Journal of Business Research 152 (2022) 144–153

Contents lists available at ScienceDirect

Journal of Business Research

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

Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization

Julien Cloarec

iaelyon School of Management, Université Jean Moulin Lyon 3, Magellan, Lyon, France

ARTICLE INFO

Keywords:
Protection motivation theory
Privacy control
Vulnerability
Self-efficacy
Falsifying information

ABSTRACT

The latest advances in data-driven marketing, such as real-time personalization, have increasingly made consumers more vulnerable. In response, some consumers deliberately falsify information in order to redress the balance of power, a practice that constitutes a serious threat to the digital economy. The topic of falsification is still largely under-researched in information systems and marketing. Based on protection motivation theory, the author conceptualizes privacy controls as a source of information and the falsification of information as a coping response, with vulnerability representing the threat appraisal mechanism and self-efficacy the coping appraisal mechanism. Through a within-subject experiment (n = 207), the results of the mediation analysis for repeated measures show that the effect of privacy controls as a source of information on the falsification of information is fully mediated by vulnerability and self-efficacy. The author provides insights for managers regarding the significant trade-off between reducing consumer vulnerability and maintaining the usefulness of the data.

1. Introduction

> *"Social media users are building false online identities to throw off advertisers and muddle databases—generating lots of ads for slippers. Creative consumers also fake out retailers, grocery stores and other data collectors."*
>
> (The Wall Street Journal, 2018)
>
> "Against online surveillance, Internet users 'poison' their personal data"
>
> (Le Monde, 2022)

The latest advances in data-driven marketing, such as real-time personalization, have made consumers more vulnerable (Swani et al., 2021). The data collected is becoming increasingly sensitive, leading to greater consumer vulnerability (Brough & Martin, 2021). Market power and supremacy in surveillance technology have made digital platforms the rulers of data (Acquisti et al., 2020; Aubert-Hassouni & Cloarec, 2022) by taking advantage of information asymmetry (Chen et al., 2018). Although users state that websites collect too much information without their permission (Chen & Rea, 2004), it has long been evident that consumers lack sufficient knowledge and control of their data (Cloarec, 2020; Culnan & Williams, 2009). Heightened by the networked nature of social media (Chen et al., 2018; Cloarec et al., 2022), this situation stems from the sense of helplessness known as digital resignation (Draper & Turow, 2019). In response, some consumers deliberately falsify information in order to redress the balance of power, a practice that constitutes a serious threat to the digital economy (Kolotylo-Kulkarni et al., 2021). Alashoor et al. (2017) show that the data obtained from social media is thus partly false due to these privacy concerns. However, the topic of falsification remains largely under-researched in information systems and marketing (Miltgen & Smith, 2019).

To counteract this consumer subversion, Mattison Thompson & Siamagka (2022) emphasize the importance of firm-initiated privacy ethics. Some authors refer to the notion of corporate digital responsibility, according to which firms should encourage consumers to be more aware of and to assert control over their data (Lobschat et al., 2021), in terms of data collection and management decisions (Du & Xie, 2021). Despite the advent of privacy regulations aiming to reduce consumer vulnerability (Krafft et al., 2017), there are few such initiatives. For example, it has been shown that privacy policies can alleviate falsifying behaviors (Martin & Murphy, 2017). However, to be effective, privacy controls require effort on the part of users (Mousavi et al., 2020). And because a trade-off exists between reducing consumer vulnerability and maintaining the usefulness of the data (Zhang & Watson IV, 2020), calls for moderated use of users' personal information have been not followed up (Martin & Murphy, 2017).

There is currently little research on the key role of privacy empowerment, mainly characterized by privacy control (Bandara et al., 2021).

E-mail address: julien.cloarec@univ-lyon3.fr.

https://doi.org/10.1016/j.jbusres.2022.07.045
Received 30 March 2021; Received in revised form 17 July 2022; Accepted 22 July 2022
Available online 29 July 2022

Among the scholars working in this area, Morey et al. (2015) claim that teaching users how to control their data is an enlightened principle. This type of marketing intervention can foster operant resource development (Bieler et al., 2021). In particular, Morewedge et al. (2021) state that.

> *"Perceived control may be particularly impaired if firms remove actual user control by fixing how data is collected, accessed, and presented. A shift to experiential consumption of data, however, could increase psychological ownership of that data if firms give consumers more control of its disclosure, display, and delivery, facilitating identification with the data and its consumption"*

In line with this research stream and in contrast to prior studies that consider privacy controls as a coping response or as a moderator (Martin et al., 2017a; Mousavi et al., 2020), the present paper considers privacy controls as a source of information. Falsification has been studied through a various theoretical perspectives, such as the theory of planned behavior, social exchange theory, power-responsibility equilibrium, privacy calculus, construal level theory, social contract theory and gossip theory (Table 1). Although no theory regarding falsification of data has yet predominated in any literature stream (Miltgen & Smith, 2019), prior IS research on privacy through protection motivation theory appears promising, as it conceptualizes the falsification of information as a privacy-protective behavior. Protection motivation theory has been applied to several contexts (Table 2): social media, antimalware software, home computers and networks, electronic medical records, location-based services, and online behavior. Accordingly, the author here adopts a research model based on protection motivation theory. To test it, a within-subject design was implemented, in which French respondents (n = 207) were exposed to Facebook privacy controls. As recommended by the literature, the author analyzes the data with a mediation analysis for repeated measures (Montoya & Hayes, 2017), with vulnerability being viewed as a threat appraisal mechanism and self-efficacy as a coping appraisal mechanism. The results of the mediation for repeated measures show that both indirect effects are significant and negative. Regarding the threat appraisal mechanism, privacy controls as a source of information reduces vulnerability, which in turn increases falsification of information. Conversely, for the coping appraisal mechanism, privacy controls as a source of information increase self-efficacy, which in turn reduces falsification of information.

In the following sections, the paper 1) reviews the literature on falsification and privacy protection motivation theory, 2) develops a model from hypotheses based on protection motivation theory, 3) presents the methods and data, 4) reports the results, and 5) concludes with a general discussion.

2. Background and development of hypotheses

2.1. Falsification

Although the subject of falsification of data has been attracting researchers' attention over the last two decades (Table 1), no theory of falsification of data has yet established itself in any literature stream (Miltgen & Smith, 2019). Data is at the core of business today and is essential for marketers to operate. Research on the contexts of online behavior (Bandara et al., 2021, 2021; Horne et al., 2007; Lwin & Williams, 2003; Poddar et al., 2009) and retail behavior (Lwin et al., 2007; Mattison Thompson & Siamagka, 2022) shows that consumers who are reluctant to share their data tend to falsify it. This is also the case in data-breach contexts (Labrecque et al., 2021; Martin et al., 2017a). While the construct of privacy concerns is frequently used, other antecedents have also been studied, including felt invasion (Poddar et al., 2009), social contract violation (Labrecque et al., 2021), privacy empowerment (Bandara et al., 2021, 2021), organization privacy ethical care (Mattison Thompson & Siamagka, 2022), fair play (Horne et al., 2007; Miltgen & Smith, 2019; Poddar et al., 2009), and trust (Bandara et al., 2021; Chen et al., 2021; Martin et al., 2017a; Mattison Thompson & Siamagka, 2022; Miltgen & Smith, 2019).

Table 1
Prior research on falsification.

Source	Context	Framework	Antecedents of falsification	Main findings
Lwin and Williams (2003)	Online behavior	Theory of Planned Behavior	Attitude, behavioral control, moral obligation	Attitudes, perceived behavioral control, and perceived moral obligation are significant drivers of falsification.
Horne et al. (2007)	Online behavior	Economic and social exchange theories	Cost-benefit gap	The cost-benefit of disclosure influences falsification, but fairness perceptions do not.
Lwin et al. (2007)	Banking, car rental, medical service	Power–Responsibility Equilibrium	Privacy concerns	Consumers balance perceived deficits in privacy protection by power holders with defensive actions
Poddar et al. (2009)	Online behavior	Stimulus-Organism-Response	Criticality of exchange, felt invasion, fair play	Consumers' motivations vary from very simple rules to more customized rules
Youn (2009)	Privacy protection among young adolescents	Protection motivation theory	Privacy concerns, Privacy self-efficacy	Privacy concerns have an impact on risk-coping behaviors such as seeking falsification.
Alashoor et al. (2017)	Social media	protection motivation theory and the theory of planned behavior	Privacy concerns	Privacy concerns impact self-disclosure accuracy negatively.
Martin et al. (2017b)	Data breaches of public companies	Gossip theory	Emotional violation, Cognitive trust	Violation and trust mediate the effects of data vulnerabilities on outcomes.
Miltgen and Smith (2019)	Lottery	Privacy calculus	Relevance, Perceived benefits, Perceived risks, Trust	Context can play a significant role in moderating some of the relationships.
Chen et al. (2021)	Contact tracing	Social exchange theory	Cognitive trust, Affective trust	Cognitive trust reduces willingness to falsify, whereas affective trust increases it.
Bandara et al. (2021b)	Online behavior	Construal level theory	Privacy concerns, privacy empowerment, psychological distance of privacy	Psychological distances moderate the relationship between privacy concerns and privacy behavior.
Labrecque et al. (2021)	Data breach	Social contract theory	Stress, Perceived social contract violation	Stress and perceptions of social contract violation impact falsification.
Bandara et al. (2021a)	Online behavior	Power responsibility equilibrium theory	Privacy concerns, privacy empowerment, trust	Damaged trust triggers falsification.
Mattison Thompson and Siamagka (2022)	Online retail	Organizational ethical care	Organization privacy ethical care, perceived information control, trust towards organization	Organizational privacy ethical care is a positive driver of the amount and the accuracy of information consumers are willing to share with firms.

Table 2
Prior research on privacy through protection motivation theory.

Source	Context	Antecedents of falsification	Main findings
Alashoor et al. (2017)	Social media	Privacy concerns	Privacy concerns impact self-disclosure accuracy negatively.
Boss et al. (2015)	Antimalware software	Perceived severity, perceived vulnerability, rewards, response efficacy, self-efficacy, and response cost.	Fear appeals partially mediate the relationships between threat appraisals constructs and antimalware software use intention.
Crossler & Bélanger (2014)	Home computers and networks	perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost	Perceived severity, response efficacy, and self-efficacy are positively associated with security practices. Perceived vulnerability is negatively associated with security practices.
Kuo et al. (2014)	Electronic medical records	Privacy concerns	Collection, secondary use, and errors are positively associated with protective responses.
Junglas et al. (2008)	Location-based services	Big five personality traits	Conscientiousness and openness to experience are positively associated with concern for privacy.
Yao et al. (2007)	Online behavior	Need for privacy, self-efficacy	Need for privacy is positively associated with concern about privacy directly and indirectly through beliefs in privacy rights.
Youn (2009)	Online behavior	Privacy concerns, Privacy self-efficacy	Privacy concerns has an impact on risk-coping behaviors such as seeking falsification.
Dinev & Hart (2004)	Online behavior	Perceived vulnerability and perceived control	Perceived vulnerability is positively associated with privacy concerns.

2.2. *Protection motivation theory*

Protection motivation theory (PMT) was originally developed by Rogers (1975) and was revised and improved by Maddux & Rogers, 1983) for more general use in persuasive communication. PMT is historically associated with work on the impact of appealing to fear to bring about behavioral change (i.e., fear would lead individuals to protect themselves). In the analysis of users' intention to protect themselves from a hazard (Maddux & Rogers, 1983), the balance between the evaluation of the threat (i.e., fear and the benefits of protecting oneself) and the evaluation of coping strategies (i.e., self-efficacy and the cost of protecting oneself) is considered. Maddux and Rogers (1983) introduced the concept of self-efficacy as a new cognitive variable mediating protection motivation. Derived from Bandura's social learning theory (1997), this concept refers to the individual's perceived ability to adopt the proposed recommendation or to do what is suggested. Research shows that self-efficacy is a good predictor of intention to adhere to recommendations and to motivate individuals to protect themselves (Floyd et al., 2000).

In privacy research, PMT has been used to study social media (Alashoor et al., 2017), antimalware software (Boss et al., 2015), home computers and networks (R. Crossler & Bélanger, 2014), electronic medical records (Kuo et al., 2014), location-based services (Junglas et al., 2008), and online behavior (Dinev & Hart, 2004; Yao et al., 2007; Youn, 2009). In this research stream, the most relevant constructs appear to be self-efficacy (Boss et al., 2015; R. Crossler & Bélanger, 2014; Yao et al., 2007; Youn, 2009) and vulnerability (Boss et al., 2015; R. Crossler & Bélanger, 2014; Dinev & Hart, 2004) (see Table 2 for further details regarding the main findings.

In the present study (see Fig. 1), the author conceptualizes privacy controls as a source of information and falsification of information as a coping response. The author develops a cognitive mediating process based on the literature. Vulnerability thus represents the threat appraisal mechanism, while self-efficacy represents the coping appraisal mechanism.

2.3. *Privacy control as a source of information*

Social networking sites (SNS) offer consumers a degree of control regarding their privacy and the information shared and collected by SNS. There are various kinds of privacy controls on different platforms and they all affect the user's privacy experience by triggering a sense of privacy protection (Xu et al., 2012). Indeed, privacy controls give rise to a psychological benefit, in that users feel in control of their privacy protection (Krafft et al., 2017; Mousavi et al., 2020; Xu et al., 2012). However, this feeling of privacy protection is highly subjective as it depends on the users' perception as to whether they really have power and on their ease of acquiring it (Mourey & Waldman, 2020). Users are more favorable to personalized ads when they feel that they exercise control (Tucker, 2014). Hence, providing users with privacy controls is a powerful restorative factor for empowering them and making them more receptive to personalization efforts (Martin & Murphy, 2017). In the literature the combination of privacy controls with proactive customer opt-ins regarding personalization is seen as the best practice (Steinhoff et al., 2019). Indeed, privacy control becomes an operant resource (Hibbert et al., 2012) that increases the willingness to disclose information overall (Mothersbaugh et al., 2012).

2.4. *Falsification of information as a coping response.*

Prior research shows that strong privacy controls (i.e., a privacy-enhancing factor) can alleviate falsification of information (i.e., a consumer outcome in the psychology of privacy) (Martin & Murphy, 2017; Norberg & Horne, 2014), possibly because consumers tend to falsify more when they perceive less privacy control (Lwin and Williams, 2003, Wirtz and Lwin, 2009). The asymmetry of information between consumers and SNS providers make consumers highly sensitive to perceived imbalances of power (Martin & Murphy, 2017). Indeed, the more users feel the need for privacy control, the more likely they are to falsify the information they provide (Punj, 2017). Such coping responses by providing false information makes users feel more in control of their privacy (Alkire et al., 2019; Lwin & Williams, 2003). On the other hand, researchers have found that stronger privacy controls lead to greater engagement in permission-based data exchange with firms (Krafft et al., 2017). We thus hypothesize that:

H1: Privacy controls decrease falsification of information.

2.5. *Vulnerability as threat appraisal mechanism*

Consumers often cite feelings of vulnerability in their perceptions of marketing efforts (Kshetri, 2014). When firms collect personal information covertly, it makes users feel more vulnerable (Aguirre et al., 2015). By sharing their personal information online, users feel vulnerable, because they may be exposing themselves too much (Martin et al., 2020; Palmatier & Martin, 2019). Martin et al., (2017a, p. 37) define vulnerability as a "customer's perception of his or her susceptibility to being harmed as a result of various uses of his or her personal data." Such vulnerability affects users' subsequent consumer behavior (Janakiraman et al., 2018). The nature of this vulnerability is not data-dependent, because feelings of violation and betrayal increase the need to punish the source, for example by falsifying information (Grégoire & Fisher, 2008; Smith, 2014).

Although there is a control paradox (i.e., users provide more information when they feel they have stronger perceptions of privacy

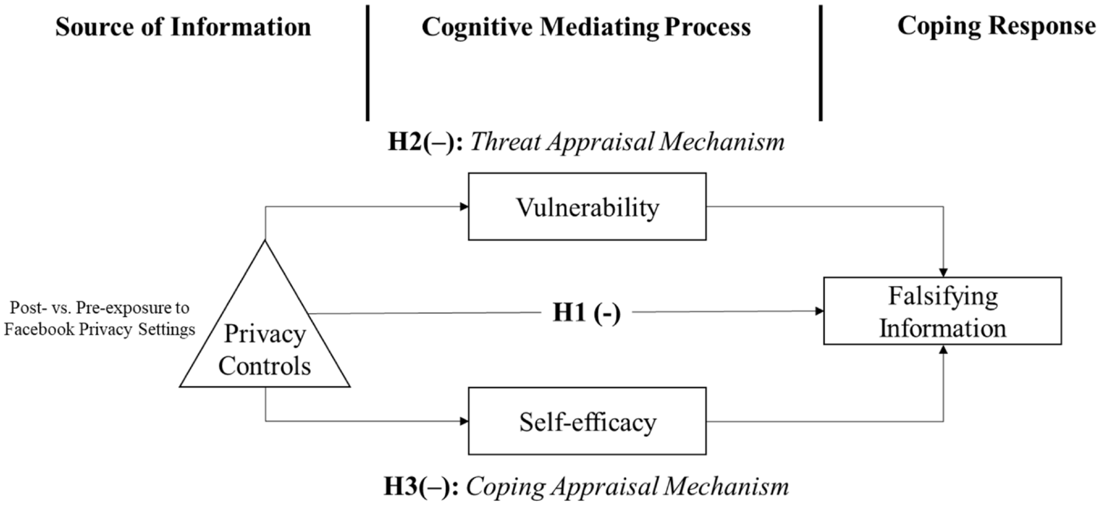
Source of Information
Cognitive Mediating Process
Coping Response
H2(–): Threat Appraisal Mechanism
Vulnerability
Post- vs. Pre-exposure to Facebook Privacy Settings
Privacy Controls
H1 (-)
Falsifying Information
Self-efficacy
H3(–): Coping Appraisal Mechanism

Fig. 1. Research model.

control) that makes users potentially become more vulnerable, it is largely unconscious (Brandimarte et al., 2013). The literature shows that improving decision-making competencies can help users overcome the vulnerabilities caused by imbalances of power (Anderson et al., 2016). Because consumers feel vulnerable when they lack knowledge (Culnan, 1995), providing them with knowledge should therefore reduce their vulnerability.

In line with (Martin et al., 2017a; Milne et al., 2009) and (Martin & Murphy, 2017), we expect that vulnerability increases falsification of information. For this reason, consistently with (Mousavi et al., 2020, p. 5), who state that "members anticipate the disclosure-induced privacy loss to reduce because privacy customization decreases one's vulnerability to privacy breach", we hypothesize that:

H2: Vulnerability mediates the negative effect of privacy controls on falsification of information.

2.6. *Privacy self-efficacy as a coping appraisal mechanism*

Control and self-efficacy are core components of users' psychological empowerment (Bandara et al., 2021a). Bandura (1986) states that the feeling of mastery increases self-efficacy. Contextual knowledge about privacy settings and privacy self-efficacy are key to triggering privacy-protective behaviors (Crossler & Bélanger, 2019). Protection motivation theory (Rogers, 1975) posits that self-efficacy is a coping appraisal mechanism, defined as an "individual's belief in his or her capability to perform activities with skill" (Spreitzer, 1995, p. 1443). Bandura (1993) shows that self-efficacy is task-specific. For example, the more Internet users report self-efficacy, the more they feel comfortable online (Peltier et al., 2009). This still holds when the level of analysis on social media themselves is lowered (James et al., 2017). Chen and Chen (2015) thus adapted the concept to the perception of the user's ability to protect his or her privacy (i.e., privacy self-efficacy). Despite privacy concerns, privacy self-efficacy leads to continuous social media use, thus alleviating the privacy paradox (Bright et al., 2021). Self-efficacy is usually the strongest and most consistent antecedent of online protection behavior (Wottrich et al., 2019); and related to privacy controls, it is a trigger for a privacy coping response (Milne et al., 2009; Youn, 2009). Mousavi et al. (2020) assert that "promoting user awareness of available privacy controls and users' ability to comprehend the scope of each control will help […] the effort needed for appraising coping strategies". Improving users' self-efficacy is an important objective, according to (LaRose et al., 2008). Marketing interventions, such as awareness and education, are the best way to improve self-efficacy (Milne et al., 2009). Thus, we hypothesize that:

H3: Self-efficacy mediates the negative effect of privacy controls on falsification of information.

3. Methods

3.1. *Data*

In October 2019 the author conducted an online survey among French-speaking consumers. At the beginning of the questionnaire, the respondents were told that their decision to participate in the study was voluntary and that they were free to withdraw from the study at any time. The author also explained that refusing to participate in the study, or withdrawing from it, would not result in any penalty or loss of benefits that they would otherwise receive. The respondents were assured them that the study was purely academic, that the results would be made available to the public in academic research journals, and that the data would remain confidential and would be treated anonymously, thus reducing common method bias (Podsakoff et al., 2003). The sample is composed of 207 French-speaking respondents. Women account for 71.5 % of the sample, the average age is $M_{age} = 24.10$ (SD = 6.61), and the respondents are mainly students (79.2 %) with a bachelor's degree (65.7 %).

3.2. *Measurement instruments*

The 7-point Likert scales are adapted from the literature: the questions for falsification of information (e.g. "*When thinking about how I provide personal information to Facebook, I am likely to give the company false information*") and vulnerability (e.g., "*The personal information that the company has about me makes me feel vulnerable*") come from Martin et al. (2017a), the items for self-efficacy (e.g., "*I am confident in my ability to use privacy controls on Facebook*") are adapted from Meuter et al. (2005), and the instruments for consumer control (e.g., "*On Facebook, I believe I have control over what happens to my personal information*") are adapted from Martin et al. (2017a) and Mothersbaugh et al. (2012).

3.3. *Research design*

A within-subject design was adopted to test the effect of privacy controls on falsification of information (Fig. 2). The process is as follows: first, the participants answered the questionnaire about the focal constructs (consumer control, vulnerability, self-efficacy, and falsification of information); second, they browsed their Facebook privacy settings (i.e., "About Facebook Ads" and "Your Ad Preferences"); and third, they answered the same questionnaire about the focal constructs.

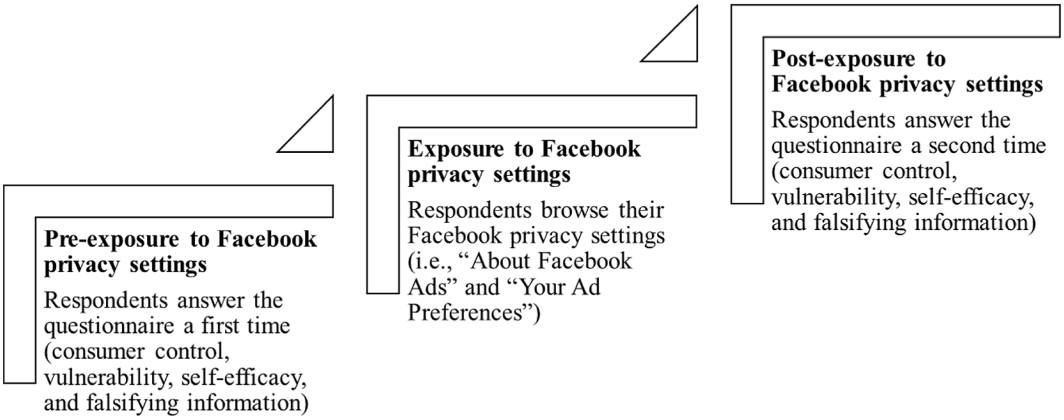
Pre-exposure to Facebook privacy settings
Respondents answer the questionnaire a first time (consumer control, vulnerability, self-efficacy, and falsifying information)
Exposure to Facebook privacy settings
Respondents browse their Facebook privacy settings (i.e., "About Facebook Ads" and "Your Ad Preferences")
Post-exposure to Facebook privacy settings
Respondents answer the questionnaire a second time (consumer control, vulnerability, self-efficacy, and falsifying information)

Fig. 2. Within-subject research design.

3.4. Method of analysis

Even though within-subject designs are common in marketing, less attention has been given to mediation analyses. To overcome this issue, Montoya and Hayes' (2017) procedure were implemented. Their mediation analyses for repeated measures are based on the work by Judd, Kenny, and McClelland (2001), which has been used in leading marketing journals (e.g., Spiller, 2011; Warren & Campbell, 2014). Montoya and Hayes (2017) followed the latest improvements in mediation analysis (i.e., bootstrap confidence intervals for inference about the indirect effect) to remedy the flawed Baron and Kenny (1986) approach of Judd, Kenny, and McClelland (2001) (i.e., causal-steps logic).

Following Montoya and Hayes (2017), the path coefficients of the research model can be estimated by the following set of equations:

Equation 1. First Segment of the Mediating Effect

$$M_{j2i} - M_{j1i} = a_j + e_{M_{ji}}$$

Equation 2. Second Segment of the Mediating Effect

$$Y_{2i} - Y_{1i} = c^{`} + \sum_{j=1}^{k} b_j\left(M_{j2i} - M_{j1i}\right) + \sum_{j=1}^{k} d_j[0.5\left(M_{j1i} + Mj2i\right) - \overline{0.5\left(M_{j1} + M_{j2}\right)}\,] + e_{Y*_i}$$

In Equations 1 and 2, M_{11} and M_{21} are the mediators before exposure to Facebook privacy settings (i.e., vulnerability and self-efficacy); M_{12} and M_{22} are the mediators after exposure to Facebook privacy settings; Y_1 (i.e., before exposure to Facebook privacy settings) and Y_2 (i.e., after exposure to Facebook privacy settings) are falsification of information. The specific indirect effect through mediator j is $\widehat{a}_j\widehat{b}_j$ and the total indirect effect, which is the sum of the specific indirect effects: $\sum_{j=1}^{k} a_j b_j$. To summarize, exposure to Facebook privacy settings impacts the differences in mediators' measurements (i.e., before vs after exposure to Facebook privacy settings), which in turn impact the difference in falsification of information. To make sure that the differences in mediators' measurements genuinely impact the difference in falsification of information, the model controls for the average of the mediators' measurements. The confidence interval method is bias-corrected bootstrap with 5,000 samples (Zhao et al., 2010).

3.5. Assessment of the measurement model

The author estimated the structural model on R 4.1.1 with the {lavaan} package (Rosseel, 2012) and used the{semTools} package (Jorgensen et al., 2021) to assess the reliability, the average variance extracted and the discriminant validity of the constructs.

The model with pre-exposure to Facebook privacy settings achieved a good fit according to the standard indices: chi-square test (161), degrees of freedom (84), root mean square error of approximation (RMSEA; 0.07), Tucker-Lewis index (TLI; 0.92), comparative fit index (CFI; 0.94), and the standardized root mean square residual (SRMR; 0.06). The model with post-exposure to Facebook privacy settings also achieved a rather good fit: chi-square test (177), degrees of freedom (84), root mean square error of approximation (RMSEA; 0.07), Tucker-Lewis index (TLI; 0.94), comparative fit index (CFI; 0.95), and the standardized root mean square residual (SRMR; 0.07).

The author then assessed the psychometric properties of the measurement instruments. Reliability (i.e., Cronbach's $\alpha > 0.7$; Table 3), convergent validity (i.e., average variance extracted (AVE) > 0.5; Table 3), and heterotrait-monotrait discriminant validity (i.e., heterotrait-monotrait ratio < 0.85 (Henseler et al., 2015); Tables 4 and 5) were all satisfactory.

3.6. Common method variance

Finally the author established that common method variance was not an issue for the study (Podsakoff et al., 2003). The author used the ConMET package (De Schutter, 2021) to test competitive models where items from two constructs load on the same latent variable. All the configurations significantly decreased the fit of the measurement model (i.e., χ^2 significantly increases with $p < .001$), as shown in Table 6. In addition, the author tested the performance of Harman's One Factor (Harman, 1967) and found from the results that it performed poorly compared to the measurement model ($p < .001$).

4. Results

4.1. Manipulation check

A paired *t*-test analysis shows that respondents report higher privacy control after exposure to Facebook privacy settings ($M_{\text{post-exposure}} = 3.69$, $SD = 1.39$) than before ($M_{\text{pre-exposure}} = 3.18$, $SD = 1.33$, $t_{(206)} = 5.10$, $p < .001$), thus supporting the manipulation. Similarly, respondents report higher self-efficacy after exposure to Facebook privacy settings ($M_{\text{post-exposure}} = 4.40$, $SD = 1.26$) than before ($M_{\text{pre-exposure}} = 4.21$, $SD = 1.21$, $t_{(206)} = 2.25$, $p < .025$). Conversely, they report lower vulnerability after exposure to Facebook privacy settings ($M_{\text{post-exposure}} = 4.21$, $SD = 1.30$) than before ($M_{\text{pre-exposure}} = 4.39$, $SD = 1.22$, $t_{(206)} = –2.49$, $p < .014$), as well as lower falsification of information after exposure to Facebook privacy settings ($M_{\text{post-exposure}} = 3.82$, $SD = 1.73$) than before ($M_{\text{pre-exposure}} = 3.95$, $SD = 1.68$, $t_{(206)} = –2.12$, $p < .036$).

4.2. Estimation of the research model

The results (Fig. 3) show that the direct and isolated effect of privacy

Table 3
Quality of the measurement instruments.

	α		AVE		Source
	Pre	Post	Pre	Post	
Falsifying information	0.88	0.92	0.71	0.79	Martin et al. (2017a)
When thinking about how I provide personal information to Facebook…					
…I am likely to give the company false information.					
…I purposely try to trick the company when providing my personal data.					
…I think it is fine to give misleading answers on personal questions					
Vulnerability	0.83	0.89	0.52	0.67	Martin et al. (2017a)
The personal information that the company has about me makes me feel…					
…insecure					
…exposed					
…threatened					
…vulnerable					
…susceptible					
Self-efficacy	0.79	0.84	0.53	0.61	Meuter et al. (2005)
I am fully capable of using privacy controls on Facebook.					
I am confident in my ability to use privacy controls on Facebook.					
Using privacy controls on Facebook is well within the scope of my abilities.					
My past experiences increase my confidence that I will be able to successfully use privacy controls on Facebook					
Consumer control	0.68	0.77	0.54	0.56	Martin et al. (2017a) Mothersbaugh et al. (2012)
On Facebook, I believe I have control over what happens to my personal information.					
It is up to me how much Facebook uses my information					
On Facebook, I have a say in whether my personal information is shared with others					

Table 4
HTMT discriminant validity (pre-exposure to Facebook privacy settings).

	M	*SD*	F	V	S	C
F	3.95	1.68	1.00			
V	4.39	1.22	0.16	1.00		
S	4.22	1.21	0.04	0.15	1.00	
C	3.18	1.33	0.26	0.14	0.50	1.00

Notes. F: Falsifying Information, V: Vulnerability, S: Self-efficacy, C: Control.

controls on the falsification of information is negative and significant (b = –0.14, p <.05), thus supporting H1. After the integration of the mediator, the negative effect is no longer significant (b = –0.08, p >.05), which is potential support for a fully mediated effect. Regarding the threat appraisal mechanism, the results show that vulnerability significantly increases falsification of information (b = 0.15, p <.05) and that privacy controls significantly decrease it (b = –0.18, p <.05), thus partially supporting H2. Regarding the coping appraisal mechanism, the results show that self-efficacy significantly decreases falsification of information (b = –0.12, p <.05) and that privacy controls significantly increase it (b = 0.19, p <.05) self-efficacy, thus partially supporting H3.

Table 5
HTMT discriminant validity (post-exposure to Facebook privacy settings).

	M	SD	F	V	S	C
F	3.82	1.73	1.00			
V	4.21	1.30	0.25	1.00		
S	4.40	1.26	0.08	0.25	1.00	
C	3.69	1.39	0.08	0.19	0.67	1.00

Notes. F: Falsifying Information, V: Vulnerability, S: Self-efficacy, C: Control.

Table 6
Estimation of common method variance.

Models	Pre-exposure to Facebook privacy settings			Post-exposure to Facebook privacy settings		
	χ2	df	Δχ2	χ2	df	Δχ2
Proposed model	161	84		177	84	
C and S	264	87	103***	265	87	88***
C and V	319	87	157***	402	87	225***
C and F	307	87	146***	644	87	467***
S and V	592	87	431***	904	87	727***
S and F	499	87	338***	645	87	468***
V and F	492	87	332***	618	87	441***
Harman's One Factor	910	90	749***	1445	90	1268***

Notes. F: Falsifying Information, V: Vulnerability, S: Self-efficacy, C: Control, *** p <.001.

4.3. Mediation analysis for repeated measures

The results of the mediation analysis for repeated measures (Table 7) show that the total indirect effect of privacy controls on the falsification of information is negative and significant (b = –0.05, p <.01, 99 % CI = [–0.1215, –0.0036]. Similarly, the specific indirect effects that arising from vulnerability (b = –0.03, p <.05, 95 % CI = [–0.0709, –0.0007]) and self-efficacy (b = –0.02, p <.05, 95 % CI = [–0.0548, –0.0004]) are negative and significant, thus supporting H2 and H3. The pairwise contrast between the two specific indirect effect shows no significant difference (b = –0.01, p >.05, 95 % CI = [–0.0577, 0.0365]).

4.4. Robustness checks

4.4.1. Post-hoc power analysis

The post-hoc power analysis is able to determine whether the sample size is sufficient to provide robust estimates (Moshagen & Erdfelder, 2016). The author used the semPower package (Jobst et al., 2021) to evaluate the power of the analysis. The pre- and post-exposure to Facebook privacy settings model, given that RMSEA is 0.07, the sample size is 207, the degrees-of-freedom are 84, and the alpha is 0.05, the computation shows that the power is satisfactory (>0.999). Fig. 4 shows the associated central and non-central χ^2 distributions.

4.4.2. Controlling for privacy concerns

To account for potential confounding effects, the author controlled for privacy concerns in a supplementary mediation analysis for repeated measures. The scale is taken from Malhotra et al. (2004) and is reliable (a > 0.7 for the pre- and post-exposure to Facebook privacy settings). The results show that the total indirect effect from privacy controls on the falsification of information is negative and significant (b = –0.06, p <.05, 95 % CI = [–0.1130, –0.0156]. With regard to the new mediator, the specific indirect effect that runs through privacy concerns is not significant (b = –0.01, p <.05, 95 % CI = [–0.0366, 0.0138]). In line with

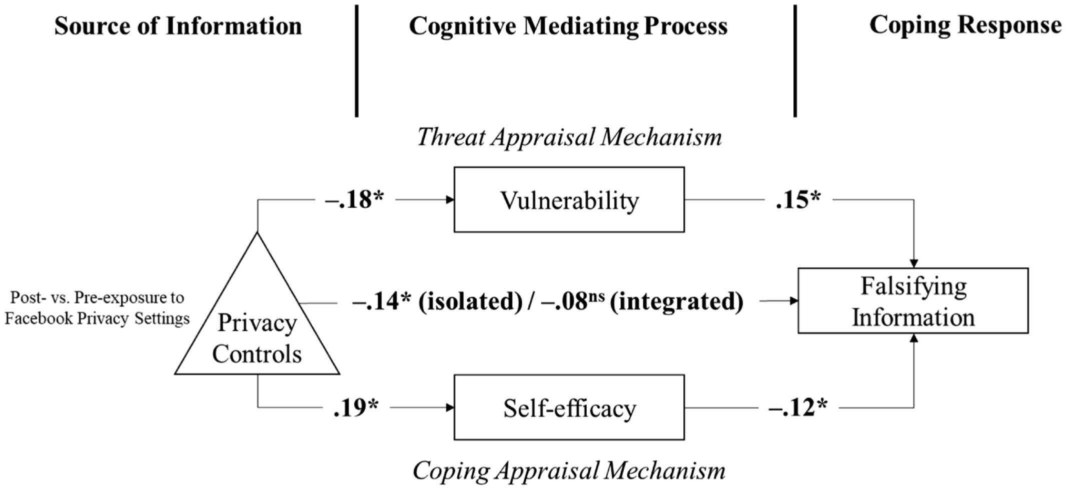
Source of Information
Cognitive Mediating Process
Coping Response
Threat Appraisal Mechanism
–.18*
Vulnerability
.15*
Post- vs. Pre-exposure to Facebook Privacy Settings
Privacy Controls
–.14* (isolated) / –.08ns (integrated)
Falsifying Information
.19*
Self-efficacy
–.12*
Coping Appraisal Mechanism

Fig. 3. Results of the estimation (within-subject design).

Table 7
Results of the mediation analysis for repeated measures.

	Effect	95 % CI		99 % CI	
		Lower	Upper	Lower	Upper
Total	–0.05**	–0.1019	–0.0131	–0.1215	–0.0036
Vulnerability	–0.03*	–0.0709	–0.0007	–0.0917	0.0049
Self-efficacy	–0.02*	–0.0548	–0.0004	–0.0687	0.0082

Notes. ***p* <.01, **p* <.05.

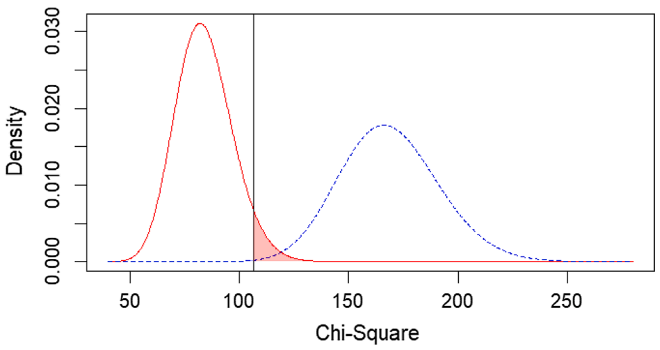

Fig. 4. Associated central and non-central χ^2 distribution.

H2 and H3, the results for the two core mediators are consistent. Indeed, the specific indirect effects that run through vulnerability (b = –0.03, p <.05, 95 % CI = [–0.0683, –0.0001]) and self-efficacy (b = –0.02, p <.05, 95 % CI = [–0.0556, –0.0001]) are negative and significant.

5. Discussion

5.1. Academic contributions

The present research contributes to the literature in several ways. First, privacy control is conceptualized as a source of information in a protection motivation framework (Rogers, 1975), which no prior research has done (cf. Table 2). The aim is to explore an under-represented coping response (i.e., falsification of information), as only two prior studies investigate falsification through protection motivation theory (Alashoor et al., 2017; Youn, 2009). The results from the within-subject design experiment show that the direct effect of privacy control on the falsification of information is significant and negative. This negative direct effect becomes non-significant when integrated into the mediation model. While the literature only shows a significant direct impact of control on the falsification of information (M. O. Lwin & Williams, 2003), the results of the mediation for repeated measures reveal the key role of the cognitive mediating process (i.e., the effect privacy control as a source of information on falsification of information is fully mediated).

Second, the author provides two key constructs for the fully mediated model. In line with prior research (Boss et al., 2015; Crossler & Bélanger, 2014), the author includes vulnerability as a threat appraisal mechanism and self-efficacy as a coping appraisal mechanism. The results of the mediation for repeated measures show that both indirect effects are significant and negative. Regarding the threat appraisal mechanism, privacy controls as a source of information reduces vulnerability, which, in turn, increases the falsification of information. Conversely, for the coping appraisal mechanism, privacy controls as a source of information increase self-efficacy, which in turn reduces falsifying information. This mediation role of vulnerability and self-efficacy extends prior work on falsification and protection motivation theory, in which these constructs were not part of a psychological mechanism (Youn, 2009).

Third, as part of the mediation analysis for repeated measures, the results of the pairwise contrast analysis show that the strength of the threat appraisal mechanism and of the coping appraisal mechanism are statistically the same (i.e., there is no significant difference between the two indirect effects). This finding is of importance because the theory states that if the coping appraisal mechanism (resp. threat appraisal mechanism) outweighs the threat appraisal mechanism (resp. the coping appraisal mechanism), the coping response is more likely to be adaptive (resp. maladaptive) (Tanner et al., 1991). By balancing these effects, the author extends research on privacy protection motivation theory (Boss et al., 2015; Crossler & Bélanger, 2014).

5.2. Managerial implications

In March 2019, Facebook announced that it had discovered that some passwords were stored in plaintext, that is, without protection to make them unreadable (a standard security measure) (Time, 2019). The discovery was made in January 2019 during a routine review conducted by the social network. In total, between 200 and 600 million Facebook users were affected by the situation, an internal Facebook source said.. About nine million requests would have been made internally by some 2,000 Facebook engineers and developers to access these passwords. In the following days, Facebook displayed a native post on how to create a strong password – a marketing intervention just like the one in the present research (i.e., exposure to Facebook privacy settings). The results of the present research show that this kind of marketing intervention helps reduce privacy-protecting behaviors such as the falsification of information.

The within-subject design approach allows the results to be robust among all consumers on average. It is critical because the success of such a marketing intervention (e.g., showing privacy settings to consumers) depends on its successful implementation (Bieler et al., 2021). The within-subject design experiment evaluates the constructs before and after a treatment (e.g., showing privacy settings to consumers). The author also provides insights regarding the important trade-off between reducing consumer vulnerability and maintaining the usefulness of the data (Zhang & Watson IV, 2020). Indeed, using privacy controls as a source of information helps reduce vulnerability. The data is less likely to be falsified because the total indirect effect that runs from privacy controls to falsifying information is negative and significant.

5.3. Limitations and future research

This research has certain limitations. First, the author is aware that Facebook privacy settings can provide illusory privacy control, as the firm chooses the settings in the first instance (Acquisti et al., 2020). Such illusory privacy control can be harmful for consumers, as they are more likely to take privacy-related risks (Acquisti et al., 2020). Future research could perhaps directly manipulate the privacy settings instead of using a real-world example, which would enable researchers to find ways to remedy the potential illusory privacy control.

Second, the author only investigates falsifying behavior as a coping response, whereas there are many other possibilities (Martin et al., 2017a). For example, researchers could implement the same within-subject design to investigate web privacy protection techniques such as Privacy Badger or Disconnect, which are the most effective on the market (Mazel et al., 2019).

Third, low R^2 levels suggest that further research could integrate the present research model. While the author controlled for privacy concerns – a key antecedent of falsification –, other mediators could be added. For example, in line with social exchange theory (that has also been used to explain falsification (cf. Chen et al., 2021; Horne et al., 2007)), further research could integrate trust as a mediator (cf. Bandara et al., 2021; S. (Joseph) Chen et al., 2021; Martin et al., 2017a; and Miltgen & Smith, 2019 for the link between trust and falsification). Recent research on privacy and new technologies also suggest that well-being might be a relevant mediator (Meyer-Waarden et al., 2022; Meyer-Waarden & Cloarec, 2022).

Finally, even though the within-subject design reduces the importance of demographics in terms of analysis, the current sample is limited mainly to French students. Further research should explore other populations. For instance, comparison could be made between the United States (opt-out privacy policy) and the European Union (opt-in privacy policy) (Kumar et al., 2014).

CRediT authorship contribution statement

Julien Cloarec: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization.

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. (2020). Secrets and likes : The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758. https://doi.org/10.1002/jcpy.1191

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox : The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems, 41*, 62–96. https://doi.org/10.17705/1CAIS.04104.

Alkire, L., Pohlmann, J., & Barnett, W. (2019). Triggers and motivators of privacy protection behavior on Facebook. *Journal of Services Marketing, 33*(1), 57–72. https://doi.org/10.1108/JSM-10-2018-0287

Anderson, L., Spanjol, J., Jefferies, J. G., Ostrom, A. L., Nations Baker, C., Bone, S. A., Downey, H., Mende, M., & Rapp, J. M. (2016). Responsibility and well-being: Resource integration under responsibilization in expert services. *Journal of Public Policy & Marketing, 35*(2), 262–279. https://doi.org/10.1509/jppm.15.140

Aubert-Hassouni, C., & Cloarec, J. (2022). Privacy regulation in the age of artificial intelligence. In *SAGE Handbook of Digital Marketing*. SAGE Publications Ltd.

Bandara, R. J., Fernando, M., & Akter, S. (2021a). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing, 55*(1), 219–246. https://doi.org/10.1108/EJM-06-2019-0515

Bandara, R. J., Fernando, M., & Akter, S. (2021b). Construing online consumers' information privacy decisions : The impact of psychological distance. *Information & Management, 58*(7), Article 103497. https://doi.org/10.1016/j.im.2021.103497

Bandura, A. (1986). *Social foundations of thoughts and action.* Prentice-Hall.

Bandura, A. (1993). Perceived self-efficacy in cognitive development and functioning. *Educational Psychologist, 28*(2), 117–148. https://doi.org/10.1207/s15326985ep2802_3

Bandura, A. (1997). Self-efficacy: The exercise of control. *Freeman.*

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

Bieler, M., Maas, P., Fischer, L., & Rietmann, N. (2021). Enabling cocreation with transformative interventions: An interdisciplinary conceptualization of consumer boosting. *Journal of Service Research, 109467052110036*. https://doi.org/10.1177/10946705211003676

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Bright, L. F., Lim, H. S., & Logan, K. (2021). "Should I Post or Ghost?" : Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing, mar.21499*. https://doi.org/10.1002/mar.21499

Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing, 40*(1), 108–110. https://doi.org/10.1177/0743915620929999

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Chen, K., & Rea, A. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems, 44*(4), 85–92.

Chen, S.(Joseph), Waseem, D., Xia, Z.(Raymond), Tran, K. T., Li, Y., & Yao, J. (2021). To disclose or to falsify : The effects of cognitive trust and affective trust on customer cooperation in contact tracing. *International Journal of Hospitality Management, 94*, Article 102867. https://doi.org/10.1016/j.ijhm.2021.102867

Chen, W., Huang, G., Miller, J., Lee, K.-H., Mauro, D., Stephens, B., & Li, X. (2018). "As we grow, it will become a priority" : American mobile start-ups' privacy practices. *American Behavioral Scientist, 62*(10), 1338–1355. https://doi.org/10.1177/0002764218787867

Cloarec, J. (2020). The personalization-privacy paradox in the attention economy. *Technological Forecasting and Social Change, 161*, Article 120299. https://doi.org/10.1016/j.techfore.2020.120299

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing, 49*(3), mar.21587. https://doi.org/10.1002/mar.21587

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Crossler, R. E., & Bélanger, F. (2019). Why would i use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge-belief gap. *Information Systems Research, 30*(3), 995–1006. https://doi.org/10.1287/isre.2019.0846

Culnan, M. J. (1995). Consumer awareness of name removal procedures : Implications for direct marketing. *Journal of Direct Marketing, 9*(2), 10–19. https://doi.org/10.1002/dir.4000090204

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly, 33*(4), 673–687.

De Schutter, L. (2021). *conmet: Construct Measurement Evaluation Tool* (0.1.0) [Computer software]. https://CRAN.R-project.org/package=conmet.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets : Ethical challenges and opportunities. *Journal of Business Research, 129*, 961–974. https://doi.org/10.1016/j.jbusres.2020.08.024

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Grégoire, Y., & Fisher, R. J. (2008). Customer betrayal and retaliation : When your best customers become your worst enemies. *Journal of the Academy of Marketing Science, 36*(2), 247–261. https://doi.org/10.1007/s11747-007-0054-0

Harman, H. H. (1967). *Modern factor analysis*. University of Chicago Press.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hibbert, S., Winklhofer, H., & Temerak, M. S. (2012). Customers as resource integrators: Toward a model of customer learning. *Journal of Service Research, 15*(3), 247–261. https://doi.org/10.1177/1094670512442805

Horne, D. R., Norberg, P. A., & Cemal Ekin, A. (2007). Exploring consumer lying in information-based exchanges. *Journal of Consumer Marketing, 24*(2), 90–99. https://doi.org/10.1108/07363760710737094

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management, 54*(7), 851–865. https://doi.org/10.1016/j.im.2017.01.001

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Jobst, L. J., Bader, M., & Moshagen, M. (2021). A tutorial on assessing statistical power and determining sample size for structural equation models. *Psychological Methods*. https://doi.org/10.1037/met0000423

Jorgensen, T. D., Pornprasertmanit, S., Schoemann, A. M., & Rosseel, Y. (2021). *semTools: Useful Tools for Structural Equation Modeling*. https://cran.r-project.org/package=semTools.

Judd, C. M., Kenny, D. A., & McClelland, G. H. (2001). Estimating and testing mediation and moderation in within-subject designs. *Psychological Methods, 6*(2), 115–134. https://doi.org/10.1037/1082-989X.6.2.115

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy : An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce : A systematic review and agenda for future research. *Journal of Business Research, 126*, 221–238. https://doi.org/10.1016/j.jbusres.2020.12.006

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions? *Journal of Interactive Marketing, 39*(3), 39–54. https://doi.org/10.1016/j.intmar.2017.03.001

Kshetri, N. (2014). Big data׳s impact on privacy, security and consumer welfare. *Telecommunications Policy, 38*(11), 1134–1145. https://doi.org/10.1016/j.telpol.2014.10.002

Kumar, V., Zhang, X.(Alan), & Luo, A. (2014). Modeling customer opt-in and opt-out in a permission-based marketing context. *Journal of Marketing Research, 51*(4), 403–419. https://doi.org/10.1509/jmr.13.0169

Kuo, K.-M., Ma, C.-C., & Alexander, J. W. (2014). How do patients respond to violation of their information privacy? *Health Information Management Journal, 43*(2), 23–33. https://doi.org/10.1177/183335831404300204

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong : Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research, 135*, 559–571. https://doi.org/10.1016/j.jbusres.2021.06.054

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71–76. https://doi.org/10.1145/1325555.1325569

Le Monde. (2022). *Contre la surveillance en ligne, des internautes «empoisonnent» leurs données personnelles*. https://www.lemonde.fr/pixels/article/2022/04/29/contre-la-surveillance-en-ligne-des-internautes-empoisonnent-leurs-donnees-personnelles_6124107_4408996.html.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research, 122*, 875–888. https://doi.org/10.1016/j.jbusres.2019.10.006

Lwin, M. O., & Williams, J. D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters, 14*(4), 257–272. https://doi.org/10.1023/B:MARK.0000012471.31858.e5

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses : A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572–585. https://doi.org/10.1007/s11747-006-0003-3

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy : A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy : Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., … Weaven, S. K. (2020). Data privacy in retail. *Journal of Retailing, 96*(4), 474–489. https://doi.org/10.1016/j.jretai.2020.08.003

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Mattison Thompson, F., & Siamagka, N. (2022). Counteracting consumer subversion : Organizational privacy ethical care as driver of online information sharing. *Psychology & Marketing, 39*(3), 549–597. https://doi.org/10.1002/mar.21579

Mazel, J., Garnier, R., & Fukuda, K. (2019). A comparison of web privacy protection techniques. *Computer Communications, 144*, 162–174. https://doi.org/10.1016/j.comcom.2019.04.005

Meuter, M. L., Bitner, M. J., Ostrom, A. L., & Brown, S. W. (2005). Choosing among alternative service delivery modes : An investigation of customer trial of self-service technologies. *Journal of Marketing, 69*(2), 61–83. https://doi.org/10.1509/jmkg.69.2.61.60759

Meyer-Waarden, L., & Cloarec, J. (2022). "Baby, you can drive my car" : Psychological antecedents that drive consumers' adoption of AI-powered autonomous vehicles. *Technovation, 109*, Article 102348. https://doi.org/10.1016/j.technovation.2021.102348

Meyer-Waarden, L., Cloarec, J., Adams, C., Aliman, D. N., & Wirth, V. (2022). Home, sweet home: How well-being shapes the adoption of artificial intelligence-powered apartments in smart cities: *Systèmes d'information & management, Volume 26*(4), 55-88. https://doi.org/10.3917/sim.214.0055.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Miltgen, C. L., & Smith, H. J. (2019). Falsifying and withholding : Exploring individuals' contextual privacy-related decision-making. *Information & Management, 56*(5), 696–717. https://doi.org/10.1016/j.im.2018.11.004

Montoya, A. K., & Hayes, A. F. (2017). Two-condition within-participant statistical mediation analysis: A path-analytic framework. *Psychological Methods, 22*(1), 6–27. https://doi.org/10.1037/met0000086

Morewedge, C. K., Monga, A., Palmatier, R. W., Shu, S. B., & Small, D. A. (2021). Evolution of consumption: A psychological ownership framework. *Journal of Marketing, 85*(1), 196–218. https://doi.org/10.1177/0022242920957007

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93*, 96–105.

Moshagen, M., & Erdfelder, E. (2016). A new strategy for testing structural equation models. *Structural Equation Modeling: A Multidisciplinary Journal, 23*(1), 54–60. https://doi.org/10.1080/10705511.2014.950896

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context. *Journal of Service Research, 15*(1), 76–98. https://doi.org/10.1177/1094670511424924

Mourey, J. A., & Waldman, A. E. (2020). Past the privacy paradox : The importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research, 5*(2), 162–180. https://doi.org/10.1086/708034

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems, 135*, Article 113323. https://doi.org/10.1016/j.dss.2020.113323

Norberg, P. A., & Horne, D. R. (2014). Coping with information requests in marketing exchanges : An examination of pre-post affective control and behavioral coping. *Journal of the Academy of Marketing Science, 42*(4), 415–429. https://doi.org/10.1007/s11747-013-0361-6

Palmatier, R. W., & Martin, K. D. (2019). Data privacy marketing audits, benchmarking, and metrics. In *The intelligent marketer's guide to data privacy* (pp. 153–168). Springer International Publishing. https://doi.org/10.1007/978-3-030-03724-6_8.

Peltier, J. W., Milne, G. R., & Phelps, J. E. (2009). Information privacy research : Framework for integrating multiple publics, information channels, and responses. *Journal of Interactive Marketing, 23*(2), 191–205. https://doi.org/10.1016/j.intmar.2009.02.007

Poddar, A., Mosteller, J., & Ellen, P. S. (2009). Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs, 43*(3), 419–448. https://doi.org/10.1111/j.1745-6606.2009.01147.x

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research : A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Punj, G. (2017). Consumer intentions to falsify personal information online : Unethical or justifiable? *Journal of Marketing Management, 33*(15–16), 1402–1412. https://doi.org/10.1080/0267257X.2017.1348011

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosseel, Y. (2012). lavaan : An R package for structural equation modeling. *Journal of Statistical Software, 48*(2), 1–36.

Smith, E. R. (2014). Evil acts and malicious gossip : A multiagent model of the effects of gossip in socially distributed person perception. *Personality and Social Psychology Review, 18*(4), 311–325. https://doi.org/10.1177/1088868314530515

Spiller, S. A. (2011). Opportunity cost consideration. *Journal of Consumer Research, 38* (4), 595–610. https://doi.org/10.1086/660045

Spreitzer, G. M. (1995). Psychological empowerment in the workplace : Dimensions, measurement, and validation. *Academy of Management Journal, 38*(5), 1442–1465. https://doi.org/10.5465/256865

Steinhoff, L., Arli, D., Weaven, S., & Kozlenkova, I. V. (2019). Online relationship marketing. *Journal of the Academy of Marketing Science, 47*(3), 369–393. https://doi.org/10.1007/s11747-018-0621-6

Swani, K., Milne, G. R., & Slepchuk, A. N. (2021). Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices : Replication and extension. *Journal of Interactive Marketing, 56*, 137–158. https://doi.org/10.1016/j.intmar.2021.03.001

Tanner, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model : A normative model of fear appeals. *Journal of Marketing, 55*(3), 36–45. https://doi.org/10.1177/002224299105500304

The Wall Street Journal. (2018). *You Weren't Born in 1905? Why People Lie to Facebook*. https://www.wsj.com/articles/you-werent-born-in-1910-why-people-lie-to-facebook-1522682361.

Time. (2019). *Facebook Employees Had Access to « Hundreds of Millions » of Users' Passwords*. https://time.com/5556152/facebook-passwords-employees/.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. https://doi.org/10.1509/jmr.10.0355

Warren, C., & Campbell, M. C. (2014). What makes things cool ? How autonomy influences perceived coolness. *Journal of Consumer Research, 41*(2), 543–563. https://doi.org/10.1086/676680

Wottrich, V. M., Reijmersdal, E. A., & Smit, E. G. (2019). App users unwittingly in the spotlight : A model of privacy protection in mobile apps. *Journal of Consumer Affairs, 53*(3), 1056–1083. https://doi.org/10.1111/joca.12218

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns : A study of location-based services. *Information Systems Research, 23*(4), 1342–1363. https://doi.org/10.1287/isre.1120.0416

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710–722. https://doi.org/10.1002/asi.20530

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zhang, J. Z., & Watson, G. F., IV (2020). Marketing ecosystem : An outside-in view for sustainable advantage. *Industrial Marketing Management, 88*, 287–304. https://doi.org/10.1016/j.indmarman.2020.04.023

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering baron and kenny : Myths and truths about mediation analysis. *Journal of Consumer Research, 37*(2), 197–206. https://doi.org/10.1086/651257

Julien Cloarec is an Assistant Professor of Data Science at iaelyon School of Management, Université Jean Moulin Lyon 3. He holds an M.Eng. in Computer Science, as well as a Ph.D. in Management Science, for which he was awarded the Best Thesis Prize by the French-Foundation for Management Education (FNEGE) and a Special Distinction by the French Marketing Association (AFM). He is Vice-President of the French Society of Management and a Board/Council Member of the French Marketing Association. As an academic, he seeks to offer insights on consumer privacy and artificial intelligence. His research was published in several journals, such as Psychology & Marketing, Technovation, Technological Forecasting and Social Change, and the French Journal of Management Information Systems.