REVIEW ARTICLE

Psychology Marketing WILEY

Digital technologies and privacy: State of the art and research directions

Daniele Scarpi[1] | Gabriele Pizzi[1] | Shashi Matta[2]

[1]Department of Management—University of Bologna (IT), Bologna, Italy

[2]WFI Ingolstadt School of Management—University of Eichstätt-Ingolstadt (DE), Eichstätt, Germany

Correspondence
Daniele Scarpi, Department of Management—University of Bologna (IT), Via Capo di Lucca, 34, 40126 Bologna, Italy.
Email: daniele.scarpi@unibo.it

Abstract

Digital technologies have transformed every aspect of marketing and have brought consumer privacy front and center of research and discourse over the last two decades. Whereas companies and consumers have arguably benefited through the availability and use of data made possible by digitalization, consumer privacy-related concerns raise compelling questions that researchers, companies, and policymakers are addressing. In this review paper, we review privacy related to digital technologies in marketing, highlighting the constantly evolving nature of the field. We provide an overview of the rich contributions made by the articles in the special issue on digital technologies and privacy, and the original insights they provide for researchers and practitioners in four domains—communication, retailing, pricing, and product personalization. We identify and outline future research directions in each of these four domains to expand our understanding of privacy at the intersection of psychology and marketing by motivating new scholarly research and providing actionable insights to managers and policymakers.

KEYWORDS
digital technologies, privacy, review paper

1 | INTRODUCTION

Privacy is a defining issue of our time. In a world where digital technologies impact every aspect of our lives as consumers, the notion of what privacy means, and its consequences, is steadily changing and evolving. Indeed, the scope of what privacy means to consumers has vastly expanded from Warren and "Brandeis" assertion that privacy is the right to be left alone (Warren & Brandeis, 1890) or "Altman's conceptualization of privacy as the selective control of access to oneself or" one's group (Altman, 1976). It now includes the integrity and safety of personal information across platforms/channels/contexts, the right to decide how personal data are used at various stages (Malhotra et al., 2004), and the ability to trade personal information for customized value offerings from marketers (Kraft et al., 2017).

Researchers have contended that many product and marketing innovations result from novel applications of consumer data in digital contexts (Hoffman & Novak, 2018; Lenard & Rubin, 2013) and that consumer privacy concerns about the use of their personal datasets up a trade-off between privacy and innovation (Bleier et al., 2020). This tension is also inherent in the so-called privacy paradox, which refers to the discrepancy between "consumers" expressed privacy concerns and their digital behavior (Xu et al., 2011). Recently, the widespread use of "consumers" digital records during the COVID-19 pandemic has further raised active discussion and debate about privacy (Brough & Martin, 2021). Therefore, this review paper on

consumer privacy at the intersection of psychology, marketing, and digital technologies makes a timely and meaningful contribution to the rich stream of scholarship to enrich our collective understanding of this evolving topic.

The review paper spans four domains—communication, retailing, pricing, personalization of products and services—and utilizes multiple research approaches, including surveys, experiments, linguistic content analysis, and a meta-analysis. Together, these provide novel insights for researchers and managers into "consumers" privacy-related attitudes and behaviors while interacting with digital technologies. In the following sections, we review the research on privacy in the context of digital technologies in marketing in each of the four domains mentioned above (see Figure 1), highlight in this review paper the unique contributions of the articles in the special issue on digital technologies and privacy, and propose future research ideas in these domains (see Figure 2). We conclude with a discussion of additional avenues of research that can motivate scholarly research on privacy across these domains and inform managers and policymakers. Figure 1 provides a conceptual figure across the four domains, while Table 1 summarizes the special issue articles in each domain.

2 | PRIVACY AND COMMUNICATION

Communication privacy is the notion that consumers should be able to share information digitally so that it will only be accessible to their intended recipients. It is particularly relevant to digital communication, and the most frequent research setting is social media

(Aboulnasr et al., 2022; Martin & Palmatier, 2020). Privacy concerns have increased over time due to data breaches and data mismanagement by social media companies, such as the Cambridge Analytica data breach of Facebook users in 2018. Recent research on privacy in social media has added engagement to this equation (Mosteller & Poddar, 2017), which takes the form of posting photos, frequently logging in, and so on. Extending this stream of research, Bright et al. (2021) show that consumers' privacy concerns are negatively related to their social media engagement. Using linguistic content analysis of tweets, Visentin et al. (2021) show that words associated with privacy concerns in a tweet inhibited the virality of the tweet as measured by the number of retweets.

Several constructs have been addressed about privacy in communication: trust (e.g., Frye & Dornisch, 2010; Kamboj et al., 2018; Malhotra et al., 2004), self-efficacy (e.g., Mosteller & Poddar, 2017; Poddar et al., 2009; Yoon et al., 2020), perceived control (e.g., Hajli & Lin, 2016; Sheehan & Hoy, 2000; Taylor et al., 2009), fatigue and information overload (especially on social media; e.g., Choi et al., 2018; Luqman et al., 2017; Maier et al., 2015), perceived benefits, including hedonism (e.g., Cowan et al., 2021).

There is agreement that all these variables can matter. However, the exact relationship between these variables, and the theoretical framework holding them together, is still debated. For instance, in Christofides et al. (2009), trust directly affects information disclosure, while in Bright et al. (2021), trust is a moderator of the privacy concerns—engagement relationship. Furthermore, Krasnova et al. (2012) find higher (lower) privacy concerns in cultures with high (low) uncertainty avoidance. In different domains, cultures have been related to different mindsets (D. H. Kim et al., 2018; Rim et al., 2009) and
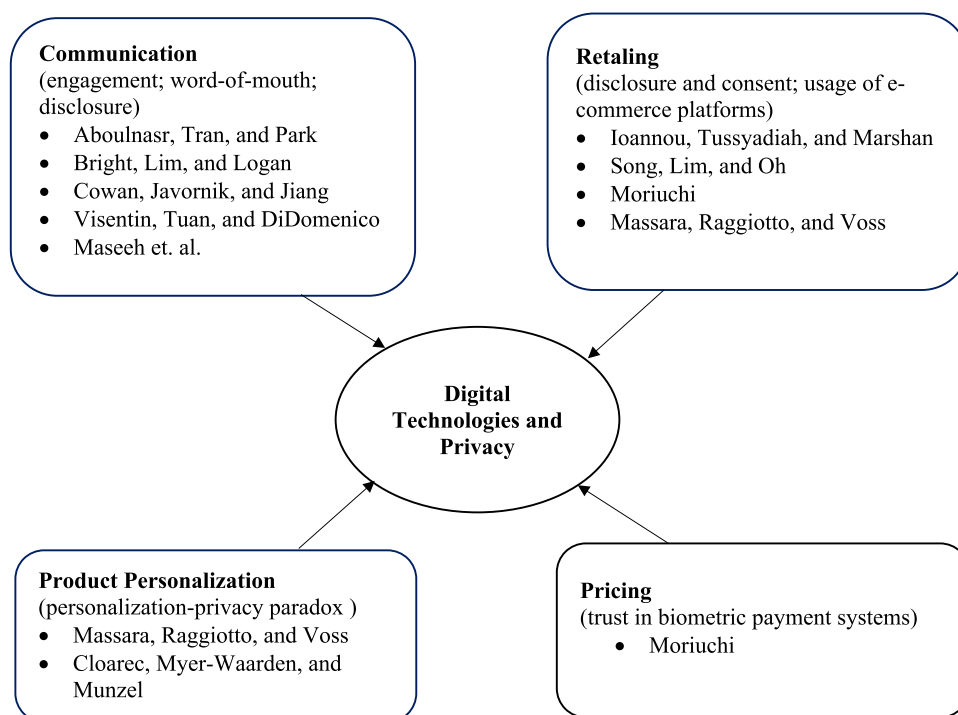

FIGURE 1 Special issue articles on digital technologies and privacy: conceptual figure.
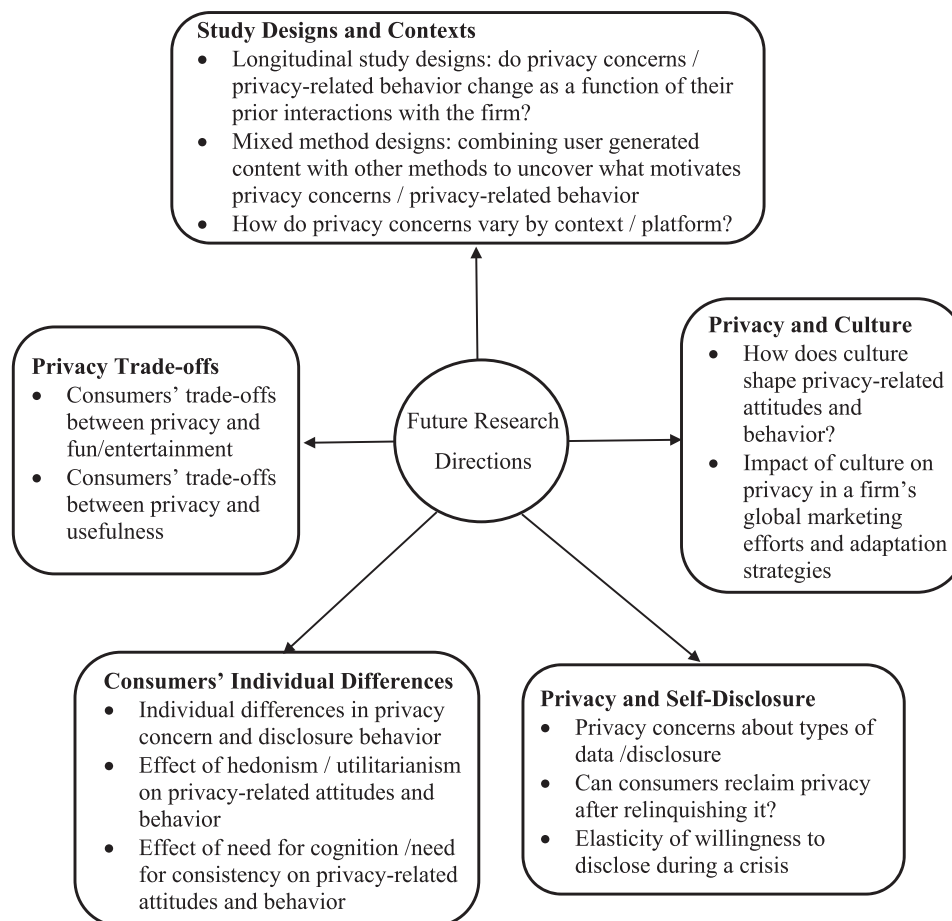
FIGURE 2 Future research on digital technologies and privacy.

addressed in terms of construal level theory (Liberman & Trope, 1998). Thus, a logical bridge could be built between Krasnova et al. (2012) and Cowan et al. (2021). They address privacy concerns from a CLT perspective, though not referring to culture but perceived usefulness, word-of-mouth, and usage intention. Similarly, Lwin et al. (2016) and Mosteller and Poddar (2017) use Regulatory Focus as the theoretical perspective to address privacy concerns in communication.

Thus, while communication is one of the most commonly addressed domains for privacy research, it also presents a scattered set of partially contradictory relationships. For instance, the privacy paradox in communication refers to consumers who, despite their privacy concerns, still keep disclosing instead of protecting their personal information (Taddicken, 2014). This phenomenon has been addressed in several contexts, such as e-commerce (Zareef & Tejay, 2021) and personalized advertising (Tucker, 2014). Future research is required here not to add additional drivers of privacy concerns, but rather to combine the evidence from previous studies in a single, consistent, theoretical framework. In this vein, Maseeh et al. (2021) offer a metanalysis of privacy studies, while Aboulnasr, et al. (2022) offer a literature review table focused specifically on privacy in communication.

In addition, looking diachronically at studies on privacy in communication, the lines are more and more blurred with those of

new technologies and privacy-related constructs. As social media are evolving technologically, so are privacy concerns. For instance, Cowan et al. (2021) investigate the impact of filters that consumers use as augmented reality overlays of the physical environment. This consideration also allows Cowan et al. (2021) to address hedonism's role and advance a relationship between usefulness, hedonism, and flow in communication. Do consumers relax their privacy concerns when they derive fun from social media? There is much room for future research here. For instance, translating Hoffman and Novak's (2009, 2018) considerations about flow into today's domain of privacy in communication would allow investigating novel prospects. Similarly, considerations about the fun-usefulness dyad could be investigated from the recent perspective that hedonic and utilitarian considerations guide different mental representations of the same experience (Scarpi, 2021a, 2021b).

3 | PRIVACY AND RETAILING

The last two decades have witnessed an increasing adoption of digital technologies by online and offline retailers (Roggeveen & Sethuraman, 2020). On the one hand, shopper-facing technologies enable retailers to provide customers with a plethora of self-service

TABLE 1 Special issue articles on digital technologies and privacy across four domains.

Authors	Main findings	Research method(s)	Key dependent variables	Privacy-related variable(s)	Domain(s)
Aboulnasr, Tran, and Park	Consumers' social networking site identification and the degree to which they disclose personal information on that social networking site affect their brand engagement on that platform	Online survey	Social media brand engagement	Personal information disclosure	Communication
Bright, Lim, and Logan	Privacy concern has a negative effect on social media engagement and this relationship changes to positive when users have high trust in the social media platform	Online survey	Social media engagement	Privacy concern; privacy protection behaviors	Communication
Cowan, Javornik, and Jiang	Privacy concerns with an augmented reality (AR) face filter on social media decrease behavioral intentions and word-of-mouth, mediated by perceived usefulness and flow	Online survey; online experiment	Intention to use AR face filter apps; share word-of-mouth	Privacy concern; privacy policy disclosure (concrete or abstract)	Communication
Visentin, Tuan, and Di Domenico	Words associated with privacy concerns in a tweet inhibit the virality of the tweet, whereas words associated with conspiracy theories in a tweet improve the probability of retweeting	Linguistic content analysis	Number of retweets of a tweet	Privacy concerns	Communication
Maseeh et. al.	"Consumers" privacy concerns are positively affected by risk perceptions, while benefit perceptions, familiarity, reputation, privacy policy, and trust significantly mitigate their privacy concerns. Privacy concerns negatively affect attitude towards, and usage of e-commerce platforms	Meta-analysis	Attitude towards, and usage of e-commerce platform	Privacy concerns	Communication; retailing
Ioannou, Tussyadiah, and Marshan	"Consumers" trait mindfulness has a negative effect on their privacy concerns, and privacy concerns negatively influence "consumers" willingness to disclose personal information to firms online	Online experiments	Willingness to disclose personal information	Privacy concerns	Retailing
Song, Lim, and Oh	Consumers' perceived usefulness of personalization technology is positively related to their behavioral intentions to use an e-commerce mobile app, and consumers' privacy concerns and willingness to self-disclose moderate this relationship	Online Experiments	Intentions to use am e-commerce mobile app	Privacy concerns; willingness to self-disclose; personalization	Retailing
Moriuchi	Consumers prefer using a biometric payment system in physical stores than online. Consumers' trust and attitude toward the technology have a stronger mediating role for online than in-store intention to use	Online survey; online experiment	Intention to use biometric payment system	Perceived risk; trust in technology	Retailing; pricing

TABLE 1 (Continued)

Authors	Main findings	Research method(s)	Key dependent variables	Privacy-related variable(s)	Domain(s)
Massara, Raggiotto, and Voss	The relationship between perceived privacy-related risk and consent for personal data disclosure is mediated by "consumers" mental accounting of risks and perceived benefits related to data disclosure, and familiarity with the data collector	Online experiments	Consent for data disclosure	Perceived privacy-related risk	Retailing; product personalization
Cloarec, Myer-Waarden, and Munzel	Happiness with the Internet is a strong driver of "consumers" willingness to disclose information in exchange for personalization, surpassing even the more widely used privacy-related constructs (i.e., trust and risk beliefs)	Online survey	Willingness to disclose information in exchange for personalization	Trust beliefs; risk beliefs	Product personalization

and customized services (Inman & Nikolova, 2017). On the other hand, the proliferation of retail technologies which need to be fed with data has raised significant privacy issues from the consumer side (Margulis et al., 2020). Indeed, recent research has documented that privacy concerns might significantly undermine "consumers" intentions to adopt in-store technologies as long as the cost connected to the data disclosure is not outweighed by the benefits provided by the technology (Pizzi & Scarpi, 2020).

Marketing literature has traditionally explained "consumers" acceptance of retail technologies employing the Technology Acceptance Model (TAM hereafter), which posits that technology acceptance is driven by consumer perceptions of the technology's usefulness and ease of use (Davis, 1989). Yet, the original formulation of the TAM model does not fully incorporate the growing privacy concerns stemming from the adoption of digital technologies into its conceptual structure. Thus, Song et al. (2021) incorporate privacy concerns into the TAM model, showing that consumers' privacy concerns and willingness to self-disclose significantly moderate the personalization-intention relationship. Specifically, they found that the usefulness and the accuracy of personalized recommendations on e-commerce websites are insufficient to drive "consumers" behavioral intention as long as "consumers" privacy concerns and self-disclosure preferences are not fully addressed.

Maseeh et al. (2021), in their meta-analysis, summarize the main antecedents of e-commerce "customers" privacy concerns from extant studies. Results from the meta-analysis show that risk perceptions exert the strongest impact on privacy concerns which can be dampened by the clarity of the privacy policy and the e-tailer's trustworthiness (Maseeh et al., 2021). Accordingly, a relevant challenge for future research is systematically incorporating these relevant dimensions of privacy concerns into more traditional models based on the TAM. Massara et al. (2021) similarly find that the relationship between perceived privacy-related risk and consent for personal data disclosure when purchasing online is mediated by consumers' mental accounting of risks and perceived benefits related to data disclosure and familiarity with the firm.

Further research is also needed to understand consumers' individual differences in their privacy-related behavior when shopping online. For instance, Ioannou et al. (2021) examine a previously unexplored individual difference variable, trait mindfulness, finding that consumers' trait mindfulness negatively affects their privacy concerns and influences willingness to disclose personal information to firms online.

At the same time, such a huge emphasis on privacy concerns in the context of online retailing has not found a corresponding interest in privacy concerns in the offline channel (Pizzi & Scarpi, 2020). Yet, addressing the difference between the potential privacy threats which might arise in the offline compared to the online context is not a trivial issue (Bahri et al., 2018). On the one hand, the physical proximity between the consumer and the retail environment might increase "consumers" trust (Darke et al., 2016). On the other hand, consumers shopping in an offline retail store might be exposed to a wider variety of technologies which imply the disclosure of

information beyond registration data and usage behavior (Kindt, 2013).

Literature in retailing has addressed several in-store technologies that might significantly challenge "consumers" beliefs about how their personal data are fully protected in offline retail stores (Bonetti et al., 2018). For instance, research has proposed technological solutions to unobtrusively track "customers" movements, such as Bluetooth or RFID tags to monitor the inventory (Phua et al., 2015) and better segment customers (Landmark & Sjøbakk, 2017). Similarly, other scholars advanced AI-enabled face recognition cameras to track the paths followed by consumers while shopping (Garaus et al., 2021).

Another stream of literature has focused on checkout systems to provide seamless payment experiences to customers through self-scanning devices (Inman & Nikolova, 2017), biometric fingerprints (Clodfelter, 2010), or facial recognition (Moriuchi, 2021; van Esch et al., 2021) identification. In-store technologies have also been found to improve the experiential side of shopping through the application of Augmented Reality (van Esch et al., 2019) or smart mirrors (Pantano et al., 2017) or by providing an immersive shopping experience in a digitally rendered Virtual Reality store (Pizzi et al., 2019).

Overall, these technologies provide an unprecedented opportunity for retailers to get deep insights into "customers" behaviors inside a physical store—similarly to online retailers relying on cookies and analytics—and provide customers with superior shopping experiences. Alongside this direction, literature has shown that consumers are willing to disclose their behavioral and biometric information when they perceive that the personalization benefit they receive in exchange is worth the risk of losing their personal data (D. Kim et al., 2019). In this regard, recent literature has witnessed a pervasive personalization-privacy paradox in "consumers" behaviors dealing with the disclosure of personal information in retail contexts (Martin & Murphy, 2017). Recent research has provided meaningful indications on how retailers can facilitate "consumers" acceptance of data disclosure by leveraging, for instance, warmth perceptions (Aiello et al., 2020) or gamification (Bidler et al., 2020). However, much more research is needed to explore the psychology of "customers" data disclosure to interpret them according to a less paradoxical lens. At the same time, more empirical and theoretical work is required to understand if and to what extent different types of data (e.g., behavioral and biometric) give rise to different types of privacy concerns (Ioannou et al., 2020) and their consequences on "consumers" intentions and behaviors.

4 | PRIVACY AND PRICING

Retailers adopt new in-store technologies to offer more customized and engaging shopping experiences to their customers and gather more detailed insights into "shoppers" behaviors. Among these, literature has devoted attention to payment methods, addressing automatic checkout and self-scanning "tools" ability to stimulate customer satisfaction via utilitarian (e.g., less waiting times) and hedonic (e.g., more fun using the devices) benefits (Marzocchi & Zammit, 2006).

Recent studies have investigated the effectiveness of the latest technological innovations related to automatic checkouts, such as fingerprint authentication at checkout (Clodfelter, 2010) or the "Just Walk Out" technology (e.g., Amazon Go). These technologies allow customers to be automatically charged the price thanks to AI-enabled object recognition software, which detects the products put by each customer in their shopping cart (Cui et al., 2021). Although providing a more frictionless experience to customers, these tools are not free from limitations in terms of potential loss of control over the shopping experience and personal data (van Esch et al., 2021). A recent study has built on the unified theory of acceptance and use of technology and the theory of mind (Moriuchi, 2021). It demonstrates that consumers are skeptical of using biometric data for automatic checkout purposes, especially in the online channel, and that performance expectations and perceived risk on usage intention are moderated by self-efficacy.

However, beyond providing customers with a seamless checkout experience, these technologies display the potential to improve "retailers" ability to charge personalized prices significantly. Indeed, recent research has paved the way for "retailers" usage of big data to estimate "customers" price elasticity at the individual customer level (Bradlow et al., 2017). In this vein, literature has addressed algorithmic pricing as a suitable approach for setting the optimal product price at the customer level (Buhmann et al., 2020). Such algorithms need to be fed with a considerable amount of customer-level data (Fisher et al., 2018; Miklós-Thal & Tucker, 2019).

Technologies such as AI-enabled face recognition cameras can help retailers gather the input information to customize messages in-store (Garaus et al., 2021) in a way that could also be applied to set customized prices. Extant research has demonstrated that delivering an accurate, personalized pricing strategy improves "retailers" profitability (Sahay, 2007). Still, at the same time, it might generate privacy concerns from the customer's perspective (Miettinen & Stenbacka, 2015). In this vein, the literature has extensively attempted to provide the computational tools to set the most accurate algorithms for price personalization. However, literature on how consumers react to personal data requests by price personalization algorithms is still scattered (Seele et al., 2021). In these regards, Xia et al. (2010) explored "consumers" fairness perceptions of personalized prices, relating fairness to the quality of the output (i.e., the price charged) rather than of the procedures (i.e., the perceived risk of data disclosure). Therefore, there is still room in the literature to explore in-depth how algorithmic price personalization might trigger "consumers" privacy concerns.

5 | PRIVACY AND PERSONALIZATION OF PRODUCTS AND SERVICES

Several firms now compete in mature markets, where they usually offer products of about the same (high) quality to consumers with high expectations. The old strategic options of quality or price leadership no longer represent the market 10 years ago. On the one

hand, quality often means the possibility to personalize a product or service. Once exclusive to the top-end of the luxury market (e.g., Rolls Royce co-designing with the customers its 5000 cars per year), personalization is now becoming more and more common for goods with a much lower price tag (Torn & Vaneker, 2019; Vesanen, 2007). For instance, the personalization of a smartphone cover or ingredients in take-away food. On the other hand, price leaders have started eroding the market share of their competitors also by offering personalization. For instance, Amazon allows to select a custom delivery place and date and to add a custom greeting card.

The pervasive diffusion of personalization is largely due to modern technologies that significantly lowered the cost of personalized or atypical products (Scarpi et al., 2019; Sodhi & Tang, 2017). However, as goods personalization increases, so do concerns for privacy because personalization requires—by definition— knowledge about the buyer's socio-demographics, geolocation, behavior, and—in some cases—even biometric data (e.g., personalized running shoes by Nike) (Toch et al., 2012). Sometimes these data are acquired with the awareness of the customer, and other times—more worryingly— without it (Sundar & Marathe, 2010).

Nowadays, scholars (Jiang et al., 2013) and practitioners treat personal information as a strategic intangible resource. Accordingly, the issue of privacy concerns in products and services is usually read from the theoretical perspective of Social Exchange Theory (Emerson, 1981). According to it, individuals are willing to provide resources if they feel this helps them gain benefits (Molm et al., 2000). Thus, Social Exchange Theory has been used to understand consumers' willingness to disclose personal information (the resource) in exchange for personalization (the benefit) (Martin & Murphy, 2017). A complementary theoretical perspective is that of a trade-off between information disclosure (the loss) and personalization acquisition (the gain) (White, 2004).

Such a simple yet powerful theoretical structure has been quickly enriched by considering several other variables that could interact and shape the outcome of the social exchange or trade-off (Cloarec2021). For instance, in assessing their costs for disclosing personal information, consumers ponder the risk of disclosing the safety of the shared data so that trust and perceived risk both come into the equation (Malhotra et al., 2004; Toch et al., 2012; White, 2004).

The more recent development of the Social Exchange Theory approach to understanding the relationship between privacy and "goods" production has shown that it can successfully combine several theories. For instance, Cloarec et al. (2021) add Construal Level Theory (Liberman & Trope, 1998) to the equation, providing an example of how future research could integrate Social Exchange Theory with different perspectives. Reading the privacy paradox in terms of psychological distance, Cloarec et al. (2021) bring happiness into the equation. Happiness raises individuals' construal level (Labroo & Patrick, 2009), leading individuals to apply an intertemporal discount: present costs (i.e., information disclosure) are weighted less than future gains (i.e., personalization of products and services). While such a phenomenon has been documented in other contexts

(e.g., healthy vs. vice foods; Laran, 2010; Wertenbroch, 1998), it is novel in the domain of privacy.

Similarly, other studies have started addressing hedonism and utilitarianism regarding privacy (Pizzi & Scarpi, 2020), showing that consumers' reaction changes depending on shopping orientation. "Consumers" decision-making process differs from hedonic and utilitarian products (Roggeveen et al., 2015), online and offline (Scarpi, 2012). Furthermore, recent works have related hedonism and utilitarianism to Construal Level Theory (Scarpi, 2021a, 2021b), which has been proven to increase the explanatory power of Social Exchange Theory (Cloarec et al., 2021). Thus, hedonism and utilitarianism appear to be possible integrations to the Social Exchange Theory framework for understanding the trade-off between disclosing personal information and gaining personalization benefits.

In summary, given that privacy in products and services is a relatively under-researched area but is quickly gaining momentum as personalization can also involve the delivery of services (Huang & Rust, 2021), there appears to be much space for future research in this direction.

6 | CONCLUSION AND ADDITIONAL AVENUES FOR FUTURE RESEARCH

Every new consumer technology brings new challenges and questions about consumer privacy. Navigating these challenges requires a deep understanding of "consumers" evolving perceptions of privacy and their related cognitive, emotional, and behavioral responses. The research included in this review paper aims to deepen the understanding of digital technologies and privacy across four domains—communication, retailing, pricing, and product personalization. These articles posed novel research questions for new and emerging digital technologies and utilized multiple research approaches, including surveys, experiments, linguistic content analysis, and a meta-analysis. In the preceding sections, this review paper addressed the research on privacy in the context of digital technologies in marketing in each of the four domains, highlighted the unique contributions of articles in the special issue on digital technologies and privacy, and proposed future research ideas in these domains.

In addition to the future research ideas presented within each of the four domains, we identified three additional avenues for future research that cut across the four domains and provide fruitful paths for further inquiry.

6.1 | Privacy trade-offs and crises

Disclosure of personal information was a key variable examined in multiple articles and much of the research on consumer privacy. "Consumers" willingness to disclose personal information can be influenced by various individual difference variables and situational

variables: one contemporary context that provided a veritable stress test was the COVID-19 pandemic. Though research in the special issue on digital technologies and privacy did not explicitly address the pandemic, other recent research has argued that consumers lost much of their control over sensitive personal data such as their health and location data during the pandemic (Brough & Martin, 2021). A broader research question is whether privacy, once relinquished by consumers in times of crisis, can be reclaimed by them. In other words, how elastic is "consumers" willingness to disclose personal information in times of crisis, and does this elasticity vary across the four domains? Insights from this line of inquiry can inform the discourse on consumer rights, policy interventions, and managerial practice.

6.2 | Privacy and culture

Extant research has acknowledged that the privacy environment (including privacy regulations) could differ among countries, and marketers should tailor their approach to data collection and data usage accordingly. However, recent research on systematic cross-cultural differences in "consumers" privacy-related attitudes and behaviors remains scant. Not surprisingly, multiple researchers (e.g., Aboulnasr et al., 2022; Cowan et al., 2021; Ioannou et al., 2021) advocate for future research that examines the role of culture. Whereas "consumers" experience and fluency with digital technologies may vary across countries and set up different privacy expectations, the more interesting avenues for future inquiry lie in the interaction of specific cultural difference variables and the digital context. Some early evidence (Bellman et al., 2004) suggests that "consumers" cultural values (operationalized through Hofstede indices) are correlated with specific aspects of privacy-related concerns. Future research can examine how culture shapes "consumers" privacy-related attitudes and behavior and interacts with specific digital technology contexts. Given that digital technology platforms increasingly underlie most marketing activities, insights from such research on privacy and culture can strongly impact "firms" global marketing efforts and adaptation strategies.

6.3 | Study designs and contexts

Finally, as multiple researchers contend (Maseeh et al., 2021; Song et al., 2021), most studies on consumer privacy are cross-sectional, and longitudinal studies can provide richer insights. Marketers use multiple data sources on consumers across time and conduct sophisticated analyses to target consumers with personalized offerings. However, academic research on consumer privacy seems to lag practice and has not explored whether "consumers" privacy concerns or privacy-related behavior change over time and as a function of prior interactions with a company. Further, academic research on privacy has not adequately leveraged the vast amount of already existing user-generated content online and on social media to

study privacy-related attitudes and behavior. For instance, Visentin et al. (2021) use linguistic content analysis to examine whether words in a tweet associated with privacy concerns affect the virality of the tweet. Similar investigations that analyze user-generated content and even combine such analysis with other research methods can provide fertile opportunities for mixed-method approaches to uncovering privacy-related insights.

Similarly unexplored to a large extent in marketing and consumer research is the notion of how "consumers" notions of privacy, their concerns, and related behaviors vary across contexts. Indeed, as privacy researcher and ethicist Nissenbaum (2018) asserts in her theory of contextual integrity, companies should respect the context in which consumers provide personal information as these contexts set up norms about the appropriateness of the use of such personal data. Future research should investigate "consumers" privacy-related attitudes and behavior across different contexts to understand whether "consumers" privacy concerns (and the privacy paradox) are driven by expectations specific to the context. Perhaps consumers think of privacy differently when they engage with brands on social media, versus when they interact with health care service providers on an app, versus when they shop and pay for products and services on an e-commerce platform. Thus, longitudinal study designs and studies that track consumers across different contexts can broaden our understanding of how consumers think of privacy.

DATA AVAILABILITY STATEMENT
Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID
Daniele Scarpi [iD] http://orcid.org/0000-0001-9652-9109
Gabriele Pizzi [iD] http://orcid.org/0000-0002-7531-9003

REFERENCES
Aboulnasr, K., Tran, G. A., & Park, T. (2022). Personal information disclosure on social networking sites. *Psychology & Marketing*, *39*(2), 294–308.

Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., & Viglia, G. (2020). 'Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth. *Journal of Retailing*, *96*(4), 490–506.

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, *8*(March), 7–29.

Bahri, L., Carminati, B., & Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. *Online Social Networks and Media*, *6*, 18–25.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324.

Bidler, M., Zimmermann, J., Schumann, J. H., & Widjaja, T. (2020). Increasing 'consumers' willingness to engage in data disclosure

processes through relevance-illustrating game elements. *Journal of Retailing*, 96(4), 507–523.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466–480.

Bonetti, F., Warnaby, G., & Quinn, L. (2018). Augmented reality and virtual reality in physical and online retailing: A review, synthesis and research agenda, *Augmented reality and virtual reality* (pp. 119–132). Springer-Verlag.

Bradlow, E. T., Gangwar, M., Kopalle, P., & Voleti, S. (2017). The role of big data and predictive analytics in retailing. *Journal of Retailing*, 93(1), 79–95.

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*, 38(10), 1712–1722.

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

Buhmann, A., Paßmann, J., & Fieseler, C. (2020). Managing algorithmic accountability: Balancing reputational concerns, engagement strategies, and the potential of rational discourse. *Journal of Business Ethics*, 163(2), 265–280.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology & Behavior*, 12(3), 341–345.

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2021). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, 39(3), 647–661.

Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17(3), 181–188.

Cowan, K., Javornik, A., & Jiang, P. (2021). Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs. *Psychology & Marketing*, 38(10), 1799–1813.

Cui, Y. (G.), van Esch, P., & Jain, S. P. (2021). Just walk out: The effect of AI-enabled checkouts. *European Journal of Marketing Forthcoming*.

Darke, P. R., Brady, M. K., Benedicktus, R. L., & Wilson, A. E. (2016). Feeling close from afar: The role of psychological distance in offsetting distrust in unfamiliar online retailers. *Journal of Retailing*, 92(3), 287–299.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13, 319–340.

Emerson, R. M. (1981). Social exchange theory. In M. Rosenberg, & R. Turner (Eds.), *Social psychology: Sociological perspectives* (pp. 31–65). Basic Books.

Fisher, M., Gallino, S., & Li, J. (2018). Competition-based dynamic pricing in online retailing: A methodology validated with field experiments. *Management Science*, 64(6), 2496–2514.

Frye, N. E., & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior*, 26(5), 1120–1127.

Garaus, M., Wagner, U., & Rainer, R. C. (2021). Emotional targeting using digital signage systems and facial recognition at the point-of-sale. *Journal of Business Research*, 131, 747–762.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, 133(1), 111–123.

Hoffman, D. L., & Novak, T. P. (2009). Flow online: Lessons learned and future prospects. *Journal of Interactive Marketing*, 23(1), 23–34.

Hoffman, D. L., & Novak, T. P. (2018). Consumer and object experience in the internet of things: An assemblage theory approach. *Journal of Consumer Research*, 44(6), 1178–1204.

Huang, M. H., & Rust, R. T. (2021). Engaged to a robot? The role of AI in service. *Journal of Service Research*, 24(1), 30–41.

Inman, J. J., & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing*, 93(1), 7–28.

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, 54, 102122.

Ioannou, A., Tussyadiah, I., & Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing*, 38(10), 1766–1778.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24(3), 579–595.

Kamboj, S., Sarmah, B., Gupta, S., & Dwivedi, Y. (2018). Examining branding co-creation in brand communities on social media: Applying the paradigm of Stimulus-Organism-Response. *International Journal of Information Management*, 39, 169–185.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273–281.

Kim, D. H., Sung, Y., & Drumwright, M. (2018). Where I come 'from' determines, how I construe my 'future': The fit effect of culture, temporal distance, and construal level. *International Journal of Advertising*, 37(2), 270–288.

Kindt, E. (2013). Best practices for privacy and data protection for the processing of biometric data. In P Campisi (Ed.), *Security and privacy in biometrics* (pp. 339–367). Springer.

Kraft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions? *Journal of Interactive Marketing*, 39, 39–54.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, 4(3), 127–135.

Labroo, A. A., & Patrick, V. M. (2009). Psychological distancing: Why happiness helps you see the big picture. *Journal of Consumer Research*, 35(5), 800–809.

Landmark, A. D., & Sjøbakk, B. (2017). Tracking customer behaviour in fashion retail using RFID. *International Journal of Retail & Distribution Management*, 45(7/8), 844–858.

Laran, J. (2010). Choosing your future: Temporal distance and the balance between self-control and indulgence. *Journal of Consumer Research*, 36(6), 1002–1015.

Lenard, T. M., & Rubin, P. H. (2013). *The big data revolution: Privacy considerations* (pp. 1–2). Technology Policy Institute.

Liberman, N., & Trope, Y. (1998). The role of feasibility and desirability considerations in near and distant future decisions: A test of temporal construal theory. *Journal of Personality and Social Psychology*, 75(1), 5–18.

Luqman, A., Cao, X., Ali, A., Masood, A., & Yu, L. (2017). Empirical investigation of Facebook discontinues usage intentions based on SOR paradigm. *Computers in Human Behavior*, 70, 544–555.

Lwin, M. O., Wirtz, J., & Stanaland, A. J. S. (2016). The privacy dyad: Antecedents of promotion- and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern. *Internet Research*, 26(4), 919–941.

Maier, C., Laumer, S., Eckhardt, A., & Weitzel, T. (2015). Giving too much social support: Social overload on social networking sites. *European Journal of Information Systems*, 24(5), 447–464.

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.

Margulis, A., Boeck, H., & Laroche, M. (2020). Connecting with consumers using ubiquitous technology: A new model to forecast consumer reaction. *Journal of Business Research*, 121, 448–460.

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.

Martin, K. D., & Palmatier, R. W. (2020). Data privacy in retail: Navigating tensions and directing future research. *Journal of Retailing*, 96(4), 449–457.

Marzocchi, G. L., & Zammit, A. (2006). Self-scanning technologies in retail: Determinants of adoption. *The Service Industries Journal*, 26(6), 651–669.

Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., & Ashaduzzaman, M. (2021). Privacy concerns in e-commerce: A multilevel meta-analysis. *Psychology & Marketing*, 38(10), 1779–1798.

Massara, F., Raggiotto, F., & Voss, G. W. (2021). Unpacking the privacy paradox of consumers. *Psychology & Marketing*, 38(10), 1814–1846.

Miettinen, T., & Stenbacka, R. (2015). Personalized pricing versus history-based pricing: Implications for privacy policy. *Information Economics and Policy*, 33, 56–68.

Miklós-Thal, J., & Tucker, C. (2019). Collusion by algorithm: Does better demand prediction facilitate coordination between sellers? *Management Science*, 65(4), 1552–1561.

Mohammed, Z. A., & Tejay, G. P. (2021). Examining the privacy paradox through 'individuals' neural disposition in e-commerce: An exploratory neuroimaging study. *Computers & Security*, 104, 102201.

Molm, L. D., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology*, 105(5), 1396–1427.

Moriuchi, E. (2021). An empirical study of consumers' intention to use biometric facial recognition as a payment method. *Psychology & Marketing*, 38(10), 1741–1765.

Mosteller, J., & Poddar, A. (2017). To share and protect: Using regulatory focus theory to examine the privacy paradox of 'consumers' social media engagement and online privacy protection behaviors. *Journal of Interactive Marketing*, 39, 27–38.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, 24(3), 831–852.

Pantano, E., Rese, A., & Baier, D. (2017). Enhancing the online decision-making process by using augmented reality: A two country comparison of youth markets. *Journal of Retailing and Consumer Services*, 38, 81–95.

Phua, P., Page, B., & Bogomolova, S. (2015). Validating Bluetooth logging as metric for shopper behaviour studies. *Journal of Retailing and Consumer Services*, 22, 158–163.

Pizzi, G., & Scarpi, D. (2020). Privacy threats with retail technologies: A consumer perspective. *Journal of Retailing and Consumer Services*, 56, 102160.

Pizzi, G., Scarpi, D., Pichierri, M., & Vannucci, V. (2019). Virtual reality, real reactions?: Comparing 'consumers' perceptions and shopping orientation across physical and virtual-reality retail stores. *Computers in Human Behavior*, 96, 1–12.

Poddar, A., Mosteller, J., & Ellen, P. S. (2009). 'Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs*, 43(3), 419–448.

Rim, S., Uleman, J. S., & Trope, Y. (2009). Spontaneous trait inference and construal level theory: Psychological distance increases nonconscious trait thinking. *Journal of Experimental Social Psychology*, 45(5), 1088–1097.

Roggeveen, A. L., Grewal, D., Townsend, C., & Krishnan, R. (2015). The impact of dynamic presentation format on consumer preferences for hedonic products and services. *Journal of Marketing*, 79(6), 34–49.

Roggeveen, A. L., & Sethuraman, R. (2020). How the COVID-19 pandemic may change the world of retailing. *Journal of Retailing*, 96(2), 169–171.

Sahay, A. (2007). How to reap higher profits with dynamic pricing. *MIT Sloan Management Review*, 48(4), 53–60.

Scarpi, D. (2012). Work and fun on the internet: The effects of utilitarianism and hedonism online. *Journal of Interactive Marketing*, 26(1), 53–67.

Scarpi, D. (2021a). A construal-level approach to hedonic and utilitarian shopping orientation. *Marketing Letters*, 32(2), 261–271.

Scarpi, D. (2021b). The importance of consumer engagement in brand heritage advertising: How feeling close to a brand can increase willingness to pay more. *Journal of Advertising Research*, 61(3), 334–345.

Scarpi, D., Pizzi, G., & Raggiotto, F. (2019). The extraordinary attraction of being ordinary: A moderated mediation model of purchase for prototypical products. *Journal of Retailing and Consumer Services*, 49, 267–278.

Seele, P., Dierksmeier, C., Hofstetter, R., & Schultz, M. D. (2021). Mapping the ethicality of algorithmic pricing: A review of dynamic and personalized pricing. *Journal of Business Ethics*, 170(4), 697–719.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62–73.

Sodhi, M., & Tang, C. S. (2017). Supply chains built for speed and customization. *MIT Sloan Management Review*, 58(4), 58419.

Song, Y. W., Lim, H. S., & Oh, J. (2021). "We think you may like this": An investigation of electronic commerce personalization for privacy-conscious consumers. *Psychology & Marketing*, 38(10), 1723–1740.

Sundar, S. S., & Marathe, S. S. (2010). Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research*, 36(3), 298–322.

Taddicken, M. (2014). The "Privacy Paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19, 248–273.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. Electronic Commerce Research, 9(3), 203–223.

Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, 22(1-2), 203–220.

Torn, I. A. R., & Vaneker, T. H. (2019). Mass personalization with Industry 4.0 by SMEs: A concept for collaborative networks. *Procedia Manufacturing*, 28, 135–141.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546–562.

van Esch, P., Arli, D., Gheshlaghi, M. H., Andonopoulos, V., von der Heidt, T., & Northey, G. (2019). Anthropomorphism and augmented reality in the retail environment. *Journal of Retailing and Consumer Services*, 49, 35–42.

van Esch, P., Cui, Y., & Jain, S. P. (2021). Self-efficacy and callousness in consumer judgments of AI-enabled checkouts. *Psychology & Marketing*, 38(7), 1081–1100.

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing*, 41(5/6), 409–418.

Visentin, M., Tuan, A., & Di Domenico, G. (2021). Words matter: How privacy concerns and conspiracy theories spread on Twitter. *Psychology & Marketing*, 38(10), 1828–1846.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.

Wertenbroch, K. (1998). Consumption self-control by rationing purchase quantities of virtue and vice. *Marketing Science*, 17(4), 317–337.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, *14*(1-2), 41–51.

Xia, L., Kukar-Kinney, M., & Monroe, K. B. (2010). Effects of 'consumers' efforts on price and promotion fairness perceptions. *Journal of Retailing*, *86*(1), 1–10.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52.

Yoon, J., Vonortas, N. S., & Han, S. (2020). Do-It-Yourself laboratories and attitude toward use: The effects of self-efficacy and the perception of security and privacy. *Technological Forecasting and Social Change*, *159*, 120192.