used Internet in tablets, mobiles, or smartphones.

Privacy concern, which this study conceptualized as the level of individuals' worry about government surveillance, was captured by asking respondents to rate their agreement to the following statement, on a scale of 1 (strongly disagree) to 4 (strongly agree): American citizens should be concerned about the government's monitoring of phone calls and internet communications ($M$ = 3.24, $SD$ = 0.77).

Two privacy behaviors were measured. The first dimension was protection, which was measured by asking whether each respondent was involved in any information protective activities, with a dichotomous measure (Yes = 1; No = 0). The wording was: "Have you ever asked someone to remove or correct information about you that was posted on the internet, including things like photos or videos, or have you never done this?" ($M$ = 0.20, $SD$ = 0.40).[1] The second dimension was disclosure, which was assessed by asking whether each respondent was involved in publicly disclosing one's identities online. The wording was: "Have you ever posted comments, queries or information on the internet, using…" Following this, two items were asked: (1) your real name; (2) a username or screen name that people associate with you. A two-item additive index formed a dichotomous (Yes = 1; No = 0) measure ($M$ = 0.67, $SD$ = 0.38; inter-item correlation $r$ = 0.345, $p$ < .01; with Oblimin principal component/factor loading 0.820 and eigenvalue 67.22).

This study accounts for variance attributable to two sets of covariates: (1) socio-demographics and (2) Internet use frequency. There existed considerable variations in each of socio-demographics, such as age ($Median$ = 42, $SD$ = 14.87), gender (49.6% women), income ($M$ = 13.32, $SD$ = 4.02, in a 19-scale classification), race (69.4% whites), and education ($M$ = 3.07, $SD$ = 0.98, in a scale anchored from 1 for less than high school to 4 for post-graduate degree), providing contexts comparable to those of the U.S. general population. In addition, we controlled for a basic usage of Internet, which may affect the extent to which one is involved in privacy behavior. The frequency of Internet use was assessed on a four scale (less often (1) to several times a day (4), $M$ = 3.83, $SD$ = 0.46).

Two sets of analyses were performed. Descriptive statistics were used to detect behavioral congruence with three levels of concern so that we can make visual inspections on each level. This was followed by an overall curve estimation that examined the model fitness when assuming a linear relationship between concern and behavior. Second, OLS regressions were run on the dependent variable of privacy disclosure (the additive scale) and logistic regressions were for privacy protection (the binary item). In order to detect the hypothesized non-linearity more precisely, the split between the high and low concern groups (high ≥ median 0.66) was warranted—that is, by isolating the two levels of privacy concern (that already showed difference in its descriptive inspection), analyses aimed to parcel out corresponding levels of behavioral responses that would have otherwise masked respective patterns in a collapsed model. Put differently, as Analysis 1 focused on the function of higher concern, separate regressions helped detect distinctive patterns respectively on their own right, compensating for the overall pattern of non-linearity eye-observed in its entirety.

[1] The finding that a small subset of respondents took any action in regards to privacy protection ($M$ = 0.20, $SD$ = 0.40) is intriguing. First, this indicates that the presence of protective response, in general, may not be widespread, to begin with. Second, however, relatively large variations of this particular response show that the distribution did not seem to converge around groups with particular traits but generally diffused, pointing out the presence of privacy paradox at least in the dimension of privacy protection as opposed to disclosure.

### 3.2. Results

Fig. 1 displays two distinctive patterns, when the level of behavior was measured against a linear increase of concern when broken down into three levels (25%; 50%; 75%, in each quartile percentile). For protection, there was no action at low and middle levels of concern, whereas an increase in action was found at the high level of concern, lending support to H1a and H1b. The size of increase, however, remained tiny. Only 24% of those who expressed high concern took any action to protect privacy. For disclosure, the behavior did not linearly follow different levels of concern, also supporting H1a (lower concern). Nevertheless, when it comes down to H1b (higher concern), the non-linear pattern is different from what was shown in protection, with the behavioral response staying extremely flat regardless of different levels of concern. As many as 74% of the respondents with high concern said that they disclosed personal identities online. This is not much different from those with the low level of concern as 77% of them reported to have done so. The test of curve estimation reaffirmed these descriptive observations, with none of the model fit for the linearity between concern and behavior found significant ($F = 0.156^{ns}$, $\beta = 0.02$ disclosure; $F = 2.364^{ns}$, $\beta = 0.07$ protection).

In Table 1, two observations stand out, for those with higher concern. First, controlling socio-demographics and Internet use frequency, the high concern was not found associated with protection, which suggests that behavioral congruence hardly sustains even among those with higher concern. Second, however, the association between high concern and disclosure was found positive ($\beta = 0.14$, $p < 0.00$), indicating that congruence existed among those with high concern with regard to disclosure. Nevertheless, the direction of congruence was paradoxically reverse (the more concerned, the more disclosure). For those with low concern, both models for protection and disclosure showed poor fits, although the overall model for disclosure was significant ($F = 2.312$, $p < 0.05$). The concern did not show any significance, instead attributing the explanatory power to other sociodemographic variables. The regression also had no significance for protection. That is, the models of high concern better explained the variations of privacy behaviors ($F = 5.528$ disclosure, $p < 0.00$; Chi-square $= 29.367$ protection, $p < 0.00$) than those of low concern.

### 3.3. Discussion

Analysis 1 demonstrated complex working relationships between concern and behavior because the patterns of non-linearity revealed more complexities than what was expected in H1. Specifically, the low concern lends support for H1a in that concern did not have behavioral explanation, as manifest in the tenuous model fit. The findings regarding the high concern, while supporting H1b, revealed the co-presence of complex patterns—the one with no apparent association between concern and protection, and the other with the reverse association between concern and disclosure (the more concerned, the more disclosure).

The reverse association shown at the level of high concern adds complication to the puzzle by illustrating that there is a threshold point from which the increase in concern results in, not the decrease but the increase in disclosure. This non-linear, opposite pattern is interesting because there appears no cognitive reason to succumb helplessly to data submission when people are concerned. Psychological reactance or boomerang effect (i.e., attempted influence causing a person to adopt the opposite position) as often found in a lab-experiment may not be a plausible explanation, because there was no attempt for intended persuasion, to begin with. Still, when one expands conceptual contours of boomerang effect, the role of high concern backfiring and thus forcing one to adopt the opposite position (of more disclosure) may emerge as a potential explanation deserving further inquiries.

Collectively, the findings that the increase of concern in intensity, not only (1) fails to correspond with protection, but also (2) translates into more disclosure, suggest two additional explanations. On the one hand, people's decision related to privacy protection may be better explained by other external factors such as individual skills, confidence, sociodemographic backgrounds (Park and Shin, 2020) or other situational contexts (Mansur, 2018). This account lends credibility, given significant influences of gender (Exp ($\beta$) = 2.12, $p < 0.01$) and age (Exp ($\beta$) = 0.96, $p < 0.00$) at the level of high concern. On the other hand, as for disclosure, it is possible that concern may not function as a threshold of curtailing the release of personal data. Or concern can simply fail to serve as a sufficient cause for triggering protective change. Instead, high concern can be a consequence of unavoidable data submission associated with high Internet use. Given a cross-sectional data do not control a precise temporal order, this account for reverse causality may be

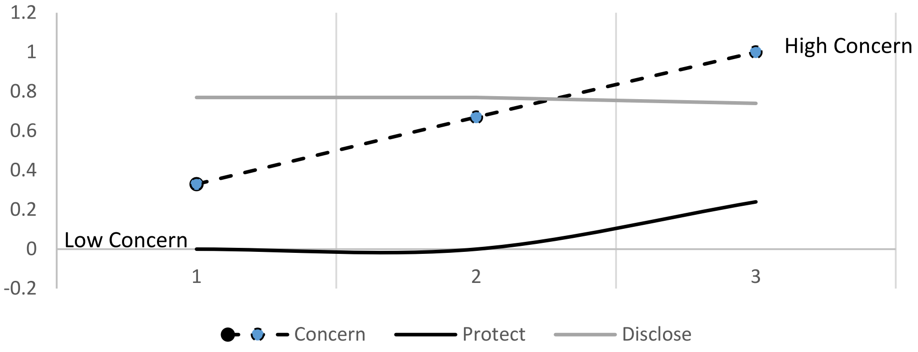

**Fig. 1.** Non-linear behavioral responses as compared to linear increase in concern. *Note*. Scale adjusted to 0 to 1 for direct comparison against each level of concern (1 = low; 2 = middle; 3 = high).

**Table 1**
Non-linear Pattern of Behavioral Response to Different Levels of Concern.

| | **Disclosure** | | | | **Protection** | | | |
|---|---|---|---|---|---|---|---|---|
| | *n* | β | *p*-value | $R^2$ | *n* | Exp (β) | *p*-value | *Nagelkerke* $R^2$ |
| **High Concern** | 322 | 0.14 | 0.00 | 0.10 | 324 | 2.01 | 0.41 | 0.13 |
| Higher than 0.66 | | | F | 5.528*** | | | Chi-square | 29.367*** |
| **Low Concern** | 59 | −0.07 | 0.52 | 0.23 | 61 | 1.21 | 0.99 | 0.17 |
| *List-wise excluded* | Multivariate OLS | | F | 2.312 * | Logistic Regression | | Chi-square | $6.378^{ns}$ |

*Notes*. Logistic regression was used for a binary measure of protection. Control includes income, education, gender, race, age, and Internet use frequency. * $p < .05$, ** $p < .01$, *** $p < .001$.

plausible. In this vein, high disclosure can be a threshold for inducing high concern, not the reverse. At the end, behavioral responses to concern turned out to be, not only non-linear (differentiated by the levels of high and low), but also convoluted (varied by the types of privacy behavior). This suggests that inner workings of privacy decision remain complex, highlighting that concern and its variations in intensity alone may not be the sufficient determinant for harnessing behavior into one way (protection) or the other (disclosure).

## 4. Analysis 2: Indirect relationship

The basic tenet of Analysis 2 is that heuristics are mediators for privacy concern, with a focus on the release of personal data. Prior studies point to two possible factors that might complicate behavioral response to concern: (1) reward and (2) trust.

First, reward is a psychological enticement for immediate gratification that triggers a quick response (Jai and King, 2016). A role of reward—the willingness to trade privacy for instantaneous benefit or convenience—has been well documented as it is not uncommon for people to give up personal information in exchange for content, discounts, or prizes (Park, 2021; White, 2004). A direct negative association between concern and reward is plausible, with high concern related to less reward-seeking—likely for the concern of personal data being released in exchange of using various online content and services. On the other hand, trust can serve as an overall guiding principle which helps moderate the relationship between concern and the decision of privacy release. Studies (Miltgen and Smith, 2015; Trüdinger and Steckermeier, 2017) hinted on the possibility of trust as a significant factor to influence the extent of behavioral response to privacy concern, as the greater trust will be likely to moderate how the concern influences one's decision about being enticed to release data. People who put the greater trust (on surveillance entities) may be willing to forego opportunities for the greater protection. That is, people will rely on heuristic cues for trust, when they are concerned about how much information to share in uncertain situations, because they are not certain about exactly how their personal information will be used, with what consequences.

Analysis 2 suggests the expectation is that people, in translating levels of their data concern, will go through the two heuristic processes. Trust, helping people quickly evaluate overall data environments, can be the main moderating step in one's evaluation on whether to act upon concern. Here reward can still intervene between concern and behavior, as it alleviates the cognitive burden of processing potential consequences of data release. Put differently, people can be easily manipulated by how they are instantly rewarded. Even the attitude that is as innocuous as trust might nudge the person to reveal more of herself than necessary, because it facilitates instant gains of reward and gratification with no immediately discernible harm of privacy loss. In other words, one's decision in respect to concern may be indirect via reward, but also compounded by the trust factor, exacerbating the difficulty of ascertaining a direct influence from privacy concern. Accordingly, Study 2 proposes the relationship between concern and one's decision to surrender privacy will be mitigated by reward, as people seek instant gratification, such as the reward of specific gains, thus more likely to disclose privacy, while any contextual cue for trust can also moderate their concern, likely to increase privacy disclosure (H2).

### 4.1. *Methods*

The sample for Analysis 2 consisted of the Knowledge Networks (KN) respondents administered by the Pew Research. These respondents were from the KN panel used in Study 1. As in Analysis 1, those with no mobile-based Internet access were filtered out, leaving a total of 389 participants for analysis. To examine the proposed moderated mediation model of concern, Andrew Hayes' (2012) PROCESS on SPSS (Model 7) was used, with 10,000 bootstrap resamples at bias-corrected and accelerated 90% confidence intervals. For concern (IV), disclosure (DV), and covariates (socio-demographics and frequency of Internet use), the same measures as in Study 1 were used. Additional measures of the moderator (trust) and the mediator (reward) were as follows:

Trust was measured by asking respondents to rate the level of their general belief in the government legitimacy (Iyengar, 1980), i.e. the extent to which they trust the government to do the right thing, on a scale of 1 (never) to 4 (just about always). The wording was: How much of the time do you think you can trust the government in Washington to do what is right? ($M = 2.03$, $SD = 0.57$).[2]

Reward was assessed by an item that asked the willingness to disclose personal information for the purpose of using online service.

[2] However, trust is a complicated issue, as it is influenced by party identification and the party in power. What makes it even more complex is blurred private–public sectors that are equally vulnerable under surveillance, as trust (or mistrust) over government apparatus interfaces with commercial digital platforms whereby data surveillance occurs.

Each respondent was asked, on a scale of 1 (strongly disagree) to 4 (strongly agree), to estimate their agreement to the following statement: I am willing to share some information about myself with companies in order to use online services for free ($M = 2.56$, $SD = 0.71$).

### 4.2. Results

H2 predicted the indirect, compounded process of moderated mediation. Analyses from Model 7 PROCESS lend the support for H2, with the moderate effect size (β = 0.30, $SE = 0.15$, LLCI = 0.10, ULCI = 0.63). Fig. 2 details each of two paths in the model—(1) interactive relationship between concern and trust on reward and (2) relationship between reward and disclosure—respectively. As expected, in predicting reward, the interaction between concern and trust was found to be significant (β = 1.42, $p < .01$), indicating that high concern, when moderated by high trust, did not lead to less reward seeking, but facilitated it. On the other hand, concern was negatively related to reward (β = −0.43, $p < .05$), while reward was found positively associated with disclosure (β = 0.21, $p < .05$). Each of two models had modest explanatory powers, although R square for disclosure (0.13, F = 5.91, $p < .00$) was stronger than that of reward (0.07, F = 2.68, $p < .01$).

### 4.3. Discussion

The findings highlight two key points. First, each of hypothesized relationships was found to be significant, implying that the patterns of associations between concern, trust, and reward have complex but tight inner connections leading up to the disclosure of private information. Second, the significance of moderated mediation as a whole also suggests that the proposed indirect relationship may be theoretically valid, when all different paths were combined into one model. What remains key in Study 2 is that underpinning of individual decisions is built upon, not just as direct responses to the stimulus of concern or anxiety related to privacy loss. Instead, privacy disclosure may derive from one's estimate on whether the loss can be compensated (reward), as individual cost-benefit analysis may be quickly passed on to her/his trusted environment (trust). Put it differently, seemingly incongruent responses should be traced back to indirect links between concern and disclosure, within which the relationship, moderated by one's level of trust, becomes intervened by reward that encourages the suspension of systematic protection for immediate gratification.

Thus, the central issue is that instant gratification of obtaining reward, deeply embedded in digital consumption as a form of free content and service, is likely to help forego systematic decision that is needed to exercise protection. Study 2 shows that this will happen even in the context of governmental surveillance, as people delegate privacy judgement to their levels of trust, which can be an effective shortcut easing cognitive burden of assessing the likelihood of privacy violation. The fact that trust significantly moderated high concern in promoting reward-seeking is telling. In other words, inner workings of cost-benefit analysis remain hardly attributable to concern alone. Striking a similar note, the overall model of moderated mediation suggests that concern or caring may not be entirely fitting as the departure point of privacy behavior.

Fundamentally, what Analysis 2 illustrates is how vulnerable individual cognition is to the enticement of reward nudging people into under-protection, as it is exacerbated by trust which cajoles even those concerned to suspend risk perceptions. Privacy-related judgement is not encouragingly rational, despite the fact that the inclination to share, release personal data is presented as a rational choice in digital platforms such as Facebook. Uncertain future outcomes motivate people to be in favor of a short-term gain (of being rewarded) and succumb to the gratification of digital access and content that would be otherwise unavailable. In this context, it might be seen as even rational to set aside the gain (of being privacy-guarded) when people cannot see tangible benefits as consequences of their protective action, while concerned people remain unable to reserve privacy according to levels of their concern.

## 5. Study 3: Temporality

The premise of Analysis 3 is that people's prediction about their future often remains at odds with their own account about their action at present. From this, Analysis 3 suggests that the congruence between one's expressed concern and protective behavior might not occur concurrently as the actual response to data concern might well surface in a delayed sequence in future events. Scholars (Acquisti, 2004) noted this pattern of procrastination as 'delayed gratification', as there may be a temporal disjuncture between action and concern, with people's decision delayed or extended over time. Temporality, as proposed in Analysis 3, conceptualizes the role of time-discounting—cognitive valuation placed on receiving benefits 'now' compared with receiving them 'later' (Frederick et al., 2002). Here delays presume certain sequential processing because people's minds go through initial, heuristic, or temporary suppression before the functions of stimulus occur. In media effect literature, one might also find similarities to a type of 'sleeper effect' in which effect of negative political advertising, for instance, increases substantially over time, but not immediately after an initial exposure (Weaver et al. 1999). Delayed action is thus triggered in favor of immediacy after a certain stimulus or triggering event—in this case, concern.

Procrastination has psychological benefits. First, it saves time and effort that comes with privacy protection. Second, the delay of action fulfills self-serving bias in that people tend to underestimate the probability of risky events happening to them in future. Third, inaction makes sense because it rewards instantaneous comfort at the moment. In a similar vein, people's indecision and failure to make timely protective measure may not be a sign of being handicapped or deficient. Instead, people often make deliberate decisions to procrastinate with pressing concern so as to learn strategies and plan actions over time (Chou and Choi, 2005; Ferrari, 2001). Further, unlike the behavior of personal data release, the action of protection would demand the active allocation of additional time and effort because the strategies for proactive protection are distinctively apart from any other routine digital consumptions.

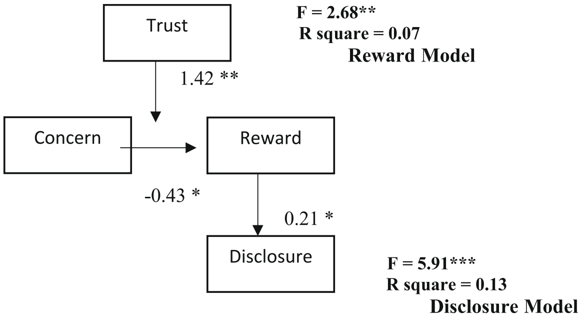

**Fig. 2.** Indirect relationship between concern and disclosure. *Note.* Control in each regression includes income, education, gender, race, age and Internet use frequency. Reported numbers are coefficients from two separate models.* p < .05, ** p < .01, *** p < .001.

Based on this reasoning, concern might go through two distinctive processes over time. The first one is a heuristic route in which concern (T1) leads to the delay of action in an immediate discount of privacy loss (T1). The second one is a systematic route in which concern (T1), which activates concern in the future (T2), eventually leads to systematic responses in a slow fashion (T2). The crucial point is that the incongruence between concern and behavior might be fixed over time, because any concerting efforts might be too cognitively demanding and time-consuming to be tangible in instant calculations. Fundamentally, the temporal delay shows the role of heuristics in trumping immediate convenience over the gain of protection as people tend to place a higher value on the near-future comfort enshrined in habitual inaction. Accordingly, Analysis 3 proposes that concern at Time 1 will have no tangible effect at Time 1. Instead, concern at Time 1 will be positively associated with concern at Time 2. More importantly, concern at Time 1 will have a direct effect on privacy protection at Time 2, affirming the delay of action (H3). In sum, the net (direct and indirect) effect of concern at Time 1 will be manifest at Time 2.

### *5.1. Methods*

The panel sample for Analysis 3 consists of Wave 1 and Wave 2 participants of the 2014–2015 Knowledge Networks (KN) surveys that were administered by the Pew Research Center (hereafter labeled as “Time 1 (T1)” and “Time 2 (T2)”, respectively). A total of 475 KN panelists among the original 607 respondents in T1 survey participated again in the online survey conducted between November 26, 2014 and January 3, 2015 (T2). As in Analysis 1 and Analysis 2, only those who used Internet in tablets, mobiles, or smartphones (*n* = 294 or 61% of the T2 panel members), were selected for analysis.

Analysis 3′s hypothesis was tested using a series of hierarchical regressions pertaining to each path. The paths were estimated for all four variables (between concern and behavior across T1 and T2), controlling socio-demographics and the frequency of Internet use. In Study 3′s analyses, behavior at T2 was employed as the dependent variable, with concern at T2 as a mediator between concern at T1 and behavior at T2, and concern at T1 was the independent variable. In addition, the indirect effect of concern at T1 on behavior at T2 was assessed, using Hayes’ (2012) PROCESS on SPSS (Model 4). This additional analysis helped evaluate the strength of the proposed mediation as a combined model. For T1, the measures of privacy concern (IV), protect (DV), and covariates (the frequency of Internet use and socio-demographics of panel participants) were the same items used in Study 1. Additional measures of privacy concern and behavior for T2 were as follows:

> Privacy concern at T2 was measured by asking respondents about the levels of their concern, on a scale of 1 (not at all concerned) to 4 (very concerned). The question wording was: “Overall, how concerned are you about government surveillance of Americans’ data and electronic communications?” (*M* = 2.62, *SD* = 0.87).

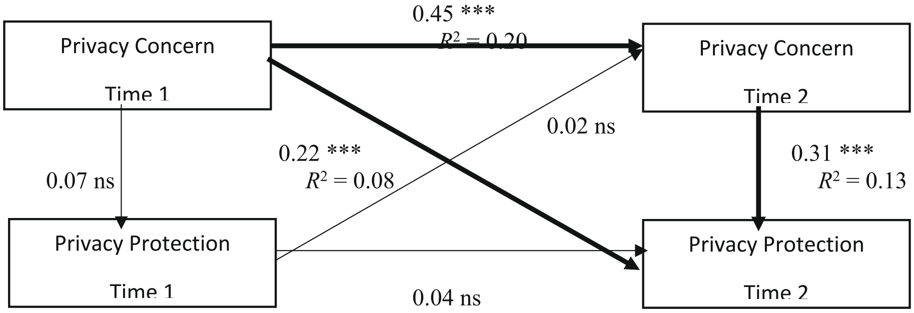

**Fig. 3.** Path regression analyses for concern and behavior across T1 and T2. *Note.* Control in each regression includes income, education, gender, race, age and Internet use frequency. Reported numbers are coefficients from each path. * p < .05, ** p < .01, *** p < .001, and bold lines indicate significant relationships.

Privacy protection at T2 was operationalized by the extent of one's involvement in protective activities. This was asked as part of a battery of questions following the prompt: "Have you done any of the following in an effort to hide or shield your information from the government?" Following this prompt, privacy protection was assessed with seven unitary items (Yes = 1; No = 0, one for each). These items were: (1) made more phone calls instead of communicating online; (2) avoided using certain terms in online communications; (3) avoided certain apps; (4) uninstalled certain apps; (5) used pseudonyms; (6) not used certain terms in search engine queries you thought might trigger scrutiny; and (7) spoke more in person instead of communicating online or over the phone. Answers were added and then averaged to create an index ($M = 1.13$, $SD = 0.26$, Cronbach $\alpha = 0.86$, with Oblimin principal component/factor loading of all items above 0.671 and eigenvalue 55.35).

### 5.2. Results

Bivariate analyses were performed to assess the relationships among four variables of concern and behavior across T1 and T2. Correlations were in the expected directions. Privacy protection at T1 was not significantly related with concern at T1 or T2, whereas there were positive associations between privacy protection at T2 and privacy concern at both T1 ($r = 0.314$, $p < .00$) and T2 ($r = 0.224$, $p < .00$).

Fig. 3 presents the results of regression analyses representing the associations between concern and behavior across T1 and T2. All hypothesized associations were found to be significant. Privacy concern at T1 had a significant relationship with privacy protection at T2 ($\beta = 0.22$, $p < .00$). Privacy protection at T2 was also predicted by concern at T2 ($\beta = 0.31$, $p < .00$), which was in turn predicted by privacy concern at T1 ($\beta = 0.45$, $p < .00$). Explanatory power of privacy concern as a block was modest (T1 concern on T2 protection, $R^2 = 0.08$; T2 concern on T2 protection, $R^2 = 0.13$). Still, these support the hypothesized paths, as (1) T1 concern relates to T2 protection and (2) T1 concern affects T2 concern, which in turn relates to T2 protection, even after taking into account covariates. As found in bivariate correlations, no concurrent association between privacy concern and protection at T1 was found and T1 privacy protection also had no predictive power for any measures at T2, supporting the premise of Study 3. The significance of the proposed indirect model in which the relationship between T1 concern and T2 protection is mediated through T2 concern was tested, using PROCESS (Model 4). The support was found ($\beta = 0.07$, SE = 0.02, LLCI = 0.03, ULCI = 0.11), indicating that the function of T2 concern as a mediator was strong enough to hold significance in a combined model.

### 5.3. Discussion

Analysis 3 adds the explanation to the puzzle of privacy concern by unlocking interrelated paths related to privacy protection. Panel datasets observed at two different times lend a unique opportunity to test the delayed response to privacy concern. The findings supported the expectation, in that concern at T1 had a direct relationship to protection at T2, but displayed no relationship to protection at T1. Study 3 aimed to illustrate that the benefit of concern can happen in such a delayed sequence, with people's privacy decision extended over time. The finding that there was no effect of T1 protection on any measures across T1 and T2 is intriguing, as this disputes the claim of reverse causality in which behavior precedes concern—at least in the case of privacy protection. T2 concern was also predicted only by T1 concern, eliminating the possibility that T1 protection may be triggering T2 concern. Additionally, no relationship was found between T1 and T2 protections, leaving T1 concern to be the most plausible explanatory factor by which one's privacy-related action are trickled down to T2.

Of course, the precise systematic route in which protection at T2 is activated remains unknown. The weak coefficient size of indirect model ($\beta = 0.07$, Model 4) points to potentially subtler routes in which concern at T2 may not play the role of mediating concern at T1. This suggests the need of alternative model specifications, in which other cognitive factors such as one's skill or knowledge should be included for stronger explanations. Alternatively, tenuous indirect finding related to T2 concern might derive from non-equivalency of measures because question wordings regarding the concern about government surveillance differed across T1 and T2. Adding one more panel at T3—with equivalent items—will help assess the extent to which longitudinal relationships depend upon (1) such item variations and (2) cognitive skill-based paths leading toward systematic decisions related to data protection.

## 6. General discussion

The present study was initiated as an effort to expand the investigation of puzzling response to data privacy concern (Hargittai and Marwick, 2016; Hoffmann et al., 2016; Masur and Trepte, 2021), as applied to the context of government surveillance (Park et al., 2018; Neuman, 1991). Each of three analyses in this study posited three heuristic structures of privacy shortcuts that are hardwired for quick judgements in a complex web of digital ecosystem. Key conceptual foundation is that privacy-related rationality is (1) non-linear, (2) indirect, and (3) temporally delayed as people resort to instant judgements, largely filtering out cognitive demand for systematic involvement in assessing uncertain future outcomes.

In triangulating findings, the premise across three analyses stayed remarkably the same in two fronts. First, the function of privacy concern remains too complex to be linearly conducive of congruent behavioral response at the time of expressed concern with no hindrance of other heuristic norms, such as reward. The finding in Analysis 1 indicates higher release of data privacy was linked to higher concern. Coupled with the vulnerability of enticing reward observed in Analysis 2, these point to the danger of relying on heuristic judgements, when it comes to privacy protection. Second, individual psychology of concern alone is too tenuous to explicate sufficient, if not necessary, explanation about privacy choice. Variations of privacy concern seem to have little direct bearings on behavioral decisions. This was evident in tenuous effects of concern found in Analysis 1 (ns for protection and concern) and Analysis 3 (β = 0.07, from T1 concern to T2 protection), as concern was tested as a starting point of model specification in predicting the increased privacy protection. Analysis 3, on the other hand, illustrates systematic, considerate reasoning—as opposed to quick heuristic processing—might be required over time before individuals fully realize the need to take protective actions (Tversky and Kahneman, 1974). The delayed protection indicates the short-sighted attitude of procrastination, as people cannot normally translate their concern into immediate protective action.

Note that this does not preclude the effectiveness of intuitive judgement that was often documented in social psychology literature (Gambino et al., 2016; Neuman et al., 2007; Sundar, 2008). As found in previous works (Baruh et al., 2017; Park, 2013), however, individual calculus, solely based on heuristics rather than complete information or knowledge, showed limits in its utility particularly in translating privacy concern into meaningful actions. At a broad level, this study's findings imply much bounded rationality in digital consumption (Neuman, 2016), within which heuristic activation or suppression of concern does not guard off potentially vulnerable decision makings related to privacy loss (Barth and De Jong, 2017).

The central point is that individual psychology does not serve as a basis of optimism for self-regulatory behavior, as people's privacy decision does not appear to be purely based on deliberated calculation—consequently, privacy is not managed in accordance with self-interest. All findings corroborate this point, in that readily-accessible cognitive judgements help reduce the difficulty of estimating the likelihood of privacy gain and loss into a set of heuristics. These tendencies certainly have advantages as they are 'economizing' the process of decision making for the benefit of efficiency as people confront constant data release in daily routines of digital consumption. The danger is that when a careful consideration is reduced to the quick moment of a choice, privacy can be over-released, surrendered over gratification, and eventually deferred to inaction. At least from this study's findings, it appears that even those highly mobile-equipped people are not competent and remain vulnerable to the potential digital surveillance.

The findings are alarming in this regard, given the absence of powerful intervention in the U.S. As privacy protection is entirely deferred to individual discretion that are subject to heuristic norms, bias for short-term benefits and enticement, and temporal misjudgment, it is hardly expected of meaningful actions when people are concerned (Park, 2021). On a practical side, if social media or digital platforms genuinely hope for protecting privacy, they should not let their users decide on whether to protect their data or not. Instead, it is advisable that personal data-driven entities design carefully-calibrated privacy settings, such as a visible privacy dashboard, which are intuitively evident and easy. In this case, strong regulatory mandates for this type of interface design will be necessary to stimulate protective action from the part of individual users.

This is not to suggest that behavioral decisions are only related to heuristic calculation that's to save time and cognitive effort. Nor is it to argue for the absence of systematic processing related to elaborate privacy decisions or other traits, such as apathy or cynicism, (Hargittai and Marwick, 2016; Zhu et al., 2021). In fact, evidence for people engaging in protective measures had been discovered, while the importance of risk knowledge as a guiding principle helping privacy-sensitive decisions was well-documented (Soumelidou and Tsohou, 2021). The modest explanatory powers of hypothesized models in each of three analyses also suggest that missing puzzles could be located in terms of privacy understandings in combination with other heuristic principles. To this end, this study's findings invite future studies to investigate the interactions between knowledge and 'shortcuts', i.e. the extent to which the function of knowledge or awareness guarding off heuristic impulses will aid people to navigate the lack of certainties in their online use (Madden et al., 2017; Park and Shin, 2020).

## 7. Limits and suggestions for future studies

Methodologically, limits of single items, particularly with their miniscule distributions of DV (protective behavior) in Analysis 1, KN panel, are noteworthy. Granted that they do not capture wide variations of behavioral patterns, the analyzed items speak about a limited range of privacy control. Analysis 2 in this regard will also need a wider range of items that reflect a valid universe of data release in digital consumption. Additionally, because it is possible behavioral incongruence detected in Analysis 2 might have derived from a discrepancy in measurement between a general level of government trust and individual data release behaviors that were not directly related to each other, further studies must add various measures of trust and reward with corresponding behavioral subtleties.[3] Still, it is important to note that while trust or reward mostly interfaces with commercial venues, personal data also get accessed and surveilled by government entities via private (social media) platforms. In this respect, despite the development of GDPR, user heuristics related to immediate reward and trust in EU contexts will remain problematic, precisely because the EU regulation does in fact mandate the principle of user 'opt-in' in exchange of free access (Park, 2021a,b).

As future studies continuously unlock persistent mysteries related to privacy concern, in-depth interview and focus group discussion would not only complement this study's findings, but also unlock precisely 'why' people fail to take actions. This points to a possibility of psychological shortcuts such as optimistic bias (Kim and Hancock, 2015; Kobsa et al., 2016) by which people elaborate their decisions by underestimating privacy risk for themselves, but overestimating the risk for others. Similarly, the third-person effect (Li, 2008) sheds light on privacy decision making as people evaluate their chance of being exposed to surveillance to be low, but believe that others are vulnerable to such threats. What focus group data will add in this debate is people's perceptions about their behaviors in their own words—for instance, new insights on convoluted ways of their releasing and protecting data, and reasoning, which survey methods cannot capture.

One of the contributions of this study is to test and replicate the insights from experimental studies (e.g., Brandimarte et al., 2013),

[3] The suggestion by the reviewer for this insight is kindly acknowledged.

using surveys. Although question items used in this study are not an exclusive list of data release and protection, it is possible to use this study's findings as an empirical basis of evidence that other studies aspire to replicate with different methodologies. There is a need for the inventory of common privacy items, which will make it easier to translate experimental findings into surveys (and vice-versa). Assuming national surveys about privacy behavior may have primed respondents to worry about surveillance, it seems still hard to argue that expressed concern documented across three analyses is a byproduct of social desirability. Puzzling functions of concern must not be taken as evidence of the void of genuine concern (thus, justification over policy inaction), but the complexity of human rationality as individual decision related to privacy cannot be reduced to the sole function of one attribute.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347 (6221), 509–514.

Barth, S., De Jong, M.D., 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. Telematics Inform. 34 (7), 1038–1058.

Baruh, L., Secinti, E., Cemalcilar, Z., 2017. Online privacy concerns and privacy management: A meta-analytical review. J. Commun. 67 (1), 26–53.

Brandimarte, L., Acquisti, A., Loewenstein, G., 2013. Misplaced confidences: privacy and the control paradox. Social Psychol. Personality Sci. 4 (3), 340–347.

Dienlin, T., Masur, P.K., Trepte, S., 2019. A longitudinal analysis of the privacy paradox. New Media Society, 14614448211016316.

Ferrari, J.R., 2001. Procrastination as self-regulation failure of performance: effects of cognitive load, self-awareness, and time limits on "working best under pressure". Eur. J. Pers. 15, 391–406.

Frederick, S., 2005. Cognitive reflection and decision making. J. Econ. Perspect. 19 (4), 25–42.

Frederick, S., Loewenstein, G., O'Donoghue, T., 2002. Time discounting and time preference: a critical review. J. Econ. Literature 40, 351–401.

Gambino, A., Kim, J., Sundar, S.S., Ge, J., Rosson, M.B., 2016. User disbelief in privacy paradox: Heuristics that determine disclosure. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 2837–2843.

Gerber, N., Gerber, P., Volkamer, M., 2018. Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. Comput. Security 77, 226–261.

Hargittai, E., Marwick, A., 2016. "What can I really do?" Explaining the privacy paradox with online apathy. Int. J. Commun. 10, 21.

Hayes, A., 2012. PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling. Retrieved from http://claudiaflowers.net/rsch8140/Hayesprocess.pdf.

Hoffmann, C.P., Lutz, C., Ranzini, G., 2016. Privacy cynicism: a new approach to the privacy paradox. Cyberpsychology: J. Psychosocial Res. Cyberspace 10 (4).

Jai, T.M.C., King, N.J., 2016. Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? J. Retailing Consum. Serv. 28, 296–303.

Kim, S.J., Hancock, J.T., 2015. Optimistic bias and Facebook use: self–other discrepancies about potential risks and benefits of Facebook use. Cyberpsychology, Behav, Soc. Networking 18 (4), 214–220.

Kobsa, A., Cho, H., Knijnenburg, B.P., 2016. The effect of personalization provider characteristics on privacy attitudes and behaviors: an elaboration likelihood model approach. J. Assoc. Inf. Sci. Technol. 67 (11), 2587–2606.

Li, X., 2008. Third-person effect, optimistic bias, and sufficiency resource in Internet use. J. Commun. 58 (3), 568–587.

Madden, M., Gilman, M., Levy, K., Marwick, A., 2017. Privacy, poverty, and big data: a matrix of vulnerabilities for poor Americans. Wash. UL Rev. 95, 53.

Madden, M., Raine, L., 2015. Americans' attitudes about privacy, security and surveillance. Retrieved from Pew Research Center. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy security-and-surveillance.

Marcus, G.E., Neuman, W.R., MacKuen, M., 2000. Affective Intelligence and Political Judgment. University of Chicago Press, Chicago, Illinois.

Masur, P.K., Trepte, S., 2021. Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. Hum. Commun. Res. 47 (1), 49–74.

Miltgen, C.L., Smith, H.J., 2015. Exploring information privacy regulation, risks, trust, and behavior. Inf. Manage. 52 (6), 741–759.

Neuman, W.R., 1990. The threshold of public attention. Public Opin. Q. 54 (2), 159–176.

Neuman, W.R., 1991. The Future of the Mass Audience. Cambridge University Press, London, UK.

Neuman, W.R., 2016. The Digital Difference: Media Technology and the Theory of Communication Effects. Harvard University Press, Cambridge, MA.

Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T., 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. Int. J. Hum Comput Stud. 65 (6), 526–536.

Park, Y.J., 2013. Digital literacy and privacy behavior online. Commun. Res. 40 (2), 215–236.

Park, Y.J., 2021a. The Future of Digital Surveillance: Why Digital Monitoring will Never Lose its Appeal in a World of Algorithm-Driven AI. University of Michigan Press, Ann Arbor, MI.

Park, Y.J., 2021b. A socio-technological model of search information divide in US cities. Aslib J. Inf. Manage. 73 (2), 144–159.

Park, Y.J., 2021. Structural Logic of Ai Surveillance and its Normalisation in the Public Sphere. Javnost-The Public 1–17. https://doi.org/10.1080/13183222.2021.1955323.

Park, Y.J., Shin, D.D., 2020. Contextualizing privacy on health-related use of information technology. Comput. Hum. Behav. 105, 106204.

Shin, D., 2020. Expanding the role of trust in the experience of algorithmic journalism: user sensemaking of algorithmic heuristics in Korean users. J. Practice 1–24.

Simon, H.A., 1955. A behavioral model of rational choice. Q. J. Econ. 69 (1), 99–118.

Soumelidou, A., Tsohou, A., 2021. Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. Telematics Inf. 61, 101592.

Sundar, S.S., 2008. The MAIN Model: A Heuristic Approach to Understanding Technology Effects on Credibility. MacArthur Foundation Digital Media and Learning Initiative, pp. 73–100.

Trüdinger, E.M., Steckermeier, L.C., 2017. Trusting and controlling? Political trust, information and acceptance of surveillance policies: the case of Germany. Government Inf. Q. 34 (3), 421–433.

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.

Waldman, A.E., 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. Curr. Opin. Psychol. 31, 105–109.

White, T.B., 2004. Consumer disclosure and disclosure avoidance: a motivational framework. J. Consumer Psychol. 14 (1 and 2), 41–51.

Zhu, M., Wua, C., Huanga, S., Zheng, K., Young, S., Yana, X., Yuana, Q., 2021. Privacy paradox in mHealth applications: an integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. Telematics Inf. 61, 101601.