Technological Forecasting & Social Change 200 (2024) 123101

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

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

Tracking technologies in eHealth: Revisiting the personalization-privacy paradox through the transparency-control framework

Julien Cloarec [a,*], Charlotte Cadieu [a], Nour Alrabie [b]

[a] Université Jean Moulin Lyon 3, iaelyon School of Management, Magellan, Lyon, France
[b] LEREPS, Université Toulouse Jean Jaurès, Toulouse, France

ARTICLE INFO

Keywords:
Personalization
Privacy
Transparency
Control
Cookies
Ehealth

ABSTRACT

Our research highlights the evolving landscape of online privacy, emphasizing the growing compliance pressure on tech companies and website owners due to GDPR regulations, particularly concerning cookie banners. The regulation of these banners for personalization underscores the trade-off known as the personalization-privacy paradox. Although recent studies emphasize the positive role of transparency and control in enhancing the digital experience, they often approached them in a static and isolated manner. We introduce a new approach to operationalizing transparency and control in our study within the context of Doctissimo, a well-known French health and wellness website recognized for aggregating user-generated health data and employing advertising trackers for marketing objectives. In Study 1, we examined banner transparency, demonstrating its positive effect on click-through intention via a preference for personalization over privacy. Study 2 focused on banner privacy controls and revealed that the impact of control was entirely mediated by the intrusion of information boundaries and the preference for personalization over privacy. This research contributes to the literature by investigating the personalization privacy paradox using an innovative operationalization within the transparency-control framework.

1. Introduction

The issue of online privacy has been a hot topic in recent years, particularly since the introduction of the European Union's General Data Protection Regulation (GDPR). Tech companies and website owners are now under increasing scrutiny to ensure compliance with GDPR's requirements for transparency, consent, and control over personal data. One area that has come under particular scrutiny is the use of cookie banners (Forbes, 2022), which are designed to inform website visitors about the use of cookies and obtain their consent.

Recent news highlight the challenges faced by website owners in complying with GDPR's requirements for cookie banners. A multi-year investigation into TechCrunch's parent entity Yahoo by the Irish Data Protection Commission has focused on compliance with key transparency requirements, including cookie banners displayed on its media properties (TechCrunch, 2022a, 2022b). The French data protection watchdog, CNIL, has fined TikTok €5 million for violating rules on cookie consent (TechCrunch, 2023). The regulator found that the cookie-consent flow on TikTok's website made it easier for users to accept cookies than to refuse them, essentially manipulating consent. Google has shared a new cookie consent popup, which will be first available on YouTube in France before rolling out across Google services in Europe. This comes after the CNIL fined Google €150 million for failing to comply with regulations on presenting tracking choices to users (TechCrunch, 2022a). Meanwhile, noyb has filed numerous GDPR complaints against websites that use the popular cookie banner software OneTrust with deceptive settings, highlighting the need for greater transparency and control over how personal data is collected and used (noyb, 2022).

Other organizations discuss the importance of transparency and control over personal data in relation to contractual obligations. The International Association of Privacy Professionals (IAPP) has outlined a number of key considerations for determining whether data processing is necessary for the performance of a contractual service, including the core substance and purpose of the contract, whether there are less intrusive alternatives for processing, and the bargaining power of the parties involved (IAPP, 2023). In addition, the IAPP emphasizes the importance of transparency in setting out what users are agreeing to when they sign up for a service or use a website. As individuals become increasingly aware of the ways in which their data is collected and used,

* Corresponding author.
E-mail addresses: julien.cloarec@univ-lyon3.fr (J. Cloarec), charlotte.cadieu@univ-lyon3.fr (C. Cadieu), nour.alrabie@univ-tlse2.fr (N. Alrabie).

https://doi.org/10.1016/j.techfore.2023.123101
Received 30 August 2022; Received in revised form 8 December 2023; Accepted 9 December 2023
Available online 20 December 2023
0040-1625/© 2023 Elsevier Inc. All rights reserved.

website owners and tech companies must take steps to ensure compliance with GDPR and other privacy regulations. This underscores the importance of transparency, consent, and control over personal data in the digital age.

The tension between personalization and privacy in the digital marketing experience has become increasingly important as consumer data is gathered, analyzed, and managed to enhance marketing performance (Wedel and Kannan, 2016). The personalization-privacy paradox conceptualized by Cloarec (2020) integrates two perspectives: consumers appreciate the value of personalization, yet the exploitation of personal information by marketers raises privacy concerns. Consequently, consumers may refuse to provide personal information, limiting personalization efforts (Awad and Krishnan, 2006; Sutanto et al., 2013). Recent research indicates that transparency and control can improve the digital experience by empowering consumers (Palmatier and Martin, 2019). Transparency refers to the ways firms disclose their collection and use of consumer personal data to generate behaviorally targeted ads (Kim et al., 2019), while control refers to the extent to which consumers feel they have control over their personal information and how it is used (Mothersbaugh et al., 2012). However, prior studies have considered transparency and control on a static level, either studied separately (Kim et al., 2019) or together (Martin et al., 2017; Palmatier and Martin, 2019).

With more interactive interfaces, such as web cookies management, control features depend on the degree of transparency offered in the first instance. In the context of digital privacy, Zhu et al. (2021) suggest that transparency and control refer to distinct cognitive routes from the elaboration likelihood theory: control perception derives from a logical, rational, central route, while transparency perception derives from a peripheral route prone to cognitive biases. This insight suggests that previous operationalizations of transparency and control are limited, and a more realistic analysis of the roles of transparency and control is required. Therefore, the research question arises: how can an operationalization of transparency and control that follows the elaboration likelihood theory help us better understand the personalization-privacy trade-offs in digital marketing? By addressing this question, we may develop more effective transparency and control mechanisms that balance personalization with privacy and reduce the tension between these two objectives (Chen et al., 2023).

The context of the studies is the use of a popular French health and wellbeing website, Doctissimo, which collects user-generated health data and implements advertising trackers for marketing purposes. The website has attracted media groups since 2008, and its value has risen up to 15 million euros in 2018. Despite being distinct from clinical information and settings, the user-generated health data is sensitive and requires specific attention. The flow of the studies involves two experiments. In Study 1, an inter-subject design was used to manipulate the level of transparency of the cookie banner, and measurement scales were used for transparency, personalization over privacy, and click-through intention. Topic modeling was also conducted on the open-ended question answers. In Study 2, an intra-subject design was used, and the intervention involved displaying the privacy controls of the cookie banner. Respondents answered questions before and after the experiment, and the results supported hypotheses related to privacy controls, intrusion of information boundaries, personalization over privacy, and click-through intention. Overall, the studies aimed to investigate the personalization privacy paradox within the transparency-control framework.

Our study significantly advances the understanding of the personalization privacy paradox, transparency, and control in the realm of digital environments. Firstly, we clarify the connection between transparent privacy interfaces and consumers' preference for personalization over privacy concerns, revealing that transparency amplifies this preference. Secondly, based on consumer input, we emphasize the pivotal role of information boundary intrusion as a mediator between transparency and the inclination towards personalization over privacy. Thirdly, our research confirms that perceived transparency positively impacts the acceptance of cookie tracking. Our research also shows that control plays a significant role, with an increase in acceptance observed upon the introduction of control settings. These insights are instrumental for organizations in designing privacy interfaces that strike a balance between personalization and privacy. Understanding the impacts of transparency and control allows for the creation of interfaces that encourage users to accept cookie tracking while respecting their privacy concerns. Moreover, our study underscores the necessity of compliance with legal transparency requirements for enhancing user acceptance of cookie tracking.

2. Background

2.1. Tracking technologies for marketing purposes

The mere presentation of privacy practices has been shown to influence consumers' experiences (Miltgen and Smith, 2019) and their disclosure intentions (Martin and Murphy, 2017; Mothersbaugh et al., 2012). This social contract has evolved with the development of regulations for tracking (Martin, 2016), moving from an access-based view where consumers' data can be leveraged as they use the service, to the control and fair information principle where consumers become responsible for understanding and providing consent regardless of its appropriateness (Martin, 2016). Consumers then make decisions based on whether the perceived benefits outweigh the costs (Martin and Murphy, 2017). However, other issues also come into play, such as visibility and readability (Vail et al., 2008), information overload, and consumer fatigue. Therefore, tracking banners in the interface seem to be a more realistic social contract than policies upon which consumers must make decisions and act.

Tracking is a fundamental technology in online advertising and marketing, relying on a text file dropped on users' browsers. Some tracking functions only during a visit, while others persist and follow consumers across their online content consumption. Collected data from tracking is shared among actors, including advertising platforms and data aggregators, to consolidate advertising segments and user profiles for customized content and advertising (Trusov et al., 2016). Legislators have framed the use of tracking, such as the European Union Directive 2009/136/CE and the General Data Protection Regulation 2016. In France, since 2013, the CNIL has imposed the tracking banners interface, applying the "control and fair information principle" (Martin, 2016). Since 2016, GDPR requires informed consent before any tracking that can potentially identify European citizens online. The consent must be free, specific, and informed, and consumers must consent to every type of tracking. However, the multiplication of choices and legal requirements often results in lengthy policies. This approach assumes that the user is responsible for the consequences of their consent, particularly in case of privacy violation. Despite policies gaining almost 20 % in simplicity (Linden et al., 2020), research has shown that it is not systematic for websites to comply with their legal requirements in terms of transparency and control (Degeling et al., 2019). To retain as much data as possible, many organizations that have invested in programmatic advertising play cat and mouse with the law.

2.2. The personalization-privacy paradox

Personalization is a marketing technique that involves tailoring marketing-mix elements to individual consumers based on their preferences, and assessing the effectiveness of the resulting actions (Wedel and Kannan, 2016). Personalized ads are designed to capture consumers' attention, and their accuracy is key to their effectiveness (Li and Karahanna, 2015; Sahni et al., 2018; Tam and Ho, 2006). To personalize products or services, firms collect customer data either implicitly or explicitly (Sundar and Marathe, 2010; Wattal et al., 2009). Consumers' voluntary disclosure of personal information enables social networking

sites to offer customized recommendations, products, and services, which enhance user satisfaction (Chen, 2013). However, individuals are increasingly hesitant to provide their personal information due to privacy concerns (Awad and Krishnan, 2006).

Consequently, many consumers adopt strategies to avoid disclosing their personal information to firms, which may limit the effectiveness of personalization efforts (Financial Times, 2017; Harris Interactive, 2016). However, firms require data for optimal targeting through personalization, resulting in a continual tension between firms and individuals. This phenomenon is known as the personalization-privacy paradox, which refers to the ongoing conflict between consumers' appreciation of the value of personalization and their concerns about the exploitation of their personal information (Cloarec, 2020).

2.3. The transparency-control framework

The transparency-control framework is based on the concept of procedural fairness (Eggers et al., 2023; Gouthier et al., 2022), where transparency and control play a crucial role in ensuring fair and ethical data collection and usage (Wiertz and Kittinger-Rosanelli, 2021). Despite the potential benefits of personalization for consumers, they may still be dissatisfied if they feel they were not adequately informed about the data collection process (Eggers et al., 2023). The importance of transparency is reflected in the GDPR in the EU, where firms are required to provide consumers with control over not just data collection but also data storage and use. The significance of transparency and control is even more pronounced in sensitive industries (Eggers et al., 2023). Studies have shown that providing more transparency and control over data collection can positively impact the acceptance of information collection. Transparency and control are also recognized as privacy-enhancing factors that help fight the unintended consequences of digital marketing (Evans et al., 2022). Transparency refers to firms disclosing the ways in which they collect and use consumer data (Kim et al., 2019), while control is the extent to which consumers feel they have control over their personal information (Mothersbaugh et al., 2012). Lack of consideration for privacy concerns can lead to outdated technology or algorithms, which in turn results in a lack of transparency and control for potential and current users about how data is used (Lobschat et al., 2021). This highlights the importance of transparency and control policies that are widely shared by companies (Rasoulian et al., 2023). Although public policy drives privacy regulations, firms should focus more on willingly granting consumers more transparency and control over their data (Schumacher et al., 2023). Transparency regarding how organizations uses customer data is essential (Bleier et al., 2020). Coercion or forcing customers, particularly in automated processes, to surrender privacy and data to access a service is questionable (Puntoni et al., 2021). External auditing of service design characteristics against industry standards and regulatory requirements of CDR may be necessary in the future (Wirtz et al., 2023).

Table 1 presents a summary of recent research on the relationship between transparency and control, and their effects on different aspects of privacy and data protection. Martin et al.'s (2017) study showed that transparency and control can alleviate the negative consequences of data breaches. Chen et al. (2017) found that organizations can provide transparency and control over predictive model-driven inferences, but they can also make control harder or easier for users. Oltvoort et al. (2019) discovered that transparency manipulation plays a central role in drone acceptance, even when it fails. Zhu et al. (2021) studied the privacy paradox in mHealth applications and found that control is elaborated via a central route, whereas transparency is elaborated by peripheral route. Alkis and Kose's (2022) survey on social media advertising in 29 European countries showed that individuals care about transparency and control when exchanging data with brands they find valuable. Eggers et al. (2023) found that providing more transparency and control on data collection positively affects the acceptance of information collection. Finally, Zhang et al.'s (2023) study on AIoT-enabled smart surveillance found that transparency can lessen the personalization-privacy paradox, while Chen et al.'s (2023) study on proximity contact tracing at hospitality venues showed that transparency and control of businesses' privacy practices influence customer cooperation and commitment. Overall, these studies suggest that transparency and control are crucial factors in privacy and data protection, and that organizations should strive to provide their users with

Table 1
Literature review.

Authors	Focus	Methodology	Results
Martin et al. (2017)	Customer data vulnerability	Online experiments (study 1 and 3), event study (study 2) 600 US respondents (study 1) 414 data breaches in the US (study 2) 202 US respondents (study 3)	Transparency and control alleviate the negative consequences of data breaches
Chen et al. (2017)	Cloaking device (i.e., a mechanism for users to inhibit the use of particular pieces of information in inference)	$n = 164,883$ US Facebook users Survey + data scraping	Organizations can provide transparency and control even into complicated, predictive model-driven inferences, but they also can make control easier or harder for their users.
Oltvoort et al. (2019)	Drone acceptance	$n = 120$ experiment (transparency (yes vs. no)	Even when transparency manipulation fails, the concept plays a central role
Zhu et al. (2021)	Privacy paradox in mHealth applications	$n = 251$ Chinese respondent Quasi-experiment	Control is elaborated via a central route, whereas transparency is elaborated by peripheral route
Alkis and Kose (2022)	Social media advertising	$n = 153,053$ individuals from 29 European countries Survey	care for transparency and control such that they can proceed with the data exchange with brands that they find valuable
Eggers et al. (2023)	information sensitivity (high vs. low) and interaction intensity (high vs. low).	Online experiments (Study 1 and 2) 841 Dutch respondents (study 1) + 302 study 2	Providing more transparency and control on data collection positively accepts the acceptance of information collection
Zhang et al. (2023)	AIoT-enabled smart surveillance	$n = 415$ Chinese respondents Online experiment	Transparency can lessen the personalization-privacy paradox
Chen et al. (2023)	Proximity contact tracing at hospitality venues	Online survey 365 US	Transparency and control of businesses' privacy practices influence customer cooperation and commitment
This study	Tracking technologies for marketing purposes	Online experiments $n_{Study\ 1} = 155$ $n_{Study\ 2} = 115$	Transparency and control have indirect effects on click-through intent regarding tracking technologies used for marketing purposes

both to increase their cooperation and commitment.

Despite recent advancements in research on the relationship between transparency and control and their effects on privacy and data protection, there are still significant limitations that need to be addressed. Some of the main limitations of previous research include the lack of real-world settings in scenario-based studies (Martin et al., 2017), reliance on psychological black-boxes in understanding control (Chen et al., 2017), and the neglect of personalization in the elaboration of transparency and control (Zhu et al., 2021). As a result, the current understanding of the effects of transparency and control is still limited (Chen et al., 2023). To address these limitations, we adopt a novel conceptualization of control based on the different stages of interaction (Chen et al., 2023).

3. Overview of the studies

3.1. Context

For this research, we selected the popular French health and well-being website Doctissimo. Established in 2000 by two medical doctors, this website provides various services, including health forums, health quizzes, and health videos and articles edited by healthcare practitioners or journalists. According to the Institut national de la santé et de la recherche médicale (Inserm), the majority of visitors are young women with postgraduate education and high purchasing power. Although the website is free, media groups have been attracted to it since 2008, and it is now wholly owned by them, with a value of up to 15 million euros in 2018. Using health datafication, it employs advertising trackers and collects user-generated content, which, although different from clinical information and settings, is sensitive and requires specific attention. The sociotechnical interface makes it easier for some users to provide information more honestly on an app than with healthcare practitioners (Ostherr et al., 2017), but users remain vulnerable to health data exploitation by a third party.

Doctissimo uses tracking technologies for marketing purposes and shares collected data with commercial partners. According to a 2019 Privacy International report, Doctissimo shared user-generated health data with partners as they responded to mental health quizzes or navigated the web. It has over 45 advertising trackers that followed and shared pages visited by internet users about depression and other mental illnesses without their consent or knowledge, which is a significant privacy violation. However, Doctissimo privacy policies have attempted to comply with regulations and have evolved towards more transparency since 2015. By conducting topic modeling, we investigated their privacy policies posted online on January 23, 2015, May 15, 2018, August 8, 2018, and September 12, 2020. Our topic modeling identified five topics: instructions (38 % of the corpus), internal data management (18 %), trust (15 %), information sharing (15 %), and advertising (15 %). There is a trend towards more transparency regarding the use of consumers' data, with the topics of information sharing and advertising becoming dominant.

Therefore, Doctissimo is an ideal interface for our research experiment as it is well-known to our respondents, has health data character, uses tracking technologies, and has been engaging in improving transparency over time.

3.2. Flow chart of the studies

Zhu et al. (2021) suggest that transparency and control in the context of digital privacy refer to distinct cognitive routes from the elaboration likelihood theory. The authors posit that the control perception derives from a logical, rational, central route, whereas the transparency perception derives from a peripheral route prone to cognitive biases. This finding implies that previous operationalizations of transparency and control may have been limited, and a more realistic analysis of the roles of transparency and control is required. Given that transparency derives from a peripheral route, we manipulated it with a between-subject experiment (Study 1), as previously done in related studies (Martin et al., 2017). However, as control derives from a logical, rational, central route and based on the novel conceptualization of control using different stages of interaction (Chen et al., 2023), we opted for an intra-subject design (Study 2).

We conducted two experiments to investigate the personalization privacy paradox within the transparency-control framework (see Fig. 1). In Study 1, we used an inter-subject design to manipulate the level of transparency of the cookie banner (i.e., high vs. low) and then asked an open-ended question about the banner. We measured transparency (Martin et al., 2017), personalization over privacy (Kim et al., 2019), and click-through intention (Aguirre et al., 2015; Bleier and Eisenbeiss, 2015) using established measurement scales. We also conducted topic modeling (Berger et al., 2020; Humphreys and Wang, 2018) on the answers to the open-ended question and integrated the results with the measurement scales in an exploratory mediation analysis. The topic intrusion of information boundaries emerged as a key mediator in our analysis. Building on Study 1, we conducted Study 2 with an intra-subject design to display the privacy controls of the cookie banner. We used measures of privacy control (Mothersbaugh et al., 2012), intrusion of information boundaries (Sutanto et al., 2013), personalization over privacy (Kim et al., 2019), and click-through intention (Aguirre et al., 2015; Bleier and Eisenbeiss, 2015) before and after the experiment.

4. Study 1

4.1. Hypotheses development

The personalization-privacy paradox is a complex phenomenon that affects both consumers and marketers (Cloarec, 2020, 2022; Cloarec et al., 2022). Consumers are increasingly aware of the value of personalization, and expect brands to provide tailored experiences based on their individual preferences and needs. However, the use of personal data by marketers to achieve this goal has raised serious privacy concerns among consumers, leading to a tension-charged cycle that is difficult to break. To address this issue, transparency has been identified as a key factor in building and maintaining consumer trust towards brands. Schnackenberg and Tomlinson (2016) proposed a comprehensive framework for understanding transparency in marketing, identifying three qualitative dimensions: the degree of information disclosure, the disclosure quality, and the accuracy quality. Palmatier and Martin (2019) defined transparency as "the company's willingness and ability to clearly explain to customers how it is collecting, using, sharing, or protecting data" (p. 101). Transparency has been a topic of great interest in the context of advertising, where an open display of reciprocity has been shown to increase consumer acceptance of free web services (Schumann et al., 2014). Moreover, research has demonstrated that when privacy policies are made more salient, consumers are more likely to incorporate privacy considerations in their online purchasing decisions. Given this background, we hypothesize that transparency plays a critical role in addressing the personalization-privacy paradox. Specifically, we propose that.

H1. Transparency increases consumers' relative desire for the personalization over their concern for privacy.

Transparency in advertising is a complex issue that has been subject to much discussion and debate. On the one hand, transparency can foster trust and positive behavior among consumers, while on the other hand, it can also have unintended consequences that can undermine brands (Portes et al., 2020). For example, Karwatzki et al. (2017) found no evidence that transparency features increase users' willingness to disclose information, based on information boundary theory. The lack of significance of transparency features may be due to the duality of their effects. While transparency features can provide relevant information for rational decision-making, they can also increase individuals' privacy

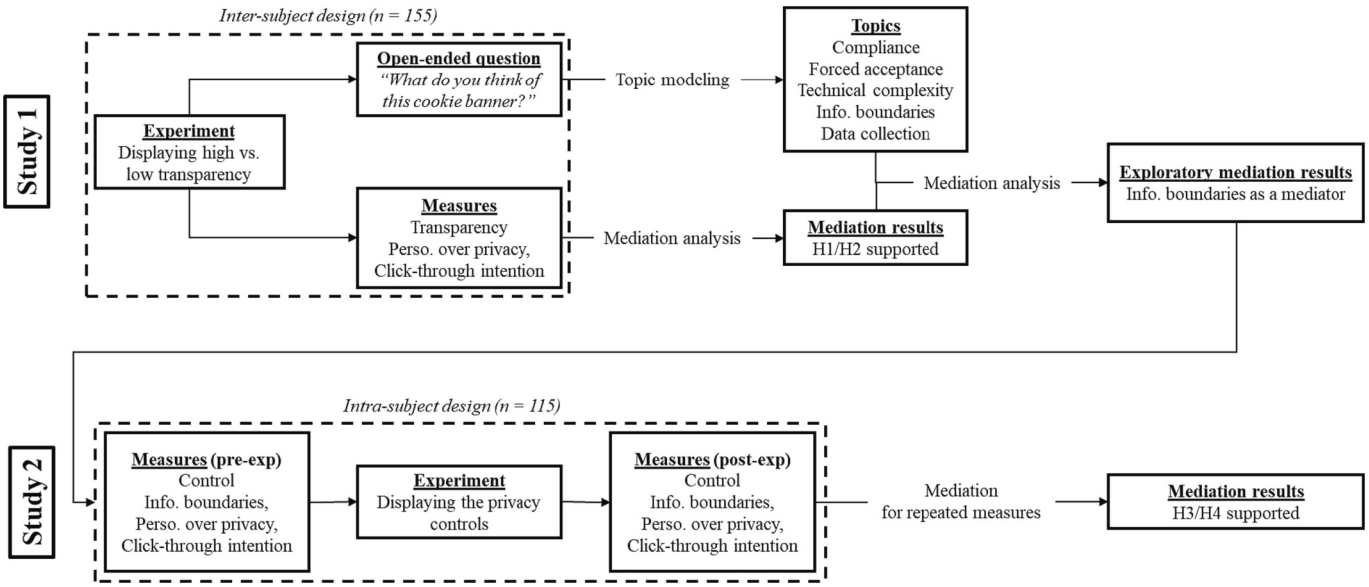


Fig. 1. Flow chart of the studies.

concerns, resulting in the concealment of personal data. This reverse impact has also been found in studies on personalized advertisements, where explicit use of personal information gives rise to privacy concerns. Therefore, it is possible that the lack of significance of transparency features in the context of the personalization-privacy paradox may be attributed to this duality of effects. However, the majority of the literature empirically demonstrates that transparency has a positive effect (Eggers et al., 2023). The research conducted by Kim et al. (2019) demonstrates that the impact of transparency on advertising performance is contingent upon whether the consumer finds the advertising practices acceptable. Martin et al. (2017) suggest that transparency can have a positive impact on consumer trust, but its effectiveness can be influenced by the quality and degree of information disclosure. Taking all of these elements into consideration, we hypothesize that transparency does not have a direct impact on the intention to accept cookies, but rather, its effect is mediated by the consumer's relative desire for personalization compared to their concern for privacy. Further research is needed to explore the complex interplay between transparency, consumer attitudes, and advertising performance in different contexts.

H2. Transparency positively and indirectly impacts click-through intention, via consumers' relative desire for the personalization over their concern for privacy.

4.2. Methodology

4.2.1. Design

We used a between-subject design (i.e., high vs. low transparency; see Appendix A) to test our hypotheses. Here is the stimulus for low transparency: "*In order to offer you an optimal experience on our website or application, we and our selected partners access and write information on your terminal (cookies and identifiers) and process personal data related to your navigation on our contents (including your IP address and the pages you have visited)*". For the high transparency, we add: "*Core Features; Storing and/or accessing information stored on an endpoint; Audience Measurement; Social Networking Features; Personalized Ads and Content, Ad and Content Performance Measurement, Audience Data and Product Development; Accurate Geolocation Data and Identification through Endpoint Analysis*".

4.2.2. Data

Participants ($N = 155$, 77.4 % female; $M_{age} = 22.8$, SD = 2.9) were recruited from two French Schools of Management.

4.2.3. Measures

We adapted the scale for transparency from Martin et al. (2017): *Doctissimo's customer data management activities are: Unclear to me/Clear to me; Confusing/Straightforward; Difficult to understand/Easy to understand; Vague/Transparent*. We assessed consumers' relative desire for the personalization over their concern for privacy with the following scale that was developed by Kim et al. (2019): "*In order to provide more personalized recommendations for you, marketers need to gather more information about you. In other words, when receiving an advertisement, there is a tradeoff between maintaining your privacy and enjoying the benefits of greater personalization. Upon seeing the above message by Doctissimo, which factor is more important to you when evaluating a targeted ad?*" on a 10-point scale (1 = Privacy is more important to me to 10 = Personalization is more important to me). We adapted the intention to click-through from Aguirre et al. (2015) and Bleier and Eisenbeiss (2015): "*To visit the Doctissimo site, I would agree to click on the 'Accept' button*".

4.3. Results

4.3.1. Manipulation check

An ANOVA (Fig. 2) on the transparency manipulation check ($\alpha = 0.90$) revealed a significant difference between conditions ($F_{(1,153)} = 8.131$, $p < .005$). Participants in the high transparency condition scored higher ($M_{\text{high transparency}} = 3.58$, $SD = 1.38$) than those in the low transparency condition ($M_{\text{low transparency}} = 2.92$, $SD = 1.50$).

4.3.2. Personalization over privacy

An ANOVA (Fig. 3) on consumers' relative desire for the personalization over their concern for privacy revealed a significant difference between conditions ($F_{(1,153)} = 6.454$, $p < .012$). Participants in the high transparency condition valued more personalization over privacy ($M_{\text{high transparency}} = 3.07$, $SD = 1.79$) than those in the low transparency condition ($M_{\text{low transparency}} = 2.40$, $SD = 1.47$). This supports H1 that states that transparency increases consumers' relative desire for the personalization over their concern for privacy.

4.3.3. Mediation

In line with H2, the impact of the high vs. low transparency conditions on click-through intention was fully mediated by participants' relative interest in personalization concern over their privacy: a 5000-sample bootstrap analysis using PROCESS Model 4 (Hayes, 2021) indicated a significant indirect effect ($b = 0.20$, $SE = 0.09$; 95 % confidence

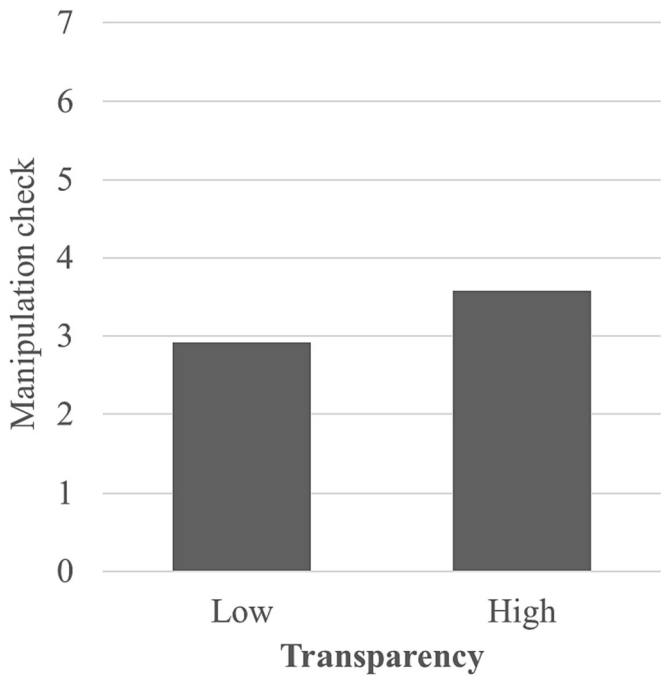


Fig. 2. Manipulation check for transparency.

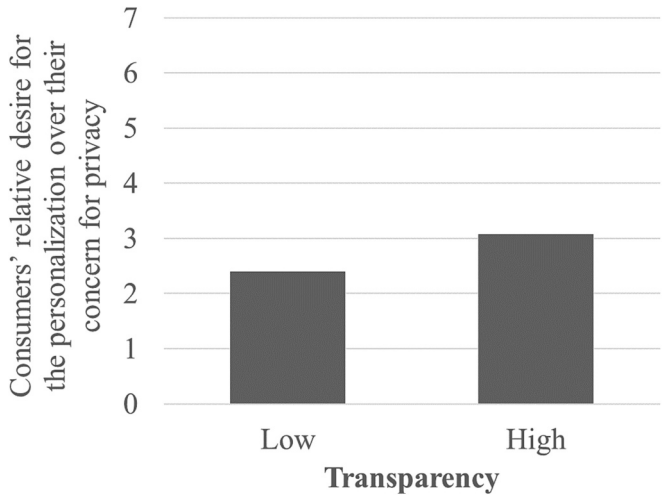


Fig. 3. ANOVA of transparency (H1).

interval: [0.03, 0.41]).

Fig. 4 summarizes the results.

4.3.4. Topic modeling

In order to gain a deeper understanding of consumers' perceptions regarding transparency and personalization in advertising, we conducted an automated text analysis using a tidy data model for natural language processing (Arnold, 2017) on open-ended responses collected through an online survey. To do this, we employed the latent Dirichlet allocation algorithm (Grün and Hornik, 2011), which is an unsupervised generative method commonly used in text mining and natural language processing. This algorithm assumes that each document in the corpus is a set of bag-of-words, where each document deals with a certain number of themes in different proportions, and each word has a distribution associated with each theme. The aim of the algorithm is to determine the distribution of words across different themes, the different proportions of themes for each document, and the proportions of appearance of a theme in the corpus. This enables us to determine the theme of a document, the words most associated with certain themes, and other important information. The Dirichlet distribution, which is the conjugate of the multinomial distribution, is used as a posteriori distribution in terms of factoring. This distribution is employed on the global proportion of themes as well as on each theme distribution on the words. Since the scores generated by the topics represent percentages (i.e., compositional data), we used their center log-ratio for the rest of the analyses (van den Boogaart and Tolosana-Delgado, 2008).

Table 2 presents the results of the topic modeling. The analysis found five distinct topics, each representing a different aspect of consumers' perceptions of transparency and personalization in advertising. These topics, in order of their distribution in the corpus, are compliance (23 %), technical complexity (23 %), data collection (21 %), forced acceptance (17 %), and intrusion of information boundaries (16 %). The compliance topic mainly focused on consumers' perceptions of the legality and regulation of online advertising practices, while the technical complexity topic centered on the difficulty and complexity of understanding online advertising processes. The data collection topic highlighted consumers' concerns about the collection, sharing, and use of their personal information by online advertisers. The forced acceptance topic dealt with consumers' perceptions of the inevitability of accepting cookies and personalized ads when using online services. Finally, the information boundaries topic focused on consumers' perceptions of the boundaries between public and private information, and the role of transparency in maintaining these boundaries.

4.3.5. Transparency on topics

An ANOVA on forced acceptance ($F_{(1,153)} = 4.175$, $p < .043$) and intrusion of information boundaries ($F_{(1,153)} = 5.411$, $p < .021$) revealed a significant difference between conditions. Participants in the high transparency condition perceived less forced acceptance ($M_{\text{high transparency}} = -0.27$, $SD = 1.66$) than those in the low transparency condition ($M_{\text{low transparency}} = 0.25$, $SD = 1.48$). Participants in the high transparency condition felt more intrusion of information boundaries (M_{high}

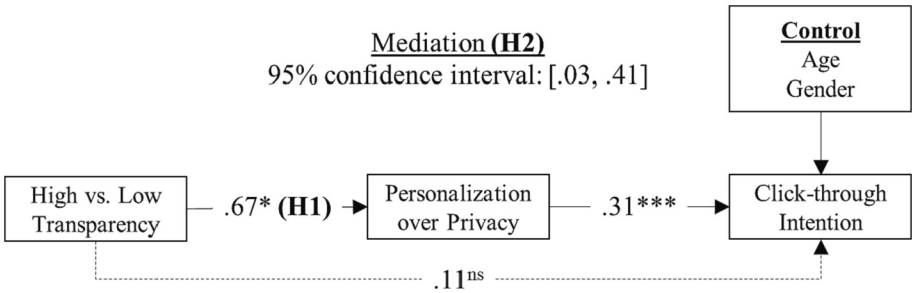


Fig. 4. Results of the top-down approach.

Table 2
Distribution of the topics.

Topics	Compliance 23 %	Forced acceptance 17 %	Technical Complexity 23 %	Intrusion of Information Boundaries 16 %	Data Collection 21 %
Content of the topics (words oredered by their contribution to the topic)	Think	Time	Understandable	Precise	Choice
	Transparent	Intrusive	Technical	Geolocation	Navigation
	Required	Need	Term	Functionality	Serve
	Must	Consult	User	Trend	Collect
	Reassuring	General	Use	Personal	Clear
	Health	Internet	Appropriate	Hide	Content
	Detail	Look Like	Attention	Fear	Internet User
	Take	Thing	Encourage	Life	Example
	Confidential	Understanding	Inform	Essential	Identifier
	Control	Enter	Lens	Want	IP

$_{\text{transparency}} = 0.26$, $SD = 1.35$) than those in the low transparency condition ($M_{\text{low transparency}} = -0.24$, $SD = 1.31$).

4.3.6. Structural model with topics

The results (Fig. 5) show that the intrusion of information boundaries decreases participants' relative interest in personalization concern over their privacy ($b = -0.27$, $p < .01$). In turn, the higher participants' relative interest in personalization concern over their privacy, the higher the click-through intention ($b = 0.30$, $p < .001$).

4.3.7. Mediation with topics

The impact of the high vs. low transparency conditions was fully mediated by the topics and participants' relative interest in personalization concern over their privacy: a 5000-sample bootstrap analysis using a self-implemented PROCESS syntax (Hayes, 2021) indicated a significant total indirect effect ($b = 0.20$, $SE = 0.10$; 95 % confidence interval: [0.04, 0.42]; see Table 3). The syntax is as follows:

process y = CTI/m = TOPIC1 TOPIC2 TOPIC3 TOPIC4 TOPIC5 PoP/ x = ExpTRANS/ cov = AGE GENRE/ conf = 95/bmatrix =1,1,0,1,0,0,1,0,0,0,1,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1/cmatrix = 0,0,0,0,0,0,0,0,0,0,0,0,1,1.

Table 3
Mediation analysis with the topics.

	b	*SE*	95 % CI	
			Lower	Upper
Total	0.20*	0.10	0.04	0.42
Ind1	0.22*	0.10	0.04	0.44
Ind2	0.01^{ns}	0.02	−0.02	0.05
Ind3	0.02^{ns}	0.02	−.02	0.05
Ind4	−0.00^{ns}	0.01	−0.02	0.02
Ind5	−0.04*	0.02	−0.09	−0.00
Ind6	−0.00^{ns}	0.01	−0.01	0.01

Ind1: Transparency → Personalization over Privacy → Click-through Intention.
Ind2: Transparency → Compliance → Personalization over Privacy → Click-through Intention.
Ind3: Transparency → Forced Acceptance→ Personalization over Privacy → Click-through Intention.
Ind4: Transparency → Technical Complexity → Personalization over Privacy → Click-through Intention.
Ind5: Transparency → Intrusion of Information Boundaries → Personalization over Privacy → Click-through Intention.
Ind6: Transparency → Data Collection → Personalization over Privacy → Click-through Intention.
* $p < .05$, ns: not significant.

4.4. Discussion

Study 1 demonstrates the significance of intrusion of information boundaries that arise due to the transparency of cookies. This finding

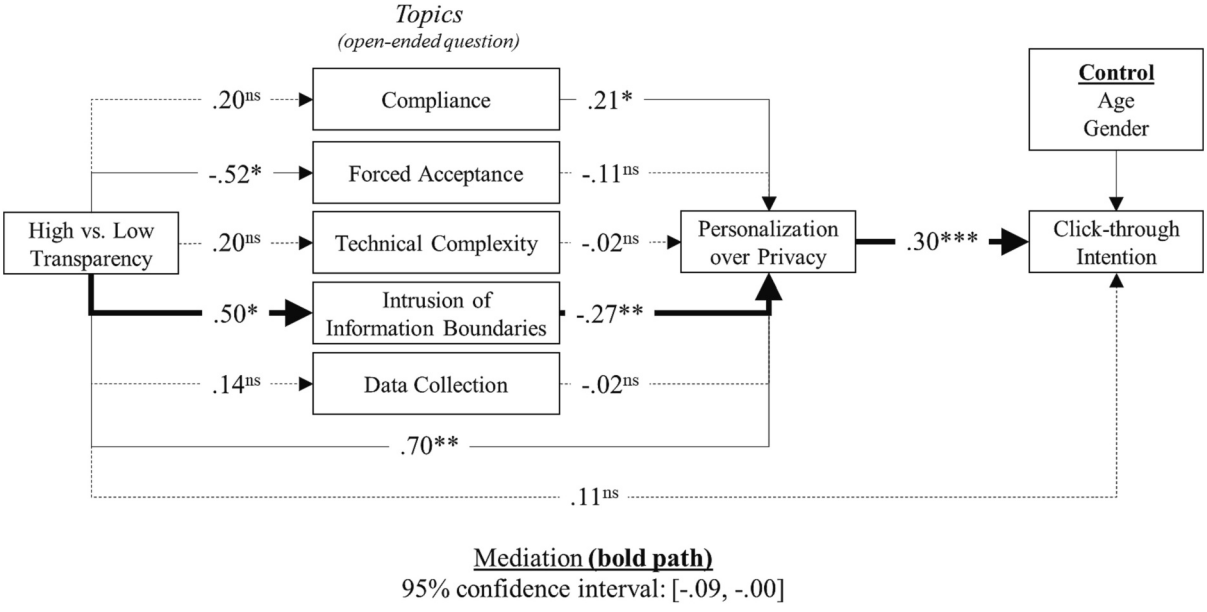


Fig. 5. Structural model.
Notes: $^{**}p < .01$, $^{*}p < .05$, ns: not significant.

reinforces the argument that transparency is essential for ensuring fair and ethical data collection and usage (Eggers et al., 2023; Gouthier et al., 2022; Wiertz and Kittinger-Rosanelli, 2021). The importance of coordination among all parties involved in data collection and usage, as emphasized in Study 1, is also echoed in the literature, which suggests that companies should focus on willingly granting consumers more transparency and control over their data (Schumacher et al., 2023).

To understand the importance of transparency and control in privacy management, Petronio's information boundary management theory (Petronio, 1991) provides a useful framework. This theory examines the regulation processes behind the disclosure of personal information by individuals and highlights the need for coordinated management efforts from all parties involved in safeguarding privacy boundaries. Petronio argues that effective privacy management requires all parties to have a shared understanding of the permeability, linkage, and ownership of boundaries. This notion of coordinated management aligns with the transparency-control framework proposed by Eggers et al. (2023) and Gouthier et al. (2022), which underlines the crucial role of transparency and control in ensuring fair and ethical data collection and usage. The framework also underscores the potential negative consequences for consumers when they feel they were not adequately informed about the data collection process.

5. Study 2

5.1. Hypotheses development

When a consumer perceives a privacy violation due to a divergence between their expectations and organizational practices, it can result in boundary turbulence within the boundary management system (Petronio, 2000). This can be caused by mistakes, involuntary disclosures, intentional breaking of boundaries, or the absence of existing rules, which can lead to cognitive and emotional responses (Grégoire and Fisher, 2008; Palmatier, 2008).

Corporate policies that are perceived to have strong control can alleviate privacy concerns (Martin and Murphy, 2017), and a better perceived control can reduce privacy concern (Xu et al., 2012) and increase the willingness to disclose sensitive information (Brandimarte et al., 2013). However, as noted by Tucker (2014), consumer control remains a psychological construct, and the perception of control can increase the effectiveness of advertising, regardless of actual control over data. The type of elicitation can also affect the perception of control, as in the case of cookie banners, where user interface design can influence the perception of a requirement or voluntary approach (Norberg and Horne, 2014).

Privacy control means allowing customers to decide how their data will be used and shared, whether for advertising or sharing with partners (Palmatier and Martin, 2019). While privacy controls have significant financial implications, consumers do not always protect their personal information (Brandimarte et al., 2013). Reasons for this may include a lack of information on how to do so (Crossler and Bélanger, 2019; Klasnja et al., 2009), feeling overwhelmed by the amount of privacy information (Temming, 2018), or lack of motivation (Crossler and Bélanger, 2019). In asymmetric relationships with data-driven firms, privacy controls can make consumers feel less vulnerable (Baker et al., 2005; Martin et al., 2017), more able to self-regulate their behaviors (Benavent, 2014), less violated by firms' data management practices (Kumar et al., 2014; Tucker, 2014), and perceive less uncertainty and sneakiness (Martin et al., 2017). Based on the above rationale, we hypothesize:

H3. Control decreases the intrusion of information boundaries.

The transparency-control framework proposes that companies should willingly grant consumers more transparency and control over their data to avoid negative consequences such as privacy violations. In this context, the studies by Mothersbaugh et al. (2012) and Brandimarte et al. (2013) highlight the importance of perceived control in increasing consumers' willingness to disclose sensitive information. This finding is consistent with the transparency-control framework's emphasis on the role of control in privacy management. Thus, we hypothesize that:

H4. Control indirectly and positively impacts click-through intention, via the intrusion of information boundaries and participants' relative interest in personalization concern over their privacy.

5.2. Methodology

5.2.1. Design

To test the impact of control on participants' interest in personalization versus their privacy concerns, we utilized a within-subject design. The process involved participants completing a questionnaire related to the primary constructs, including their desire for personalization, concerns about intrusion into personal information boundaries, and their intention to click through. Following this, we presented participants with a control panel (see Appendix B) and asked them to complete the same questionnaire. Here are the main privacy controls: "*Essential Features; Social Networking Features; Audience Measurement; Storing and/or Accessing Information on an Endpoint; Personalizing Editorial Content and Measuring Performance; Personalizing Ads and Measuring Performance; Developing and Improving Products; Using Accurate Geolocation Data; Actively Analyzing Endpoint Characteristics for Identification*". Since we informed the participants on the study's purpose, demand effect should not be a major concern (see Mummolo and Peterson, 2019).

5.2.2. Data

Participants ($N = 115$, 66.5 % female; $M_{age} = 29$, SD = 12.7) were recruited online.

5.2.3. Measures

We adapted the scale for control from Mothersbaugh et al. (2012): *On Doctissimo, I believe I have control over what happens to my personal information; It is up to me how much the company uses my information; I have a say in how my information is used by the company; I have a say in whether my personal information is shared with others*. We adapted the scale for the intrusion of personal information boundary from Sutanto et al. (2013): *I feel that Doctissimo may know about me more than I feel at ease with, I believe the information about me which I consider should only be kept to myself will be more readily available to Doctissimo than I would want to, I believe that the information about me is out there that, if used by Doctissimo, will invade my boundary of revealing about myself, I feel that my limit of disclosing information about me would be invaded by Doctissimo*. As before, we assessed consumers' relative desire for the personalization over their concern for privacy with the scale that was developed by Kim et al. (2019) and the intention to click-through by Aguirre et al. (2015) and Bleier and Eisenbeiss (2015).

5.2.4. Method of analysis

We implement Montoya and Hayes' (2017) procedure for mediation analyses for repeated measures that is based on the work by Judd et al. (2001), which has been used in top marketing journals (Spiller, 2011; Warren and Campbell, 2014). Montoya and Hayes (2017) followed the latest improvements in mediation analysis (i.e., bootstrap confidence intervals for inference about the indirect effect). Following Montoya and Hayes (2017), the path coefficients of the research model can be estimated by the following set of equations:

Effect of control on the intrusion of information boundaries

$$M_{12i} - M_{11i} = a_1 + e_{M_{1i}} \quad (1)$$

Eq. (1) aims at estimating the effect a_1 of control on the post- (M_{12i}) vs. pre-experiment (M_{11i}) first mediator (i.e., intrusion of information boundaries). The effect a_1 represents the first segment of the serial mediation for repeated measures. $e_{M_{1i}}$ refers to the errors of the

estimation.

Effects of control and the intrusion of information boundaries on consumers' relative desire for the personalization over their concern for privacy

$$M_{22i} - M_{21i} = a_2 + a_3(M_{12i} - M_{11i}) + d_0[0.5(M_{11i} + M_{12i}) - \overline{0.5(M_{11} + M_{12})}] + e_{M_{2i}} \quad (2)$$

Eq. (2) aims at estimating the effect a_3 the post- (M_{12i}) vs. pre-experiment (M_{11i}) first mediator (i.e., intrusion of information boundaries) on the post- (M_{22i}) vs. pre-experiment (M_{21i}) second mediator (i.e., consumers' relative desire for the personalization over their concern for privacy). The effect a_3 represents the second segment of the serial mediation for repeated measures. We control for the effect a_2 of control on the post- (M_{22i}) vs. pre-experiment (M_{21i}) second mediator (i.e., consumers' relative desire for the personalization over their concern for privacy). We also control for the effect d_0 of the global first mediator (i.e., intrusion of information boundaries) on the post- (M_{22i}) vs. pre-experiment (M_{21i}) second mediator (i.e., consumers' relative desire for the personalization over their concern for privacy). The term $0.5(M_{11i} + M_{12i})$ represents the mean of the first mediator (i.e., intrusion of information boundaries) for a given respondents and we compare its deviation with the overall mean of the first mediator $\overline{0.5(M_{11} + M_{12})}$ as follows: $[0.5(M_{11i} + M_{12i}) - \overline{0.5(M_{11} + M_{12})}]$. Hence, this allows make sure that the effect a_3 of the second segment of the mediation for repeated measures is robust: it is not only the concept itself that might have an effect (i.e., $d_0[0.5(M_{11i} + M_{12i}) - \overline{0.5(M_{11} + M_{12})}]$), but its intra-difference (i.e., $a_3(M_{12i} - M_{11i})$). $e_{M_{2i}}$ refers to the errors of the estimation.

Effects of control, the intrusion of information boundaries, and consumers' relative desire for the personalization over their concern for privacy on click-through intention

$$Y_{2i} - Y_{1i} = c' + \sum_{j=1}^{2} b_j(M_{j2i} - M_{j1i}) + \sum_{j=1}^{2} d_j[0.5(M_{j1i} + M_{j2i}) - \overline{0.5(M_{j1} + M_{j2})}] + e_{Y^*_i} \quad (3)$$

Eq. (3) is similar to Eq. (2). The difference is that there are two mediators (i.e., intrusion of information boundaries and consumers' relative desire for the personalization over their concern for privacy) instead of one.

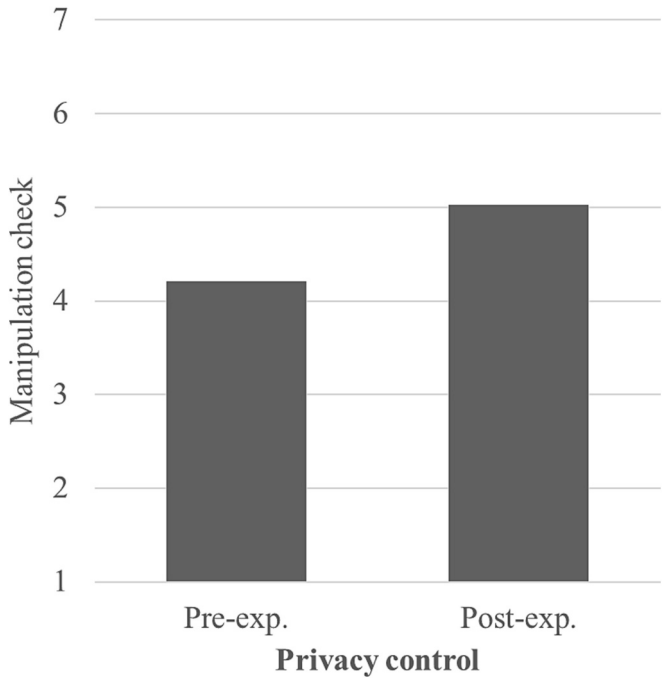


Fig. 6. ANOVA for manipulation check.

5.3. Results

5.3.1. Manipulation check

An ANOVA (Fig. 6 and Table 4) on the control manipulation check ($\alpha_{pre} = 0.80$, $\alpha_{post} = 0.77$) revealed a significant difference during the experiment ($F_{(1,230)} = 21.230$, $p < .001$). Participants perceived more control after the experiment ($M_{post} = 5.00$, $SD = 1.17$) than before ($M_{pre} = 4.2$, $SD = 1.50$).

5.3.2. Control

The results (Fig. 7) show that control decreases the intrusion of information boundaries ($b = -0.44$, $p < .001$), thus supporting H3. The lower the intrusion of information boundaries, the higher the consumers' relative desire for the personalization over their concern for privacy ($b = -0.21$, $p < .01$). In line with Study 1, the higher consumers' relative desire for the personalization over their concern for privacy, the lower the intention to click-through ($b = 0.35$, $p < .05$).

5.3.3. Mediation

The impact of the control was mediated by the intrusion of information boundaries and participants' relative interest in personalization concern over their privacy: a 5000-sample bootstrap analysis using Montoya and Hayes procedure (2017) indicated a significant and positive indirect effect at the 90 % level ($b = 0.03$, $SE = 0.03$; 95 % confidence interval: [−0.00, 0.09]; 90 % confidence interval: [0.00, 0.08]), thus supporting H4.

5.4. Discussion

Study 2 underscores the significance of control in data privacy within the transparency-control framework. This framework highlights the need for external auditing of service design against industry standards and regulatory requirements, such as the GDPR in the EU, which mandates firms to provide consumers with control over data collection, storage, and use (Eggers et al., 2023). Study 2 thus emphasizes the importance of accountability in privacy protection through external auditing (Wirtz et al., 2023).

Furthermore, Study 2 aligns with the transparency-control framework in its examination of the impact of control on consumer behavior. It suggests that strong corporate policies that provide control can assuage privacy concerns and increase willingness to disclose sensitive information. The study thus emphasizes that companies should proactively grant consumers more control over their data instead of relying on public policy to drive privacy regulations.

6. General discussion

6.1. Discussion of key findings

Our research findings serve as a cornerstone, advancing our comprehension of the intricate dynamics within the transparency-control framework. By casting light on the multifaceted effects of transparency and control on the desires of internet users for personalization while navigating their concerns about privacy, especially in the context of data collection (Kim et al., 2019), we contribute to a richer and deeper understanding of this pivotal framework. The transparency-control framework, firmly grounded in the bedrock of procedural fairness (Eggers et al., 2023; Gouthier et al., 2022), underscores the crucial interplay of transparency and control in shaping equitable and ethically sound practices in data collection and use.

Within this nuanced landscape, our study offers empirical insights into the compelling and positive influence of transparency on users' leanings towards personalization over their concerns regarding privacy. This, in turn, molds their intent to interact and engage by clicking.

Table 4
Paired-samples *t*-tests.

Control		Intrusion of Information boundaries		Personalization over privacy		Click-though intention	
Pre-exp	Post-exp	Pre-exp	Post-exp	Pre-exp	Post-exp	Pre-exp	Post-exp
4.21	5.02	5.02	4.57	2.41	2.61	4.41	4.51
$p < .001$		$p < .001$		$p < .014$		$p > .05$	

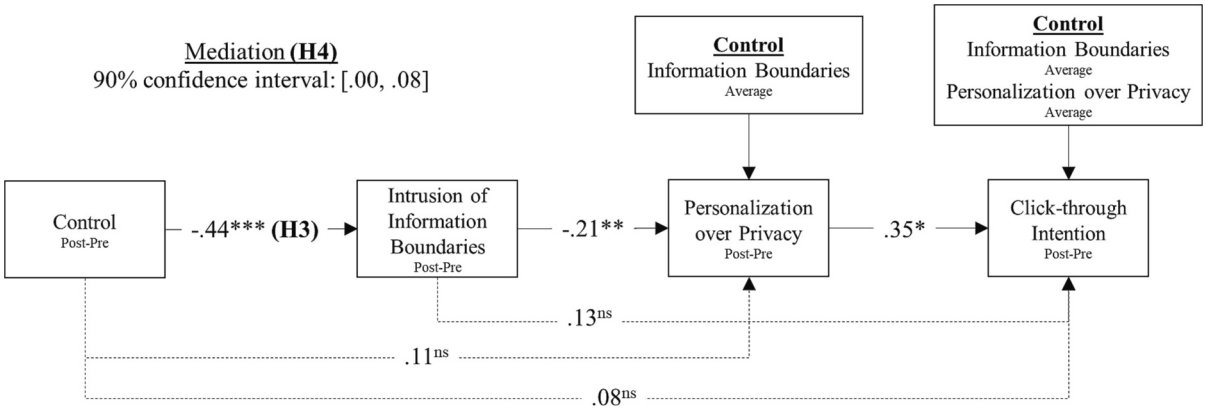


Fig. 7. Mediation for repeated measures.
Notes: $^{**}p < .01$, $^{*}p < .05$, ns: not significant.

Notably, this revelation adds layers to the ongoing discourse concerning the intricate role of transparency in the realm of advertising (Karwatzki et al., 2017; Portes et al., 2020). We should emphasize that our research leans on an easily accessible and unanticipated privacy interface—a seamless component of internet users' day-to-day digital interactions, predominantly due to regulatory mandates. Consequently, the perception of transparency has organically evolved into a swift and instinctive reflex (Zhu et al., 2021) developed by users, significantly amplifying their eagerness to actively participate and engage.

In our exploration, another significant revelation emerges—shedding light on the positive indirect effect that control exerts on users' intention to click through. Diverging from the realm of transparency, wielding control demands a more substantial cognitive investment (Zhu et al., 2021), especially when confronted with implicit data collected through the pervasive net of tracking technologies. This nuanced contrast leads users to harbor fewer doubts and showcase diminished hesitancy when making decisions to engage. The implications of this finding resonate with the observed control paradox (Brandimarte et al., 2013), wherein granting users greater control over their shared data on platforms such as Facebook invariably amplifies their inclination to share information, underscoring the intricate interplay of control mechanisms in the digital landscape.

6.2. Theoretical contribution

We contribute to the literature in several ways. Firstly, our research improves the understanding of the link between the transparency of privacy interfaces and consumers' desire for personalization over their concern for privacy in a context of implicit data collection through tracking technologies. Our research shows that transparency enhances the desire for personalization over privacy concerns. Although literature has shown transparency to be ambivalent, our study supports a positive direct effect in the case of usual privacy interfaces.

Secondly, by relying on consumers' voice, our results highlight the key role of the intrusion of information boundaries as a mediator of the relationship between transparency and consumers' relative desire for personalization over their concern for privacy.

Thirdly, our study confirms the positive influence of perceived transparency on the acceptance of cookie tracking. Overall, even though transparency raises awareness of informational boundaries for the consumer, the global effect outweighs it. The discussion remains on how transparent organizations should be, at the risk of becoming too lengthy and complicated for consumers. However, in our study, we merely focused on applying current legal requirements of showcasing the purposes and list of partners with whom the data is intended to be shared. As not all organizations follow these requirements, transparent compliance must be encouraged without fearing a daunting effect of displaying information.

Fourthly, our results on control are similar. Once people have been presented with control settings, they are more likely to accept. We propose that the reactance effect thus may not necessarily manifest when the consumer is informed about the specific tracking capabilities of the organization and perceives an obligation to validate. In such scenarios, the consumer may willingly communicate their general concerns.

6.3. Methodological contribution

In this research, we aimed to create real-life experimental settings for analysis. We incorporated the consumer's voice in generating constructs and studied the different cognitive mechanisms underlying transparency and control separately, with a psychological mechanism lens.

Firstly, using the consumers' voice to generate constructs elicited by transparency helped us build a relevant mediation model that combined top-down (i.e., Likert scales) and bottom-up (i.e., open-ended questions) approaches, instead of relying on a direct effect as in previous research (Kim et al., 2019).

Secondly, our research suggests that studying the constructs of transparency and control separately is important because consumers can easily assess the transparency of a cookie, which is the first piece of information presented on most web pages. However, learning about control requires more effort, leading to a delayed assessment. Therefore, an intra-subject design, in which consumers evaluate their online experience based on transparency followed by re-evaluation after assessing control, is more suitable for evaluating control than the two-by-two inter-subject design used in prior research on transparency and control (Martin et al., 2017).

Finally, our research assessed the effect of privacy controls through a

psychological mechanism lens, which is different from prior research on privacy controls (Krafft et al., 2017; Tucker, 2014) that mainly focuses on direct effects only, as is common in marketing research aimed at exploring consumers' decision-making (Konus et al., 2008; Rust et al., 2004).

6.4. Practical implications

This study provides valuable insights for managers, consumers, and policymakers on the relationship between transparency, control, and consumer behavior in online privacy interfaces. For managers, the study suggests that transparency is key in building trust and credibility with customers. By designing interfaces that are transparent about data collection and usage, managers can enhance the desire for personalization among consumers while still maintaining their privacy. Furthermore, managers should consider the importance of fostering a sense of control and awareness among users.

For consumers, the study emphasizes the importance of understanding the role of transparency and control in shaping their online experiences. By making informed decisions about the privacy interfaces and controls they encounter, consumers can protect their privacy while still enjoying personalized content and services. By acknowledging the potential positive impact of appropriately restrictive controls on their behavior, consumers can make more informed decisions about managing their online privacy effectively.

Policymakers can use the study to inform regulations and guidelines related to online privacy and data collection practices. The study highlights the importance of transparency in privacy interfaces, which can inform policy decisions around data privacy and consumer protection. Policymakers should also weigh the implications of not considering the reactance effect and avoid refraining from implementing adequate privacy controls that might negatively impact consumer behavior. Overall, this study provides valuable insights for managers, consumers, and policymakers on how to balance personalization and privacy in online experiences.

6.5. Limitations and future research

This study has several limitations that should be acknowledged. Firstly, while methodological advancements are still needed, future research could consider combining between- and within-subject designs in the same experiment. This approach would enable researchers to assess the effect of transparency and privacy control in a more comprehensive manner. Secondly, this study is based on a unique case (i.e., Doctissimo) and it would be beneficial to investigate other websites, such as social media or e-commerce, to gain a better understanding of the role of context. Thirdly, all participants in this study were French and it is important to consider the cultural aspects of privacy by including other populations. Fourthly, the sample size of the study might be considered a limitation, although it does fit the target audience of Doctissimo, which was the field of experiment. Fifthly, the indirect effect of control on click-through intention is slightly significant. Future research may wish to replicate this model in various settings to assess the robustness of this effect. Sixthly, given the context's focus on health data, future research could delve deeper into examining the role of well-being and privacy (Meyer-Waarden et al., 2021; Meyer-Waarden and Cloarec, 2022). Finally, it should be noted that transparency and control are context-dependent, and it is possible that more control may not have an impact on data disclosure for social media services that do not collect sensitive health data.

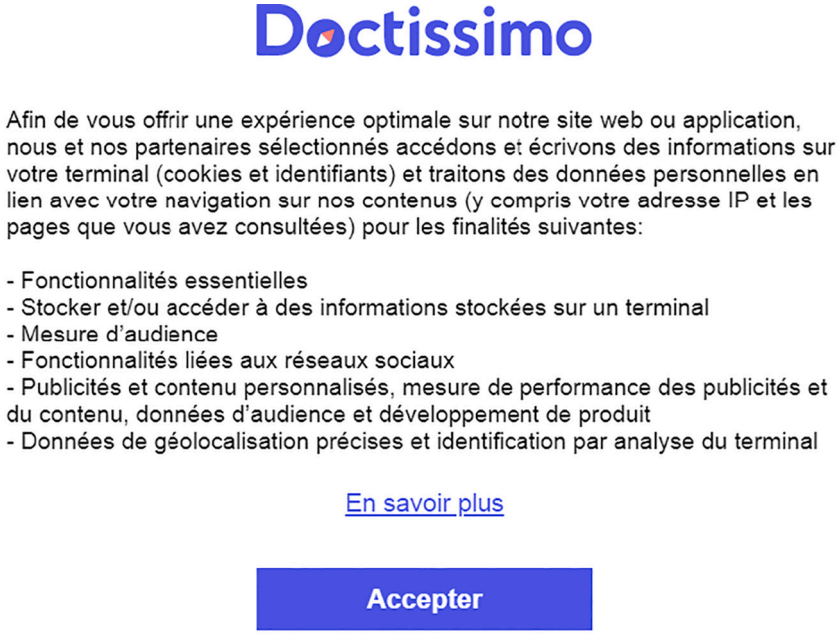
CRediT authorship contribution statement

Julien Cloarec: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Supervision, Visualization, Writing – original draft, Writing – review & editing. **Charlotte Cadieu:** Conceptualization, Writing – original draft, Writing – review & editing. **Nour Alrabie:** Conceptualization, Writing – original draft, Writing – review & editing.

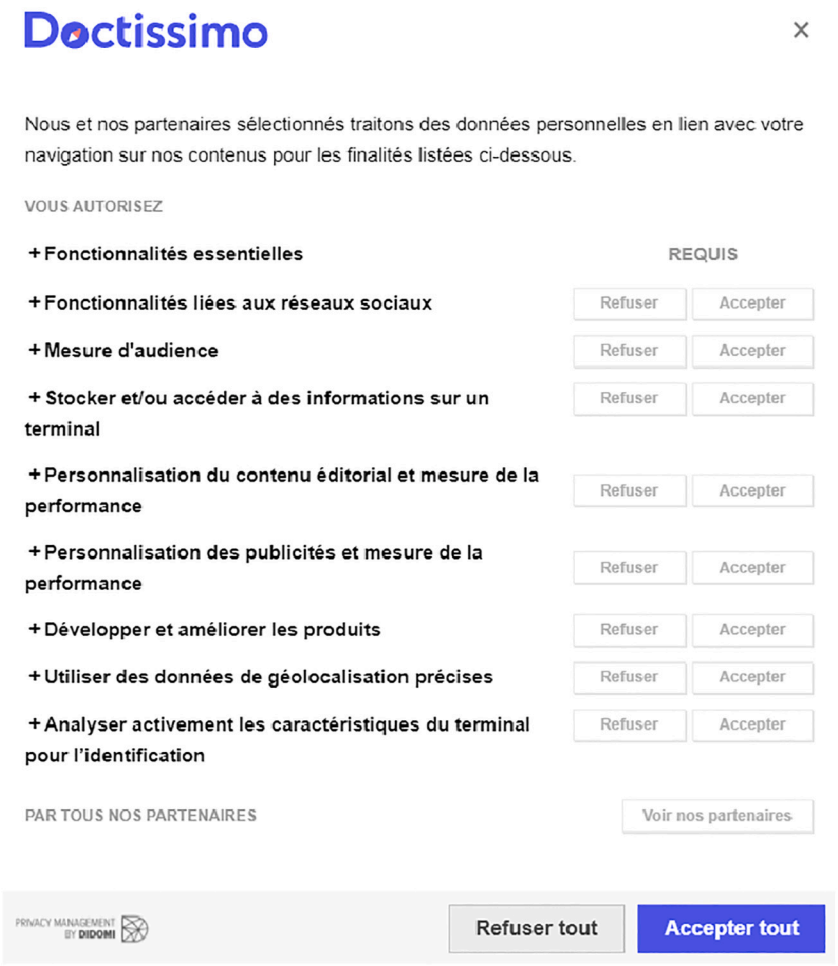
Data availability

Data will be made available on request.

Appendix A. High vs. low transparency



Appendix B. Privacy control intervention



Essential features; Social media related features; Audience measurement; Storing and/or accessing information on a device; Editorial content personalization and performance measurement; Advertising personalization and performance measurement; Developing and improving products; Using precise geolocation data; Actively analyzing device characteristics for identification.

References

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 advertise- ment effectiveness. J. Retail. 91 (1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005.

Alkis, A., Kose, T., 2022. Privacy concerns in consumer E-commerce activities and response to social media advertising: empirical evidence from Europe. Comput. Hum. Behav. 137 (107), 412. https://doi.org/10.1016/j.chb.2022.107412.

Arnold, T., 2017. A tidy data model for natural language processing using cleanNLP. R J. 9 (2), 248–267.

Awad, N., Krishnan, M., 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q. 30 (1), 13–28.

Baker, A.C., Jensen, P.J., Kolb, D.A., 2005. Conversation as experiential learning. Manag. Learn. 36 (4), 411–427. https://doi.org/10.1177/1350507605058130.

Benavent, C., 2014. Big Data: No Best Way. Le Libellio d'Aegis 10 (4), 5–14.

Berger, J., Humphreys, A., Ludwig, S., Moe, W.W., Netzer, O., Schweidel, D.A., 2020. Uniting the tribes: using text for marketing insight. J. Mark. 84 (1), 1–25. https://doi.org/10.1177/0022242919873106.

Bleier, A., Eisenbeiss, M., 2015. The importance of trust for personalized online advertising. J. Retail. 91 (3), 390–409. https://doi.org/10.1016/j.jretai.2015.04.001.

Bleier, A., Goldfarb, A., Tucker, C., 2020. Consumer privacy and the future of fata-based innovation and marketing. Int. J. Res. Mark. https://doi.org/10.1016/j.ijresmar.2020.03.006.

Brandimarte, L., Acquisti, A., Loewenstein, G., 2013. Misplaced confidences: privacy and the control paradox. Soc. Psychol. Personal. Sci. 4 (3), 340–347. https://doi.org/10.1177/1948550612455931.

Chen, R., 2013. Living a private life in public social networks: an exploration of member self-disclosure. Decis. Support. Syst. 55 (3), 661–668. https://doi.org/10.1016/j.dss.2012.12.003.

Chen, D., Fraiberger, S.P., Moakler, R., Provost, F., 2017. Enhancing transparency and control when drawing data-driven inferences about individuals. Big Data 5 (3), 197–212. https://doi.org/10.1089/big.2017.0074.

Chen, S. (Joseph), Tran, K.T., Xia, Z. (Raymond), Waseem, D., Zhang, J.A., Potdar, B., 2023. The double-edged effects of data privacy practices on customer responses. Int. J. Inf. Manag. 69, 102600 https://doi.org/10.1016/j.ijinfomgt.2022.102600.

Cloarec, J., 2020. The personalization–privacy paradox in the attention economy. Technol. Forecast. Soc. Chang. 161, 120299 https://doi.org/10.1016/j.techfore.2020.120299.

Cloarec, J., 2022. Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. J. Bus. Res. 152, 144–153. https://doi.org/10.1016/j.jbusres.2022.07.045.

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

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. Inf. Syst. Res. 30 (3), 995–1006. https://doi.org/10.1287/isre.2019.0846.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., Holz, T., 2019. We value your privacy... now take some cookies: measuring the GDPR's impact on web privacy. In: Proceedings 2019 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2019.23378.

Eggers, F., Beke, F.T., Verhoef, P.C., Wieringa, J.E., 2023. The market for privacy: understanding how consumers trade off privacy practices. J. Interacti. Mark. 109499682211, 400. https://doi.org/10.1177/10949968221140061.

Evans, R., Hajli, N., Nisar, T.M., 2022. Privacy-enhancing factors and consumer concerns: the moderating effects of the general data protection regulation. Br. J. Manag. 1467-8551, 12685 https://doi.org/10.1111/1467-8551.12685.

Financial Times, 2017. EU fines Facebook €110m over WhatsApp merger. http://www.ft.com/content/28efe3ed-6ab5-3993-8e16-f0d787aba8b3.

Forbes, 2022. The privacy compliance gap: how lack of consent enforcement is exposing brands to millions in fines and penalties. https://www.forbes.com/sites/forbestechcouncil/2022/12/19/the-privacy-compliance-gap-how-lack-of-consent-enforcement-is-exposing-brands-to-millions-in-fines-and-penalties/?sh=290419af67ef.

Gouthier, M.H.J., Nennstiel, C., Kern, N., Wendel, L., 2022. The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce. J. Bus. Res. 148, 174–189. https://doi.org/10.1016/j.jbusres.2022.04.034.

Grégoire, Y., Fisher, R.J., 2008. Customer betrayal and retaliation: when your best customers become your worst enemies. J. Acad. Mark. Sci. 36 (2), 247–261. https://doi.org/10.1007/s11747-007-0054-0.

Grün, B., Hornik, K., 2011. Topicmodels: an R package for fitting topic models. J. Stat. Softw. 40 (13), 1–30.

Harris Interactive, 2016. Baromètre de la Confiance des Français dans le Numérique.

Hayes, A.F., 2021. Introduction to Mediation, Moderation, and Conditional Process Analysis, 3rd ed. Guilford Press.

Humphreys, A., Wang, R.J.-H., 2018. Automated text analysis for consumer research. J. Consum. Res. 44 (6), 1274–1306. https://doi.org/10.1093/jcr/ucx104.

IAPP, 2023. Practical considerations from EU enforcement: legal bases and transparency. https://iapp.org/resources/article/practical-considerations-eu-enforcement/.

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

Karwatzki, S., Dytynko, O., Trenz, M., Veit, D., 2017. Beyond the personalization–privacy paradox: privacy valuation, transparency features, and service personalization. J. Manag. Inf. Syst. 34 (2), 369–400. https://doi.org/10.1080/07421222.2017.1334467.

Kim, T., Barasz, K., John, L.K., 2019. Why am I seeing this ad? The effect of ad transparency on ad effectiveness. J. Consum. Res. 45 (5), 906–932. https://doi.org/10.1093/jcr/ucy039.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P., Wetherall, D., 2009. When I am on Wi-Fi, I am fearless. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems, pp. 1993–2002. https://doi.org/10.1145/1518701.1519004.

Konus, U., Verhoef, P., Neslin, S.A., 2008. Multichannel shopper segments and their covariates. J. Retail. 84 (4), 398–413. https://doi.org/10.1016/j.jretai.2008.09.002.

Krafft, M., Arden, C.M., Verhoef, P.C., 2017. Permission marketing and privacy concerns—why do customers (not) Grant permissions? J. Interact. Mark. 39 (3), 39–54. https://doi.org/10.1016/j.intmar.2017.03.001.

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

Li, S., Karahanna, E., 2015. Online recommendation systems in a B2C E-commerce context: a review and future directions. J. Assoc. Inf. Syst. 16 (2), 72–107. https://doi.org/10.17705/1jais.00389.

Linden, T., Khandelwal, R., Harkous, H., Fawaz, K., 2020. The privacy policy landscape after the GDPR. Proc. Priv. Enhancing Technol. 2020 (1), 47–64. https://doi.org/10.2478/popets-2020-0004.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., Wirtz, J., 2021. Corporate digital responsibility. J. Bus. Res. 122, 875–888. https://doi.org/10.1016/j.jbusres.2019.10.006.

Martin, K., 2016. Understanding privacy online: development of a social contract approach to privacy. J. Bus. Ethics 137 (3), 551–569. https://doi.org/10.1007/s10551-015-2565-9.

Martin, K.D., Murphy, P.E., 2017. The role of data privacy in marketing. J. Acad. Mark. Sci. 45 (2), 135–155. https://doi.org/10.1007/s11747-016-0495-4.

Martin, K.D., Borah, A., Palmatier, R.W., 2017. Data privacy: effects on customer and firm performance. J. Mark. 81 (1), 36–58. https://doi.org/10.1509/jm.15.0497.

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, 102348. https://doi.org/10.1016/j.technovation.2021.102348.

Meyer-Waarden, L., Cloarec, J., Adams, C., Aliman, D.N., Wirth, V., 2021. Home, sweet home: how well-being shapes the adoption of artificial intelligence-powered apartments in smart cities. Systèmes d'information & Management 26 (4), 55–88. https://doi.org/10.3917/sim.214.0055.

Miltgen, C.L., Smith, H.J., 2019. Falsifying and withholding: exploring individuals' contextual privacy-related decision-making. Inf. Manag. 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. Psychol. Methods 22 (1), 6–27. https://doi.org/10.1037/met0000086.

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., Wang, S., 2012. Disclosure antecedents in an online service context. J. Serv. Res. 15 (1), 76–98. https://doi.org/10.1177/1094670511424924.

Mummolo, J., Peterson, E., 2019. Demand effects in survey experiments: an empirical assessment. Am. Polit. Sci. Rev. 113 (2), 517–529. https://doi.org/10.1017/S0003055418000837.

Norberg, P.A., Horne, D.R., 2014. Coping with information requests in marketing exchanges: an examination of pre-post affective control and behavioral coping. J. Acad. Mark. Sci. 42 (4), 415–429. https://doi.org/10.1007/s11747-013-0361-6.

noyb, 2022. 226 complaints lodged against deceptive cookie banners. https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners.

Oltvoort, A., de Vries, P., van Rompay, T., Rosen, D., 2019. "I am the eye in the sky – Can you read my mind?" how to address public concerns towards drone use. In: Oinas-Kukkonen, H., Win, K., Karapanos, E., Karppinen, P., Kyza, E. (Eds.), Persuasive Technology: Development of Persuasive and Behavior Change Support Systems. Springer, pp. 103–114. https://doi.org/10.1007/978-3-030-17287-9_9.

Ostherr, K., Borodina, S., Bracken, R.C., Lotterman, C., Storer, E., Williams, B., 2017. Trust and privacy in the context of user-generated health data. Big Data Soc. 4 (1), 1–11. https://doi.org/10.1177/2053951717704673.

Palmatier, R.W., 2008. Interfirm relational drivers of customer value. J. Mark. 72 (4), 76–89. https://doi.org/10.1509/jmkg.72.4.76.

Palmatier, R.W., Martin, K.D., 2019. Data privacy marketing audits, benchmarking, and metrics. In: The Intelligent Marketer's Guide to Data Privacy. Springer International Publishing, pp. 153–168. https://doi.org/10.1007/978-3-030-03724-6_8.

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

Petronio, S., 2000. The boundaries of privacy: praxis of everyday life. In: Petronio, S. (Ed.), Balancing the Secrets of Private Disclosures. Lawrence Erlbaum Associates Publishers, pp. 37–49.

Portes, A., N'Goala, G., Cases, A.-S., 2020. Digital transparency: dimensions, antecedents and consequences on the quality of customer relationships. Recherche et Applications En Marketing (English Edition) 35 (4), 72–98. https://doi.org/10.1177/2051570720973548.

Puntoni, S., Reczek, R.W., Giesler, M., Botti, S., 2021. Consumers and artificial intelligence: an experiential perspective. J. Mark. 85 (1), 131–151. https://doi.org/10.1177/0022242920953847.

Rasoulian, S., Grégoire, Y., Legoux, R., Sénécal, S., 2023. The effects of service crises and recovery resources on market reactions: an event study analysis on data breach announcements. J. Serv. Res. 26 (1), 44–63. https://doi.org/10.1177/10946705211036944.
Rust, R.T., Lemon, K.N., Zeithaml, V.A., 2004. Return on marketing: using customer equity to focus marketing strategy. J. Mark. 68 (1), 109–127. https://doi.org/10.1509/jmkg.68.1.109.24030.
Sahni, N.S., Wheeler, S.C., Chintagunta, P., 2018. Personalization in email marketing: the role of noninformative advertising content. Mark. Sci. 37 (2), 236–258. https://doi.org/10.1287/mksc.2017.1066.
Schnackenberg, A.K., Tomlinson, E.C., 2016. Organizational transparency. J. Manag. 42 (7), 1784–1810. https://doi.org/10.1177/0149206314525202.
Schumacher, C., Eggers, F., Verhoef, P.C., Maas, P., 2023. The effects of cultural differences on Consumers' willingness to share personal information. J. Interact. Mark. 58 (1), 72–89. https://doi.org/10.1177/10949968221136555.
Schumann, J.H., von Wangenheim, F., Groene, N., 2014. Targeted online advertising: using reciprocity appeals to increase acceptance among users of free web services. J. Mark. 78 (1), 59–75. https://doi.org/10.1509/jm.11.0316.
Spiller, S.A., 2011. Opportunity cost consideration. J. Consum. Res. 38 (4), 595–610. https://doi.org/10.1086/660045.
Sundar, S.S., Marathe, S.S., 2010. Personalization versus customization: the importance of agency, privacy, and power usage. Hum. Commun. Res. 36 (3), 298–322. https://doi.org/10.1111/j.1468-2958.2010.01377.x.
Sutanto, J., Palme, E., Tan, C.-H., Phang, C.W., 2013. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Q. 37 (4), 1141–1164. https://doi.org/10.25300/MISQ/2013/37.4.07.
Tam, K.Y., Ho, S.Y., 2006. Understanding the impact of web personalization on user information processing and decision outcomes. MIS Q. 30 (4), 865–890.
TechCrunch, 2022a. Google to update cookie consent banner in Europe following fine. https://tech. crunch.com/2022/04/21/google-to-update-cookie-consent-banner-in-europe-following-fine.
TechCrunch, 2022b. Ireland-led GDPR probe of Yahoo's cookie banners moves to draft decision review. https://techcrunch.com/2022/11/07/yahoo-gdpr-dpc-article-60/.
TechCrunch, 2023. TikTok fined in France for manipulative cookie-consent flow. https://techcrunch.com/2023/01/12/tiktok-cnil-cookie-fine/.
Temming, M., 2018. Smartphone overshare. Sci. News 193 (2), 18–21.
Trusov, M., Ma, L., Jamal, Z., 2016. Crumbs of the cookie: user profiling in customer-base analysis and behavioral targeting. Mark. Sci. 35 (3), 405–426. https://doi.org/10.1287/mksc.2015.0956.
Tucker, C.E., 2014. Social networks, personalized advertising, and privacy controls. J. Market. Res. 51 (5), 546–562. https://doi.org/10.1509/jmr.10.0355.
Vail, M.W., Earp, J.B., AntÓn, A.I., 2008. An empirical study of consumer perceptions and comprehension of web site privacy policies. IEEE Trans. Eng. Manag. 55 (3), 442–454. https://doi.org/10.1109/TEM.2008.922634.
van den Boogaart, K.G., Tolosana-Delgado, R., 2008. "Compositions": a unified R package to analyze compositional data. Comput. Geosci. 34 (4), 320–338. https://doi.org/10.1016/j.cageo.2006.11.017.
Warren, C., Campbell, M.C., 2014. What makes things cool? How autonomy influences perceived coolness. J. Consum. Res. 41 (2), 543–563. https://doi.org/10.1086/676680.
Wattal, S., Telang, R., Mukhopadhyay, T., 2009. Information personalization in a two-dimensional product differentiation model. J. Manag. Inf. Syst. 26 (2), 69–95. https://doi.org/10.2753/MIS0742-1222260204.
Wedel, M., Kannan, P.K., 2016. Marketing analytics for data-rich environments. J. Mark. 80 (6), 97–121. https://doi.org/10.1509/jm.15.0413.
Wiertz, C., Kittinger-Rosanelli, C., 2021. Illuminating the dark: exploring the unintended consequences of digital marketing. NIM Mark. Intell. Rev. 13 (1), 10–17. https://doi.org/10.2478/nimmir-2021-0002.
Wirtz, J., Kunz, W.H., Hartley, N., Tarbit, J., 2023. Corporate digital responsibility in service firms and their ecosystems. J. Serv. Res. 26 (2), 173–190. https://doi.org/10.1177/10946705221130467.
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. Inf. Syst. Res. 23 (4), 1342–1363. https://doi.org/10.1287/isre.1120.0416.
Zhang, F., Pan, Z., Lu, Y., 2023. AIoT-enabled smart surveillance for personal data digitalization: contextual personalization-privacy paradox in smart home. Inf. Manag. 60 (2), 103736 https://doi.org/10.1016/j.im.2022.103736.
Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S.D., Yan, X., Yuan, Q., 2021. Privacy paradox in mHealth applications: an integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. Telematics Inform. 61, 101601 https://doi.org/10.1016/j.tele.2021.101601.

Julien Cloarec is Full Professor of Quantitative Marketing at iaelyon School of Management, Université Jean Moulin Lyon 3, Magellan. Recognized internationally for his expertise in artificial intelligence, his research focuses on the ethical deployment of AI technologies, emphasizing user privacy protection. His interdisciplinary collaborations span regulatory agencies, professional associations, and academic entities, fostering a widespread dialogue on AI ethics. His scholarly contributions have been featured in the Journal of Business Research, Psychology & Marketing, Technovation, Technological Forecasting and Social Change, International Journal of Human Resource Management and Systèmes d'Information et Management.

Charlotte Cadieu is a Ph.D. candidate in Marketing at iaelyon School of Management, Université Jean Moulin Lyon 3, Magellan. She is not only focused on addressing privacy concerns within the business sector but also delves deeply into the realm of corporate digital responsibility. Her research has been presented at the Winter American Marketing Association (AMA) Annual Conference and the European Marketing Academy (EMAC) Annual Conference.

Nour Alrabie is an Assistant Professor of Innovation and Entrepreneurship at Université Toulouse – Jean Jaurès. She explores the complex interplay between collective actions, entrepreneurship, digital innovation, and technology ethics in our rapidly evolving digital landscape. Her research has been published in journals such as Health Services Management Research and Question(s) de Management.