Freedom from interference: Decisional privacy as a dimension of consumer privacy online

Lena V. Bjørlo[1] 📀

Abstract

The introduction of AI-based technologies has dramatically altered the premises for consumer privacy, enabling the unprecedented manipulation of consumers' decision-making online. Given these recent threats to consumer privacy and autonomy, and considering autonomy as the ultimate outcome of privacy, I propose that a reconceptualization is warranted to reflect contemporary consumer privacy challenges and to realign the concept with its theoretical foundations. To this end, I introduce the dimension of decisional privacy, focused on autonomy versus interference in consumer decision-making. Building on previous privacy literature and extending previous theorizing about information privacy and decisional privacy as complementary, I posit that these two dimensions of privacy together comprise consumer privacy. Addressing protection from interference as an under-communicated function of consumer privacy, the paper aims to clarify, exemplify, and engage in the conceptual development of decisional privacy in the context of consumer decision-making online. In addition to its significance for consumer wellbeing and democracy collectively, the extension of consumer privacy to explicitly encompass interference has theoretical implications for privacy concern, the proxy used to measure privacy, yielding important insights for marketing scholars and practitioners.

Keywords Privacy · Consumer privacy · Decisional privacy · Autonomy · Privacy concerns

Introduction

Today, most websites and apps—including TikTok, Amazon, Netflix, Spotify, and Instagram—personalize users' experiences. By curating, filtering, and providing "recommendations," algorithms predict and restrict consumers' options based on uncorrectable and unverifiable inferences about them (Wachter & Mittelstadt, 2019). Exploiting consumers' cognitive vulnerabilities, the layout and design of these interfaces are also meticulously engineered to steer consumers' decisions by making certain choices appear more appealing than others (Day & Stemler, 2020). In this sense, the introduction of AI has disrupted consumers' decision-making and presented a plethora of new threats to consumer privacy (Davenport et al., 2020; Kopalle et al., 2022; Moradi & Dass, 2022). These threats severely impact consumer

autonomy—consumers' ability to determine their own course of action and engage in deliberate and authentic decision-making (Deci & Ryan, 2000; Ryan & Deci, 2000)—indeed, to a much greater extent than before (Lanzing, 2019). It also profoundly alters the premises for consumer privacy online, creating novel privacy concerns related to interference versus autonomy in decisions. These changes underline the need for more research and discussion of what privacy means for consumers and marketing today (Brough et al., 2023; Krishna, 2020; Zhang & Watson, 2020).

Marketing and information systems scholars have collectively recognized privacy, data collection, and potential secondary use of data among the most essential ethical and social issues related to consumer wellbeing (Hong & Thong, 2013; Murphy et al., 2012; Song et al., 2021), acknowledging consumers' privacy concerns and privacy-preserving behavior as growing obstacles to e-commerce and marketing activities (Bolin, 1998; Luo, 2002; Lwin & Williams, 2003; Martin & Murphy, 2017) and to purchase behavior (Phelps et al., 2001). Previous consumer privacy literature has garnered valuable insight on the antecedents and consequences of consumers' ability to control access

✉ Lena V. Bjørlo
  lena.v.bjorlo@ntnu.no

1   Department of International Business, Norwegian University
    of Science and Technology (NTNU), Larsgaardsvegen 2,
    6009 Aalesund, Norway

to information (Horppu, 2023), examining privacy in marketing altogether (Martin & Murphy, 2017), and in various marketing applications, among them algorithmic recommendations (Banker & Khetani, 2019) and targeted advertising (Bleier et al., 2020). While consumer privacy is a well-established construct based on rigorous scholarship, less attention has been devoted to the conceptual development of the construct in light of increased interference in consumers' decisions (Ferrell, 2017). Echoing the growing literature on the acute threats to consumer autonomy (e.g., André et al., 2018; Wertenbroch et al., 2020), and reflecting contemporary privacy issues, the paper warrants and undertakes a reconceptualization of consumer privacy.

Recognized as a dimension of privacy by adjoining academic disciplines (e.g., psychology, law, and philosophy) and a prerequisite to autonomy, decisional privacy relates to freedom from interference or undue influence in decisions (Lanzing, 2019; Tavani, 2008). Decisional privacy is central to both processes preceding the actual choice (i.e., preference construction and formation of self) and to consumers' ability to make autonomous, well-informed decisions (Gutwirth et al., 2014; Wachter & Mittelstadt, 2019). Given the marketing field's exceptional focus on influence and decision-making, decisional privacy plays a unique role, providing valuable insights about consumers' behavior and decisions as they face more pervasive and unobtrusive interference than before. Extending the notion of decisional privacy and information privacy as complementary dimensions of privacy (Ganley, 2002; Koops et al., 2017; Lanzing, 2019), and emphasizing the function of consumer privacy in terms of protecting autonomy, I thus propose decisional privacy as an explicit dimension of consumer privacy.

While definitions unanimously assert that decisional privacy is premised on the absence of interference, what constitutes interference in consumers' online decision-making remains unclear. While one might argue that the motivation behind any marketing action is to influence consumers (Sunstein, 2015), the "dueness" of this influence varies. Whereas rational persuasion implies open influence, offering reasons for which consumers can deliberate, coercion implies restricting someone's options to only those aligned with the coercer's intentions (Susser et al., 2019b; Wood, 2014). Both persuasion and coercion are overt types of influence; someone who is persuaded or coerced is consciously aware of it. In this sense, overt influence strategies promote conscious decision-making by appealing to higher-order cognitive processes, whereas covert persuasion influences consumers by engaging subconscious, lower-order processes (Felsen et al., 2013; Sunstein, 2015; Susser et al., 2019a). Similarly, manipulation covertly influences choices by exploiting vulnerabilities (Susser et al., 2019a). On this basis, interference and undue influence, here used

interchangeably, encompass covert or otherwise unethical encroachment on consumers' decision-making.

To advance theory on consumer privacy, the paper engages in conceptual development of decisional privacy, developing, and refining theory through means of theory adaptation (Hulland, 2020; Jaakkola, 2020; Vargo & Koskela-Huotari, 2020). To this end, two streams of literature are first reviewed before explaining the function of decisional privacy in light of novel threats to privacy and consumer autonomy. The following section addresses the conceptual development of the construct by specifying its domain, boundaries, and key themes, and it explicates and illustrates the vague notion of interference. This discussion yields the following contributions: (1) definitions of decisional privacy and decisional privacy concerns are proposed, in addition to an integrative definition of consumer privacy; (2) antecedents, mediating variables, and outcomes of decisional privacy are proposed in a nomological network; (3) the implications of decisional privacy for consumers, the marketing discipline, and marketing practitioners are discussed, followed by the proposal of a future research agenda. Altogether, these contributions support the paper's aim to revive the discussion on consumer privacy online.

The conceptual development of decisional privacy is imperative to adequately measure and understand consumer privacy by the relevant dimensions. Faced with more sophisticated interference than ever, the strain on consumers' autonomy underlines the importance of decisional privacy as a consumer right—the right to not be unduly influenced. Extending previous work on consumer privacy in terms of controlling information about consumers' *past* decisions, this broader view of consumer privacy addresses the identity-defining potential of applications of AI to covertly influence consumers, encompassing consumers' *future* decisions and, thus, deliberately developing preferences and weighing alternatives.

Literature review

This section reviews two literature streams that have previously not been integrated in the context of consumer privacy: literature on privacy in marketing and literature on decisional privacy across disciplines. The review of how privacy has been defined, described, and conceptualized in marketing provides a "status quo" of consumer privacy as the domain theory, to which decisional privacy as the method theory aims to contribute (Jaakkola, 2020).

Privacy

Privacy has been studied by a range of disciplines outside of marketing, including psychology, sociology,

anthropology, law (Altman, 1975), education, medicine, and history (Newell, 1995), to name a few. Due to the complexity of privacy and the difficulty of reaching a consensus regarding a definition (Bleier et al., 2020; Goodwin, 1991; Martin & Murphy, 2017; Stewart, 2017), privacy is recognized as a multidimensional concept (Buchanan et al., 2007; Ioannou et al., 2021). In addition to the three main dimensions—personal privacy, information privacy, and decisional privacy (Chen et al., 2008; Harris et al., 2013; Rössler, 2005)—psychological or mental privacy has been suggested as a fourth dimension (Regan, 1995; Tavani, 2008). Most relevant to this current work on consumer privacy in online decision-making are information privacy and decisional privacy, which will be elaborated on.

A literature review of privacy in marketing

To describe how privacy is and has been defined, understood, and conceptualized within the marketing discipline, a systematic literature review was conducted in four rounds. In total, 333 papers were reviewed, of which 148 fulfilled the review criteria by offering a definition, explicit interpretation, explanation, or operationalization of privacy or a privacy-related construct. Appendix A provides a detailed methodology and an overview of marketing journals with the highest volume of papers explaining privacy or a privacy-related construct. The review identified five main privacy constructs: "privacy" in itself, "consumer privacy," "privacy concern," "information privacy," and a range of privacy concepts compiled together as "other privacy concepts," in addition to operationalizations of "privacy concerns" and "other privacy concepts." Table 1 provides an overview of the different privacy constructs' foci in terms of privacy dimensions. Tables summarizing definitions, explanations, and operationalizations by construct are provided in Web Appendices A–G.

Key insights and research gaps

While the appendix comprehensively reviews each construct, this section briefly summarizes key insights from the literature review on privacy in marketing. (1) As can be inferred from Table 1, definitions, explanations, and operationalizations of privacy, consumer privacy, information privacy, privacy concern, and other privacy constructs reflect a predominant focus on information privacy, with personal information, data, and individuals' right or ability to control others' access to this as recurrent themes. (2) The concepts "privacy" and "information privacy" are often employed interchangeably and synonymously. Information privacy is often implicitly equated with privacy for the concepts "privacy concerns" and "consumer privacy," with a few exceptions (e.g., Goodwin, 1991; Jones, 1991). (3) Except for implicit references to "the right to be let alone" and protection from intrusions in some definitions of privacy and consumer privacy, decisional privacy and decisional privacy concerns remain largely unaddressed in an explicit sense. (4) While a single paper *implicitly* proposes decisional privacy concerns, no explicit mentions of "decisional privacy" or "decisional interference" were identified, nor were scales or scale items reflecting decisional privacy concerns. While a few definitions include protection from "interference," this term remains vague and in need of clarification.

Seminal definitions of consumer privacy in marketing literature include "the right to be left alone" (Warren & Brandeis, 1890) and "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967). These definitions correspond with the dimensions of decisional privacy and information privacy, respectively. The marketing discipline has garnered valuable insights about the drivers and consequences of information privacy and information privacy concerns, including how this influences consumers' opinions, attitudes, and behaviors. In addition to research confirming that consumers'

Table 1 Research—Information and decisional privacy

Construct	Web Appendix	Information Privacy[a]	Decisional Privacy (Latent, not explicit)[b]	Total
Privacy	A	40	26	55
Consumer Privacy	B	14	6	15
Information Privacy	C	21	-	21
Privacy Concerns	D	48	1	49
Privacy Concerns—Operationalized	E	33	1	35
Other Privacy Concepts	F	44	1	47
Other Privacy Concept—Operationalized	G	12	-	12
Total		**212**	**35**	**241**

[a]Access, collection, dissemination, handling, and/or use of personal information

[a]Intrusion / External influence / Presence of others / Control of environment / Right to be let alone

privacy concern is growing (Hong et al., 2021), privacy concern has been found to reduce trust and disclosure likelihood (Plangger et al., 2023), increase consumers' skepticism towards, and avoidance of, personalized advertising (Baek & Morimoto, 2012; Strycharz & Segijn, 2022), and negatively influence consumers' attitudes and behavior (Acikgoz et al., 2023; Bright et al., 2021; Plangger et al., 2023). Given the timeliness and importance of consumer privacy, illuminating interference as an aspect of consumer privacy supplements existing knowledge of consumer privacy, aligned with the field's aim to understand how consumers are influenced. Overall, this motivates the introduction and conceptual development of decisional privacy in the context of consumers' online decision-making.

Decisional privacy

Decisional privacy has been defined as "protection against unwanted interference in our decisions" (Essén, 2008, p. 129), "an ability to make and act on one's personal choices without interference from others or the state" (Moskop et al., 2005), or "the right to protection from unwanted access in the sense of unwanted interference or of heteronomy in our decisions or actions" (Rössler, 2005, p. 9). See Table 2 for an overview. Overarchingly, the protection of self-identity and autonomy is considered the ultimate goal of privacy (Altman, 1975). By preventing interference, decisional privacy is valued for enabling autonomy in decision-making and providing fundamental support for identity, self-determination, and self-realization (Cohen, 2013; Grafanaki, 2016; Rössler, 2005). These aspects of personal autonomy represent fundamental consumer rights in a democratic society (Regan, 1995; Rössler, 2005; Susser et al., 2019a). Thus, decisional privacy is considered a prerequisite for individual autonomy (Henkin, 1974; Lanzing, 2019; Margulis, 1977; Moskop et al., 2005; Rössler, 2005).

The right to decisional privacy originated in law, centered on individuals' right to avoid interference in their private lives by the government or state (Fairfield & Reynolds, 2022). Decisional privacy has since been widely adopted as a dimension of privacy across disciplines including law (van der Sloot, 2017), philosophy (Lanzing, 2019; Rössler, 2005), medicine (Moskop et al., 2005), behavioral and social sciences (Essén, 2008; Margulis, 2003), psychology (Kapsner & Sandfuchs, 2015), and ethics (Floridi, 2006). The initial focus on protection against government interference has since evolved to encompass decisional privacy in choice contexts related to bodily autonomy (Allen, 1988), contraceptives and procreation (Cohen, 2009; Tavani, 2008), and political expression (Margulis, 2003). Over the years, applications of decisional privacy have also expanded from governmental interference to include other external actors (van der Sloot, 2017), as well as from

decisions related to reproductive freedom to include any personal choice (Ganley, 2002; Moskop et al., 2005).

Today, corporations are recognized as a pronounced threat to decisional privacy, in some parts of the world interfering even more profoundly in individuals' decision-making than governments, through corporations' use of covert algorithms (Fairfield & Reynolds, 2022; Zuboff, 2019). Consequently, decisional privacy has more recently been applied to contexts related to novel technologies (Rössler, 2005; van der Sloot, 2017), nudging (Kapsner & Sandfuchs, 2015; Lanzing, 2019), AI, and algorithms (Day & Stemler, 2020; Fairfield & Reynolds, 2022). Aligned with this recent work, I argue that decisional privacy is of great relevance to the context of consumers' online decision-making, where interference is mainly exerted on consumers by marketers, firms, and platforms, to steer their decisions.

Despite the recognition of algorithms' potential to unduly influence consumers' decisions and to erode their autonomy, decisional privacy has not been adequately theorized in the context of consumers' interactions with algorithmic decision aids (Day & Stemler, 2020). This paper thus aims to conceptualize decisional privacy in the context of consumers' online decision-making. Briefly, I propose that decisional privacy encompasses the absence of undue influence or interference in both stages related to and leading up to decision-making, including preference construction. Given the ambiguity surrounding interference and undue influence, I will later elaborate. In short, undue influence covertly targets consumers' subconscious decision-making and thwarts their ability to make deliberate and well-informed decisions, contrasting with overt persuasion, which enables deliberation in decision-making.

How decisional privacy supplements information privacy

The complementarity of decisional privacy and information privacy (Ganley, 2002; Koops et al., 2017; Lanzing, 2019) suggests that decisional privacy's focus on interference in consumer decision-making supplements information privacy's focus on consumers' right or ability to control access, collection, and analysis of their information (Lanzing, 2019; Martin & Murphy, 2017; Massara et al., 2021). Invasion of information privacy thus occurs when consumers are unable to control the flow of their personal information or are subjected to unauthorized or improper information collection, disclosure, or use (Wang et al., 1998). In light of recent technological development, decisional privacy can hereby offer new insights regarding the invasion of internal decision-making and individual judgment (Day & Stemler, 2020; Gilbert, 2007; Mulligan et al., 2016).

In this sense, consumers' information privacy remains vital, not only for the sheer purpose of consumers' ability to

Table 2 Definitions of decisional privacy

Source	Definition/explanation	Context/domain/examples provided
Allen (1988)	Decisional privacy concerns a person's decisions and choices about his private actions. Decisional privacy is an aspect of liberty: freedom to choose without unjustified coercion or constraint	Self-determination; Bodily integrity
Solove (2000)	The extent to which the state can interfere with the decisions one makes with regard to one's body and family	Decisions about one's body and family: Contraception; Reproduction; Child-rearing
Ganley (2002)	"Decisional privacy" is often used in connection with government interference, for example in areas such as reproductive freedom. Here, it is employed in a wider context to implicate the actions of external agents designed to influence any individual choice	Actions of external agents designed to influence any individual choice; Digital rights management systems
Margulis (2003)	The freedom to decide and to act in public or private as one deems appropriate, without government interference (Allen, 1988; Etzioni, 1999)	Political expression and criticism; Political choice; Family, religion, self-definition
Rössler (2005)	The right to protection from unwanted access in the sense of unwanted interference or of heteronomy in our decisions or actions	New information technology; Private decisions; Bodily autonomy, i.e., abortion
Moskop et al. (2005)	An ability to make and act on one's personal choices without interference from others or the state	Medical decisions, i.e., contraception, abortion; Life-sustaining medical treatment
Floridi (2006)	"The freedom from interference in one's own choices and decisions" and "The right to determine one's own course of actions."	Education; Health care; Marriage; Sexual options; Reproductive alternatives
Tavani (2008)	Freedom from interference in one's personal choices, plans, and decisions	Abortion; Contraception
Essén (2008)	Protection against unwanted interference in our decisions	Electronic care surveillance, monitoring devices; Older people
Borenstein (2008)	Decisional privacy refers to "freedom from governmental or other outside interference to make decisions."	Technology. Both government and private companies can violate individuals' privacy
Cohen (2009)	Decisional privacy: freedom from undue regulation or control	Nudging, paternalism; Personal decisions, i.e., marriage, divorce, sexual relations, sexual identity, expression, abortion procreation, etc
Kesan et al. (2013)	"The right of individuals to make decisions free of government intervention" and "Ability to make choices free from undue interference."	Views interference as broader than just government intervention: tests whether telling intrusive parties to "mind their own business" is viewed as a right to privacy
Kapsner and Sandfuchs (2015)	We are talking about what Rössler refers to as decisional privacy whenever we say, "This is my private decision." We do not necessarily mean that no one should know about our decision, but that no one except for ourselves should have a say in it	Nudging; Libertarian paternalism
Skinner-Thompson (2015)	"Decisional privacy" refers to the right recognized in cases such as Griswold v. Connecticut (1965), wherein the Supreme Court acknowledged that individuals have the ability to control certain fundamental decisions	Individual autonomy in legal cases against the government
Mulligan et al. (2016)	Decisional privacy protects the mental space necessary for individual judgment	Changing technological and social conditions., i.e., machine learning and data analytics
Sarikakis and Winter (2017)	Decisional privacy refers to the decisions and choices of a person with regard to their personal actions	Social media; Privacy policies
Koops et al. (2017)	Decisional privacy protects the autonomy of persons to make decisions about their body or other aspects of their private life. Decisional privacy can be seen as the positive version of intellectual privacy: the freedom to exercise one's mind	*US:* Personal decisions, i.e., related to sexuality and child-rearing. *Europe:* Personal development, personal autonomy, bodily autonomy, self-determination, and ability to conduct one's life as desired; procreation

Table 2 (continued)

Source	Definition/explanation	Context/domain/examples provided
van der Sloot (2017)	"The right to determine one's own course of actions" (Floridi, 2006) and "The freedom to decide and to act in public or private as one deems appropriate" (Margulis, 2003)	Reproductive rights; Bodily integrity; Regulation of current technologies, Data-driven decisions, i.e., profiling; development of identity
Loh (2018)	Decisional privacy "serves to secure the scope for a subject to make decisions and take action in all his social relations" (Rössler, 2005)	Choices from wardrobe to occupation, significant other, family planning, etc
Lanzing (2019)	Decisional privacy is broadly defined as the right against unwanted access such as unwanted interference in our decisions and actions (Allen, 1988; Rössler, 2005)	Nudging and hypernudging
Day and Stemler (2020)	"Ability to make decisions free of coercion" and "The invasion of internal decision-making (Gilbert, 2007)."	Dark patterns, algorithms, platforms, competition
Dimopoulos (2022)	Decisional privacy protects an individual's ability to make decisions which contribute to defining their identity and sense of self, free from the unwarranted interference of other individuals or the state (DeCew, 1997; Rössler, 2005). Decisional privacy is premised on the value of freedom from coercive interference with decision-making affecting intimate and personal affairs	Children's rights; Important decisions; Personal choices; Decisions
Fairfield and Reynolds (2022)	Solove (2006) characterizes decisional privacy as protection from government interference in "zones of privacy." Decisional privacy protects this process of moral development by protecting decision-making. Decisional privacy cases protect people's ability to make their own decisions and rationalize them, rather than another entity, traditionally the government, making decisions for them	Seeks to revive and translate concerns about decisions, previously confined to reproduction, into modern conversations about corporate-driven algorithmic decisions. Algorithms and corporations as entities, not only governments

Table 3 Information privacy and decisional privacy

Privacy dimension	Focus	Function	Direction
Information privacy	Consumers' ability or right to control access to, and flow of, personal information	Prevent undue access, collection, and dissemination of consumers' information	Inside out
Decisional privacy	Consumers' ability or right to develop authentic preferences, make autonomous decisions, and not be exposed to interference	Prevent undue influence from interfering with consumers' decision-making	Outside in

limit what others know about their previous preferences and behaviors, but also to protect their future preferences and behaviors and identity-construction through decisional privacy. Table 3 delineates and contrasts the dimensions' foci and functions, clarifying how the two supplement each other.

Based on the complementary functions of information privacy and decisional privacy in the context of consumers' online decision-making, I propose the metaphor of a two-directional shield (Fig. 1). While information privacy protects from the inside out by preventing access, dissemination, and use of consumers' information, decisional privacy shields from the outside in by preventing undue influence from interfering with consumers' preference construction and decision-making. This two-directional interpretation of privacy as "selective control of access to the self" (Altman, 1975) underlines that consumer privacy reflects both information privacy and decisional privacy (Lanzing, 2019; Tavani, 2008).

This extends the focus of consumer privacy from the ability to control personal information to the consideration of the presence of undue influence and interference in decision-making. Due to the increased possibilities for consumers to be unduly influenced without awareness of this and the growing concern for AI and algorithms crowding out human decision-making, decisional privacy is more relevant and important than ever for protecting consumer autonomy (Fairfield & Reynolds, 2022). Hence, to explicate decisional privacy as a significant aspect of consumer privacy, I begin by explaining its function in terms of protecting autonomy.

Decisional privacy protects autonomy

Autonomy, consumer autonomy, and decisional privacy

In the broadest sense, autonomy relates to freedom of choice and individuals' ability to carry out their lives according to their own authentic goals and desires by making decisions that reflect their true preferences (Deci et al., 1999; Zwebner & Schrift, 2020). Autonomy is recognized as fundamental to innate human motivations (Zwebner & Schrift, 2020)

and to the development of self-identity (Altman, 1975), as well as a central value of democratic society (Grafanaki, 2016). This value provides a foundation for personality, from which character, morality, and ethics emanate (André et al., 2018; Frankfurt, 1971). Moreover, autonomous actions are endorsed by the self (Calvo et al., 2020) and associated with increased persistence, performance, and psychological well-being (Calvo et al., 2020; Ryan & Deci, 2017).

Within consumer choice contexts, autonomy is viewed as "consumers' ability to make and enact decisions on their own, free from external influences imposed by other agents" (Wertenbroch et al., 2020, p. 430). Consumer autonomy thus relates to consumers' ability to make well-informed and independent decisions without pressure or manipulation that undermines their ability for rational deliberation (Calvo et al., 2020; Rössler, 2018). Importantly, the ability to choose freely and in a manner that reflects authentic preferences requires the absence of external influence (Ryan
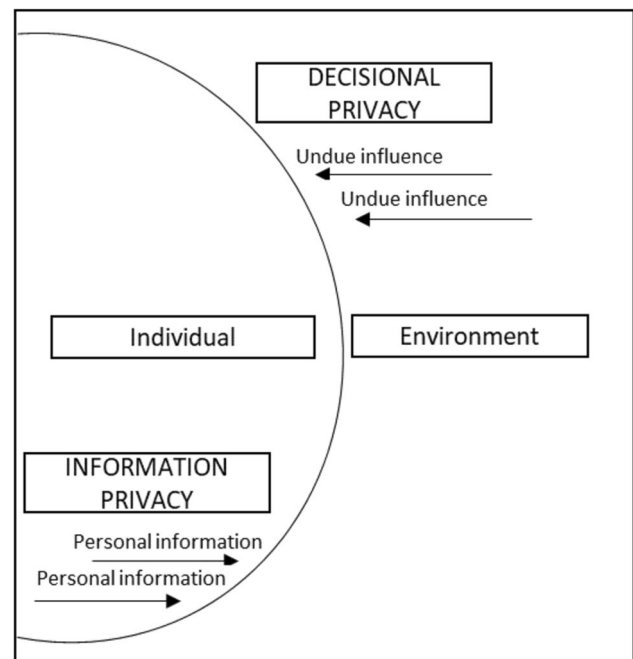

Fig. 1 Consumer privacy as a two-directional shield

& Deci, 2006; Zwebner & Schrift, 2020), both in the pre-choice stage, which is central to consumers' preference- and identity construction, and the stage in which the choice is actually made (Grafanaki, 2016).

As the ultimate outcome of privacy, autonomy is recognized as the primary reason why society values privacy (Henkin, 1974; Margulis, 1977; Mulligan et al., 2020; Rössler, 2005). Privacy promotes free, individual, and authentic decisions, enabling the development of individuality and choice consciousness (Cohen, 2000; Grafanaki, 2016; Margulis, 1974). Decisional privacy protects individuals' ability to "make decisions which contribute to defining their identity and sense of self, free from the unwarranted interference of other individuals or the state" (DeCew, 1997; Dimopoulos, 2022, p. 428; Rössler, 2005). Since the very pillars of democracy rest on individuals' freedom to decide and self-determination (Rössler, 2005), violations of decisional privacy also threaten democracy collectively.

The ability to develop and weigh preferences is necessary for consumers' formation of opinions and identity-construction (Rössler, 2005). Hence, consumer privacy should encompass both control over personal information (information privacy), as well as the protection of autonomy and identity construction (decisional privacy) (Strycharz et al., 2019). As previously mentioned, definitions of decisional privacy (see Table 2) reflect protection from interference and undesired access by others, including both physical access and access in terms of intrusions in decision-making (Rössler, 2018). However, despite these strong theoretical arguments, the empirical relationship between privacy and autonomy (Margulis, 1974; Rössler, 2018) remains understudied, especially in the context of consumer privacy.

AI-based technologies: Novel threats to decisional privacy and consumer autonomy

The use of machine learning, AI, algorithm-based personalization, and neuroscience has profound implications for marketing practice and, consequently, for consumer autonomy and privacy (André et al., 2018). These systems' use of big data to predict consumer behavior implies that consumers can be outsmarted and manipulated (Contissa et al., 2018; O'Neil, 2016), namely by the hidden practices of behavioral targeting (Nill & Aalberts, 2014), personalized advertising, and nudging (Lanzing, 2019; Tavani, 2008). Today, more examples of these practices are being brought to public attention, for example the Cambridge Analytica scandal, which serves as a disturbing real-world case of voter manipulation online (Wertenbroch et al., 2020).

Algorithms predict consumers' preferences, characteristics, habits, and personality traits based on data (Grafanaki, 2016; Tene & Polonetsky, 2013). Psychological targeting refers to "extracting people's psychological profiles from their digital footprints (e.g., their Facebook Likes, Tweets or credit card records) to influence their attitudes, emotions or behaviors through psychologically informed interventions at scale" (Matz et al., 2020, p. 116). Consequently, these inferences determine which options consumers are given and implicitly form the foundation from which consumers' future choices can be made, without conscious deliberation by consumers. This relates to the terms "algorithmic feedback loops" and "algorithmic determinism," which problematize the idea of algorithms producing the outcome they are designed to predict (Day & Stemler, 2020; Grafanaki, 2016).

As consumers choose among pre-selected options, the algorithm's predictions become self-fulfilling. Subordinating consumers' authentic preferences to the preferences of the algorithms and their engineers in this sense threatens consumer autonomy, preventing active decision-making and creating new opportunities for discriminatory, biased, and privacy-invasive profiling. Moreover, while predictive algorithms claim to anticipate consumers' preferences, basing inferences only on historic data may limit consumers' ability to evolve or grow since preferences are subject to change (André et al., 2018; Bjørlo et al., 2021).

The use of untraditional data sources by algorithms to generate unpredictable and unverifiable inferences about consumers can also threaten individuals' freedom of expression and the right to privacy and identity (Hildebrandt & Gutwirth, 2007; Wachter & Mittelstadt, 2019). Determining how consumers are seen and evaluated by third parties, inferences can threaten individuals' self-determination, autonomy, and even identity by hiddenly shaping their behavior and preferences (Gutwirth et al., 2014; Wachter & Mittelstadt, 2019; Zarsky, 2002). Recently, CNN disclosed that Uber had developed technology to infer users' intoxication level from the angle users hold their smartphone, their walking style, and whether they were typing "clumsily" (Day & Stemler, 2020). While the purpose of these inferences has not been disclosed, this example illustrates that the information itself may not necessarily be what is sensitive or cause for concern, but rather the inferences generated from it (Wachter & Mittelstadt, 2019) and how these inferences may be applied to manipulate users.

A particularly worrisome yet common application of AI and algorithms are "dark patterns," which exploit consumers' cognitive biases (Narayanan et al., 2020), leading them to make decisions they might not otherwise make, and which are not in their best interests. Dark patterns rely on deception, covert influence, manipulation, and coercion to modify users' decision space or manipulate the information flow (Mathur et al., 2021; Narayanan et al., 2020). Distinguishing consumers' decisions as deliberative (System II) or non-deliberative (System I), System II decisions involve active decision-making based on slower, more methodical choices, whereas System I decisions are characterized as semi-conscious, automatic, or hurried (Becher & Feldman,

2016; Kahneman, 2003). Dark patterns strategically exploit System I decisions by targeting known or inferred cognitive vulnerabilities, making certain options subtly appear more desirable or accessible than others (Day & Stemler, 2020). Since the influence mechanisms remain hidden from users (Mathur et al., 2021), this practice covertly steers consumers' behavior.

Despite the apparently unethical nature of the practice, previous research has identified that over 95% of well-known Android apps employ dark patterns (Di Geronimo et al., 2020). To manipulate consumers' choices, dark patterns employ subtle design elements, including placement, color, layout, and size of clickable boxes (Day & Stemler, 2020). Other examples include deceptive countdown-timers of an offer expiring when in fact there is no time limit on the offer (Narayanan et al., 2020), false statements of product scarcity ("Only 3 left! Order before it's too late") or ("In high demand. Book now!"), and false indicators of items' popularity to induce consumers' feelings of scarcity to make them "act now" (Bergdahl, 2020). Adding hidden costs, disguised as "taxes and fees," at the last step of the purchase process represents another tactic for steering consumers' decisions, commonly applied in the hotel and travel industry. In retail, Amazon frequently employs dark patterns, for instance automatically ticking subscription boxes and setting the more expensive payment option as the default choice, greying out alternative payment options (Brignull et al., 2023).

Table 4 illustrates how marketing practices facilitate and constitute decisional interference. In addition to the real-world examples presented in this table, the Internet is also ripe with examples of firms' and platforms' applications of dark patterns, as evidenced by "Darkpatternstipline. org" (Stanford Digital Civil Society Lab, n.d.) or "Deceptive.design" (Brignull et al., 2023), where users share their encounters with the use of dark patterns to spread awareness and warn others, compiling and shaming the worst offenders in a "Hall of Shame."

Since social media platforms profit from users' attention as targets for advertising, they aim to keep users on their platform for as long as possible. To achieve this, the strategic release of dopamine is frequently incorporated into the platforms' design and interface (Day & Stemler, 2020), for example luring users in through attention-grabbing push notifications. Similarly, Instagram prevents users from seeing the clock in the app, making them lose track of time and spend more time than intended. As an example of how dopamine release keeps users coming back, social media app Snapchat's popular "streaks" feature, designed to create a rush of dopamine by rewarding daily use, has proven a highly addictive feature. Similarly, the language-learning app Duolingo employs dopamine-rewarding features and principles of gamification to encourage subscription to premium services, in-app purchases, and daily use of the app, inducing cognitive resistance towards discontinuing use.

Regarding the "application of game elements to nongame contexts" (i.e., points, badges, and levels), gamification may promote addictive behavior by stimulating the brain's reward system (Hughes & Lacy, 2016, p. 311).

Similar to dark patterns, strategic dopamine release and gamification subconsciously target consumers' System I responses, exploiting principles of intrinsic reinforcement and desire for pleasure (Hughes & Lacy, 2016). Together, these examples illustrate how seemingly harmless personal information and psychological mechanisms may unexpectedly and covertly influence consumers' attitudes and behaviors, without consumers' awareness. The unobtrusive, covert, and opaque nature of these technologies underlines their manipulative potential to subtly shape consumers' preferences and steer choices (Hausman & Welch, 2010; Lanzing, 2019; Wilkinson, 2013). Obfuscating consumers' ability to engage in rational deliberation and making their actions feel organic and self-chosen (Fairfield & Reynolds, 2022; Willis, 2017), the seamless nature of algorithms threatens consumer autonomy (Grafanaki, 2016).

The need for conceptual development of decisional privacy

The pervasive influence of AI and algorithms has spurred debates on the role technology has assumed in consumer decision-making, challenging consumers' decisional privacy and autonomy to an unprecedented extent (Lanzing, 2019). While privacy has often been equated with "information privacy" in marketing literature, and while this conflation has directed much of the research attention, it does not imply that marketing literature has never addressed any features of decisional privacy. Indeed, the literature review identified mentions of *intrusion* and *interference* in relation to consumer privacy (e.g., Goodwin, 1991; Peltier et al., 2009) and privacy (e.g., Massara et al., 2021; Ottlewski et al., 2023; Phelps et al., 2000; Warren & Brandeis, 1890). Nevertheless, interference or intrusion—and decisional privacy—remains mostly unaddressed as an explicit aspect of consumer privacy, apart from a few influential works (i.e., Foxman & Kilcoyne, 1993; Goodwin, 1991; Jones, 1991; Milne, 2000; Petty, 2000).

Overall, consumer privacy has mainly been conceptualized as pertaining to the protection of information about consumers' previous decisions (i.e., purchases or browsing history). Given novel technologies' ability to covertly interfere with the construction of consumers' preferences and identities and to steer their *future* choices through inferences based on previous behavior, these future-oriented aspects should be included in the notion of consumer privacy. Moreover, given the role of influence in marketing and the field's longstanding commitment to understanding consumers' opinions, attitudes, and behavior when faced with influence, decisional privacy should

fo

—

—

Table 4 Examples of interference in marketing practices

Marketing practices	How the practice represents interference and threatens decisional privacy	Examples
Nudging (e.g., Kapsner & Sandfuchs, 2015; Lanzing, 2019)	Altering consumers' choice architecture, using "defaults" to steer opinions and actions Manipulation: intentionally and hiddenly steering people's choices, based on personalization Libertarian paternalism: nudging people toward achieving desired outcomes identified by experts	Apps nudge consumers to perform actions, i.e., using personalized notifications, default options. Fashion retailer Zalando sends app notifications based on products viewed
Psychological targeting (e.g., Matz et al., 2020)	Influence attitudes, emotions, or behavior through psychologically informed interventions at scale Tailoring interventions to individuals' psychological states and traits, and exploiting insight about their vulnerabilities, without their knowledge Psychologically tailored interventions influence attitudes, emotions, or behavior by targeting fundamental psychological motivations from profiling: assessment of psychological traits and states from digital footprints	Cambridge Analytica scandal: without being aware of it, voters were exposed to personalized influence, based on psychological profiling Teenagers targeted with Facebook advertising at emotional states when they are feeling "at their worst"
Personalized advertising/ targeting (e.g., Nill & Aalberts, 2014)	Tracking of a consumer's online activities to develop a behavioral profile of them, to which advertising can be targeted or personalized, often without their awareness Combination of data sources applied to other purposes than their original purposes	Hiddenly influencing the decision to vote by a targeted ad. Curating content based on a depressed mood, without consumers' awareness
Algorithmic recommendations (e.g., André et al., 2018; Fairfield & Reynolds, 2022; Mulligan et al., 2020)	Algorithms curate, filter, and select the specific content or products which consumers can see, as well as their order Overreliance on past behavior encourages repetition of past behavioral patterns, makes evolving less likely Algorithmic feedback loop/determinism: algorithms' output becomes the input for new decisions	Encouraging consumers to repeat choices deprives them of the ability to evolve. I.e., recommending unhealthy food to someone who wants to eat healthier, based on previous choices
Native advertising (e.g., Campbell & Marks, 2015)	Native advertising blends into the environment and unobtrusively exposes consumers to hidden influence Commercial content or advertising is disguised as recommendations, news, or organic content Consumers are less aware of native ads and may be deceived or tricked into false beliefs about the ad, including the source behind it, which may be concealed	Advertorials: Non-disruptive ads created to emulate surrounding content in a naturalistic environment. Consumers thus do not necessarily perceive advertorials as advertising, but as content
Dark patterns (Castmo & Persson, 2018; Day & Stemler, 2020; Hughes & Lacy, 2016; Mathur et al., 2021)	Subtle design choices in digital interfaces intended to elicit certain behaviors from users, leading them to make decisions they might not otherwise, e.g., disclosing data Exploits cognitive vulnerabilities to covertly guide individuals' decisions, barring well-informed decisions Dark patterns prey on cognitive heuristics, i.e., confirmation bias, to effectively manipulate individuals Strategic release of dopamine influences consumers to spend more time and attention than intended Dopamine release and gamification principles exploit the brain's reward system, triggering addictive behavior	Deceptive countdown timer on offers; Confirm shaming: shaming users who do not conform; Trick questions; Roach motels: easy to enter website, hard to exit; Tunnelling: moving users along the purchase process; Snapchat streaks Gamification in Duolingo: points, awards, badges, levels, and leaderboards

be included as an explicit dimension of consumer privacy. Hence, implicit mentions of interference must be clarified, explicated, and adapted to the context of consumer decision-making. Furthermore, to understand how decisional privacy complements information privacy and to enable empirical research on decisional privacy concerns, the proxy used to study privacy, conceptualization of this is needed. To this end, the following section engages in the conceptual development of decisional privacy.

Conceptual development of decisional privacy

This section aims to generate a more profound understanding of decisional privacy and to guide future scale development by (1) specifying the construct domain and its key themes; (2) explicating and illustrating the vague terms "interference" and "undue influence" (3) offering definitions for decisional privacy and decisional privacy concerns, and integrative definitions of consumer privacy and privacy concerns; and (4) proposing theoretically relevant constructs in a nomological network, examining antecedents and consequences of decisional privacy.

Construct development

The paper addresses the first step of the scale development process: clearly defining the construct and its domain (Churchill, 1979; DeVellis, 1991; Netemeyer et al., 2003). This step includes clarifying its boundaries with other constructs, defining the construct's conceptual domain, and identifying and outlining the "conceptual themes" or "key properties" of the construct (Jaccard & Jacoby, 2019; MacKenzie et al., 2011). While the paper does not aim to fully develop or validate a scale for decisional privacy, some ideas for scale development are proposed, founded on the conceptual analysis of previous definitions.

Specifying the construct domain and identifying key themes

Previous definitions of decisional privacy reflect a consistent focus on individuals' ability to make self-determined decisions free from interference (see Table 2). Three conceptual themes emerged from these definitions: (1) interference; (2) self-determination; and a focus on (3) individuals' choices, decisions, and actions. The first theme, *interference,* is mentioned in reference to the government (Dimopoulos, 2022; Ganley, 2002; Margulis, 2003), the state (Moskop et al., 2005), other individuals (Dimopoulos, 2022), or corporations (Fairfield & Reynolds, 2022). Some definitions simply contend that decisional privacy protects against "unwanted

interference… in decisions" (Rössler, 2005). Due to a lack of clarity regarding what constitutes interference in the context of online decision-making, this matter is elaborated below.

The second theme refers to *self-determination*, described as "individuals' ability to determine their course of action" (van der Sloot, 2017), "define their identity and sense of self" (Dimopoulos, 2022), and "make their own decisions and rationalize them" (Fairfield & Reynolds, 2022). Moreover, the function of decisional privacy is described as protecting "the autonomy of persons to make decisions" (Koops et al., 2017) and against "heteronomy in decisions" (Rössler, 2005). Contrasting with the notion of self-determination and autonomy, heteronomy refers to actions influenced by external actors, or ruled or governed by another party—something outside the self (Ryan & Deci, 2006). Third, definitions specify that what should be self-determined and free from interference are *individuals' decisions, choices, and actions*. These are mostly conceptualized, broadly, as "any individual choice" (Ganley, 2002), "personal choices" (Moskop et al., 2005), or the "freedom from interference in one's own choices and decisions" (Tavani, 2008). Out of 23 definitions, 21 explicate a focus on choices, decisions, or actions, often a combination of these.

What characterizes interference and undue influence?

Given the vagueness of "interference," the most common theme in definitions of decisional privacy, this concept requires clarification in order to conceptualize decisional privacy. Generally, interference implies (1) covert or otherwise undue influence and (2) access by (un)known actors to one's own actions and choices, enabling external actors to alter or steer these (Lanzing, 2019). In this sense, interference limits consumers' ability to make informed decisions and impairs consumers' rational choice (Hacker, 2021).

Founded in previous literature's conceptions of interference and undue influence, within the context of consumers' online decision-making, I propose that influence should be considered *undue* when it is (1) not only persuasive but coercive or manipulative (Bakir & McStay, 2023; Niker et al., 2021) and (2) characterized as covert, hidden, or subtle rather than overt, open, and detectible (Sunstein, 2015; Susser et al., 2019a). Moreover, undue influence (3) subverts consumers' rational decision-making process by targeting subconscious processes rather than engaging their deliberative processes and capacities (Day & Stemler, 2020). This implies that undue influence includes (4) attempts to steer consumers' behavior, for instance by exploiting cognitive vulnerabilities or by subsuming the goals or preferences of consumers' authentic decision-making to the goals or preferences of the influencer. The notion of undue influence or hidden persuasion is hardly anything new in marketing,

including the use of subliminal techniques (see, for example, Packard, 1957). However, the advanced ability of current digital marketing to facilitate and disperse undue influence in a highly individualized and data-driven manner that circumvents consumers' perceptions and awareness distinguishes undue influence in online decision-making from previous conceptions of such influence.

Decisional privacy and undue influence, offline and online

To aid in conceptualizing and emphasizing the distinct qualities of decisional privacy online, a comparison with undue influence *offline* is useful. Upon entering a physical store, the product assortment and store layout are predetermined by a store manager. While this arrangement evidently limits which products a consumer can choose from, the store layout, the options, and the order in which these are presented are the same for every customer, regardless of the time of day, their income, or time previously spent looking for the product. While the perception of the store differs between consumers, consumers' decision architecture remains unchanged.

In-store, a consumer may encounter a salesperson who seeks to influence their decisions based on self-serving interests that conflict with the consumer's interests, for instance having incentives to promote certain products. Unlike in an online environment, the salesperson cannot infer which stores this consumer has previously visited or know their vulnerabilities by simply glancing at them. While the salesperson can adapt their communication based on assumptions about consumers, these assumptions are founded on rudimental heuristics and personal experience rather than actual data patterns. Moreover, a seller's use of manipulative tactics is confined to more overt persuasion, compared to covert online manipulation tactics fueled by pervasive data insights. Consumers may also encounter physical persuasion in-store (i.e., promotional displays) appealing to their impulses by placing tempting items in waiting areas, or items aimed at children on shelves within their reach. While these practices may be exploitative or unfair, as they do not coerce or influence consumers hiddenly, I argue that this influence is not *undue.*

While the paper's objective is not to evaluate the appropriateness or "dueness" of influence offline, it aims to offer conceptual insights from this comparison. Persuasion offline is usually more overt and likely to engage consumers' deliberate decision-making through consumers' awareness and perceptions, and possibilities to manipulate consumers' decision architectures in-store are limited. In contrast, consumers do not even need to enter a store for influence to occur online—it can occur anywhere, anytime, and the influence is tailored and fragmented across multiple platforms. Since the covertness and opaqueness of technology make the influence less obtrusive and perceptible, interference is a greater concern for consumers online than offline. I propose that this is driven by

overtness and transparency and mediated by perceptions and privacy awareness, and I will return to elaborate on this later.

Boundaries to decisional privacy

The paper does not propose that decisional privacy as a right should be unlimited. There are, indeed, several areas where "interfering" with individuals' decisions is considered necessary to maintain law and order in society and to protect individuals (Kugler, 2014). Legislation is also required to regulate domains that pose societal risks (e.g., for alcohol, firearms, and illegal substances). Limiting individuals' freedom to act as they please is sometimes considered appropriate and necessary to protect individuals and society. Indeed, individuals' right to autonomy must be balanced against society's "greater good" (Lanzing, 2019; Mill, 2006). The paper does not argue against this balance. Rather, it upholds decisional privacy as protection from undue influence in *consumers'* decisions online, including purchase decisions, political influence, and news and content curation. While the effects of consumer manipulation are likely less visible than unregulated sales of alcohol or firearms, decisional privacy also protects consumers from the severe societal risk of de-democratizing.

The responsibility of consumers who disclose their information should also be mentioned as a boundary. Although this boundary relates mostly to the ability to control access to information and the dimension of information privacy, it also pertains to decisional privacy. While consumers cannot be released from the responsibility to read privacy policies, this task is recognized as cumbersome, made particularly difficult for consumers to understand and process (Waldman, 2020). In this regard, dark patterns and defaults are employed to steer consumers' decisions, as well as to accept privacy statements or disclose data (Gray et al., 2021) by making "accept" the easiest, most convenient, or default option. There are also boundaries with regard to consumers' desire for decisional privacy, implying that consumers may willingly forego decisional privacy for more personalized, enjoyable, and convenient online experiences that facilitate their decision-making. Lastly, privacy concerns are recognized as country-specific (Bellman et al., 2004), implying that the culture and nationality of consumers may also influence individuals' desire and preference for decisional privacy.

Defining decisional privacy in the context of consumers' online decision-making

Proposing a definition of decisional privacy

Based on the preceding discussions, the following definition of decisional privacy is proposed: "The absence of undue influence or interference in stages related to, and leading up to decision-making, including preference construction." For a discipline that studies influence, it appears unrealistic and nonsensical to

abolish influence altogether, and I contend that consumers can be exposed to influence and still have autonomy. However, this implies that their ability to engage in conscious thought processes is not compromised, as deliberation is necessary to their ability to choose and act according to authentic goals and preferences. In other words, the influence must be overt and transparent.

Proposing an integrative definition of consumer privacy

To integrate decisional privacy and information privacy, the following definition of consumer privacy is proposed: "Consumers' right or ability to control 1) access, acquisition, and use of personal information and 2) decisional interference subjected throughout all stages related to preference-construction and decision-making." The notion of control implies that consumers can regulate the extent to which they desire to exercise their right to privacy, both by divulging information and by being exposed to influence. There are several situations in which consumers may desire to share information or allow influence in exchange for perceived benefits, such as decision support. This underlines the importance of voluntary actions: if a consumer can exercise selective control, their privacy is argued to be intact.

Proposing an integrative definition of privacy concern

Since decisional privacy concerns supplement consumers' information privacy concerns, this should also be reflected in the conceptualization of privacy concern, the proxy employed to measure privacy. While information privacy concerns focus on consumers' concerns related to the collection of personal information, decisional privacy concerns reflect worries about external actors interfering with their decision-making. On this basis, "decisional privacy concerns" refer to "consumers' interest or worry towards being subjected to interference or undue influence by external actors, throughout all stages related to preference-construction and decision-making." Building on these arguments, an integrative definition of consumer privacy concerns is proposed for informational and decisional dimensions of privacy: "Consumers' interests and worries about being able to control the access, collection, and use of their personal information, as well as those about being subjected to interference by external actors throughout all stages related to preference-construction and decision-making."

Nomological network

How decisional privacy relates to other constructs is here proposed in a nomological network see Fig. 2 (Roest & Pieters, 1997). So far, the paper has focused on the consequences of decisional privacy as promoting consumer autonomy, self-endorsed decisions, and trust on an individual scale and democracy, individualism, and preventing "surveillance society" on a collective scale (Foucault, 1991; Zuboff, 2019). With regards to antecedents, previous definitions propose that decisional privacy is promoted by the absence of interference (Essén, 2008; Floridi, 2006; Tavani, 2008). Extending this notion, I propose that decisional privacy in consumers' online decision-making is driven by transparency and overtness (André et al., 2018; Lanzing, 2019).

Transparency refers to "the possibility of accessing information, intentions, or behaviors that have been intentionally revealed through a process of disclosure" (Turilli & Floridi, 2009, p. 105), promoting consumer autonomy by enabling informed and deliberate considerations (Sunstein, 2015), and reducing possibilities for manipulation. *Overtness* relates to the employment of open and recognizable persuasion strategies, activating consumers' higher-order cognitive processes, contrary to covert persuasion strategies, which aim to influence consumers through subconscious, lower-order processes (Felsen et al., 2013).

The mediating roles of decisional privacy awareness and perception

Privacy awareness is described as users' understanding, knowledge, and perception of an organization's privacy practices and policies, including the collection, storage, and use of their personal information, as well as general privacy issues (i.e., Cheung et al., 2015; Malhotra et al., 2004). A significant addition proposed here is the decisional aspect of privacy awareness, referring to "understanding, knowledge, and perception of unwanted external interference when making decisions." Awareness depends on consumers' knowledge related to decisional privacy practices and the aforementioned factors (i.e., the overtness and transparency of the influence). While decisional privacy awareness does not reduce the *presence* of interference, it may reduce its *impact* and ability to interfere in consumers' decisions-making. By alerting consumers to potential interference, decisional privacy awareness enhances consumers' abilities to make conscious decisions. I thus propose that decisional privacy awareness and perception mediate the relationship between overtness or transparency of the influence and decisional privacy and decisional privacy concern.

The relationship between decisional privacy and information privacy

Dimensions of information privacy and decisional privacy are recognized as complementary by other scholarly disciplines (Ganley, 2002; Koops et al., 2017; Lanzing, 2019), for example law and philosophy. Extending this notion to consumer privacy and marketing, I propose that together,
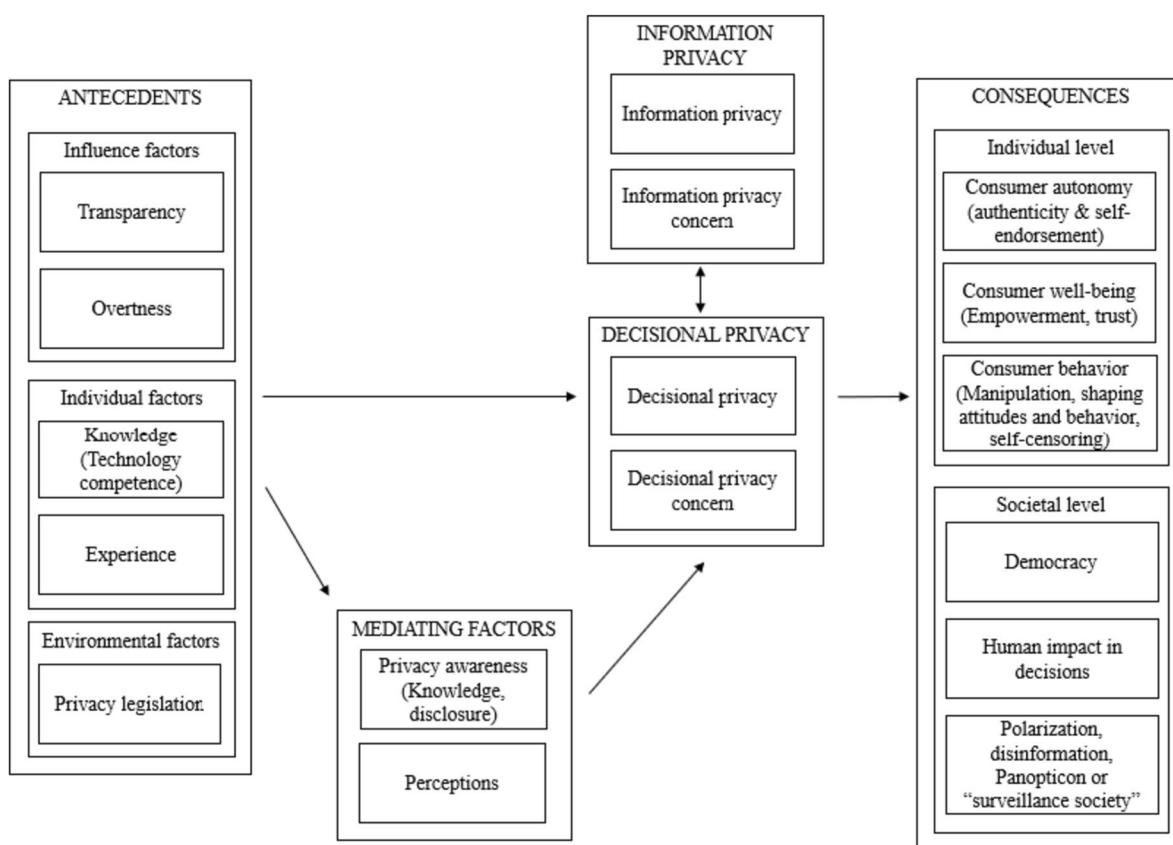
Fig. 2 Nomological network of decisional privacy

these dimensions comprise consumer privacy. As exposure to interference should decrease when consumers' ability to control access to personal information increases, information privacy should promote decisional privacy; however, it does not ensure the absence of interference. Hence, invasions of consumer privacy, consisting of both informational and decisional dimensions, can occur irrespective of access to information (Solove, 2005).

Without access to information about a consumer, external actors still possess massive amounts of aggregated data about similar consumers, from which fairly accurate predictions about this specific consumer may be made. In other words, without compromising this consumer's information privacy, the consumer may still be subjected to decisional interference by manipulative tactics altering their decision architecture (Day & Stemler, 2020). I thus argue that information privacy remains a highly necessary, but not sufficient, criterion for consumer privacy. Although not perfectly, the ability to control access or flows of information should influence consumers' ability to prevent undue influence, and conversely, restricting interference should also diminish future threats to information privacy. Theoretically, information privacy and decisional privacy thus appear to be mutually dependent.

While decisional privacy and information privacy are distinct dimensions, they may be viewed as overlapping on the notion of "use of information," in some definitions of privacy (i.e., Krafft et al., 2017; Luo, 2002), consumer privacy (i.e., Peltier et al., 2009; Phelps et al., 2000; Roznowski, 2003), and information privacy (i.e., Hoffman et al., 1999; Inman & Nikolova, 2017; Peltier et al., 2009). "Use of information" remains inherently vague, potentially referring to a wide array of indefinite activities that do not discern between due and undue information use (i.e., interference). While interference is one potential use of information, conceptual development of decisional privacy and explicating the nature of "use" as a distinct aspect of privacy are necessary to understand consumers' distinct informational and decisional privacy concerns and how the dimensions are related.

Discussion

Reconceptualizing consumer privacy to understand decisional privacy and interference in consumer decision-making implies extending our comprehension of consumer privacy to address the blurred lines between influence and interference. This section discusses the distinct implications

of decisional privacy for consumers, practitioners, and the marketing discipline. As outlined in the introduction, the "dueness" of influence varies, and good marketing practice separates persuasion from manipulation (Sunstein, 2015). Since public knowledge of undue influence practices is likely to deteriorate the reputation of a firm and marketing altogether, clearly distinguishing between acceptable and unethical forms of influence may in itself be useful and beneficial for marketers and the marketing discipline.

The role of decisional privacy in marketing and impact for conceptual development

Since the effect of influence on consumers' attitudes, intentions, behavior, and decision-making represent cornerstones in marketing and consumer behavior research, decisional privacy plays a unique role in these fields. The explication and introduction of decisional privacy implies an expansion of our collective understanding of consumer privacy as consumers' right or ability to control personal information to also include the right or ability to not be subjected to undue influence. This also widens our focus from protecting consumers' previous decisions to consider the power of inferences in shaping consumers' future decisions.

Providing a more complete representation of the privacy construct based on seminal privacy definitions and consumers' current privacy concerns should also increase coherence in terminology and awareness of the distinction between the constructs "privacy" and "information privacy," essential to the construct validity of consumer privacy. As consumers become more informed and aware of how firms exert unethical influence, privacy concerns related to decisional interference are expected to rise in the future. Further, this introduces a new set of research questions to be addressed, such as how *decisional* privacy concerns influence attitudes, intentions, and behavior. Aligned with interpretations of privacy across other research fields, decisional privacy should be reflected in the conceptualization of privacy, consumer privacy, and privacy-related constructs. In particular, understanding consumers' decisional privacy concerns is critical for scholars, marketers, and brands.

In general, decisional interference should be weighed against the "greater good" of society (Sunstein, 2015). While exceptions likely exist, marketing influence is mostly motivated by profits rather than the greater good of society. On this aspect, decisional privacy in marketing differs from decisional privacy in other domains, such as health, where interventions like nudging people towards healthy eating or the use of defaults to promote organ donorship are discussed. As a field, marketing both studies and exerts influence, and interfering with consumers' decision-making for the "greater good" of society occurs less frequently in marketing than in other domains. As marketers, we are not nudging individuals to donate their organs; we are nudging them to buy products, click on ads, download apps, or devote their attention. Driven by economic interests to steer consumers' decision-making, marketing interference primarily benefits its proprietors, not its users, or society altogether.

The notion of decisional privacy is well-aligned with several research fields' commitments to study consumer wellbeing, among them transformative consumer research (TCR) and consumer culture theory (CCT). TCR addresses various issues related to consumption, however these are not restricted to purchase behavior (Davis & Pechmann, 2020; Mick et al., 2012), with topics encompassing poverty and inequity (Chandy et al., 2021); food, obesity, consumer protection, and race (Mende & Scott, 2021); injustice and consumer vulnerability (Davis et al., 2016); and political polarization (Mende & Scott, 2021). TCR underlines the profound effect of marketing on society and consumers, as well as the potential to mitigate this effect, situating the marketing discipline in a larger societal context (Chandy et al., 2021; Newman et al., 2021).

Why decisional privacy matters for consumers

When algorithms replace parts of consumers' decision-making processes, considered formative and identity-defining, this replacement may severely impact consumers' autonomy. Previous research has shown that mere perceptions of being observed can also change consumer behavior (Foucault, 1991; Kapsner & Sandfuchs, 2015; Zwebner & Schrift, 2020). Hence, when algorithms are opaque, deceptive, and hidden, manipulation may easily go unnoticed by consumers, replacing their goals with the goals of the algorithm and its creators. An inability to distinguish whether a recommended product is aligned with their higher-level goals or rather simply a result of deceptive persuasive tactics reduces consumers' ability to engage in well-informed decision-making.

Moreover, leading consumers to act toward ends that are not self-chosen, for inauthentic reasons that do not reflect their true goals or preferences, threatens their autonomy (Susser et al., 2019b). Accordingly, not giving consumers the opportunity to view, adjust, correct, or revise algorithms' inferences, from which profiles about them are constructed, removes agency from consumers to algorithms (Wachter & Mittelstadt, 2019). In this sense, decisional privacy plays a unique role in protecting autonomy in consumers' decision-making, protecting consumers' right to make up their own minds on decisions that matter to them.

Why decisional privacy matters for marketing practitioners

From a brand's, platform's, or marketer's point of view, a competitive landscape devoid of regulation concerning

decisional privacy entails that the use of covert and manipulative persuasion tactics is permitted. This consequently implies that the most successful firms may not necessarily have the best products, the best reputation, or the most satisfied customers, but rather excel by being the most willing and able to capitalize ruthlessly on consumer data, employing the most deceptive means to manipulate consumers' decisions, and exploiting their vulnerabilities most effectively. While this dynamic shifts the competitive terms on which firms compete, public knowledge of deceptive persuasion may have detrimental effects for firms.

As an example, more than 1 billion active users across 154 countries make TikTok one of the world's most popular social media platforms (Demandsage, 2023). Recently, however, TikTok was banned by more than two dozen US states and from federal government devices in countries across the world (Chan, 2023; Maheshwari & Holpuch, 2023). The ban is mainly founded on two sets of consumer privacy concerns:

Table 5 Future research agenda for decisional privacy (DP)

Focus	Research questions, to be explored empirically or conceptually
Decisional Privacy	• How may DP be protected? • What are the drivers of perceived DP? • What are the antecedents of consumers' perceptions of DP? • What influences consumers' preference for DP? • How is the preference for DP influenced by contextual aspects, personality traits, or both?
Decision-making	• How does DP influence consumers in stages of the decision-making process? • Which psychological processes do perceptions of reduced/increased DP evoke? • How do DP concerns influence consumers' attitudes, intentions, and behavior? • In which contexts is DP of particular importance? When do consumers value DP most and least? • How do covert and overt influence impact consumers' decision-making and perceptions of DP? • How does DP influence the intention to adopt algorithmic recommendations?
Information Privacy	• How do DP and information privacy operate in tandem? • How do DP and information privacy influence each other? • How does (the absence of) DP influence information disclosure concern/intent?
Privacy concerns	• What are the implications of DP for the conceptualization of privacy concerns? • How can decisional privacy concerns be operationalized and measured? • How are consumers' decisional privacy concerns influenced by privacy awareness, including decisional privacy awareness? • In which ways does DP concern contribute to privacy-preserving behavior?
Marketing practice	• How can consumers' DP be accommodated in marketing? • How can a focus on DP contribute to more responsible marketing? • How can marketers exert influence without undermining consumers' DP? • How may the design and interface of online platforms promote DP?
AI technology	• How can AI technology be employed without undermining consumers' DP? • How can AI technology be employed to promote consumers' DP? • How do specific AI technologies challenge/promote DP? (i.e., algorithmic recommendations, nudging, psychological targeting, profiling, personalized advertising/targeting, etc.)
Consumer reactance	• (How) does the absence of DP influence consumer reactance? • Is information privacy and DP associated with different types of reactance?
Consumer autonomy	• Under which circumstances are consumers willing to forego DP and autonomy for convenience? • How does DP influence consumers' perceived and actual autonomy?
Transparency	• How does transparency influence DP? • Does disclosure influence (perceptions of) DP? • Does understanding influence (perceptions of) DP?
Customer Satisfaction	• (How) can DP contribute to customer satisfaction? • How can DP be a competitive advantage for marketers/companies/platforms?
Society/ Democracy	• What are the consequences of reduced DP for democracy and society? • How does society's increased dependence on AI technology influence consumers' DP?
Manipulation/ Undue influence	• How does DP prevent manipulation? • How do different technologies constitute "undue influence" for consumers?
Conceptual development	• How should DP be measured? • How should scales for DP-related constructs (i.e., DP concerns, DP risk, DP empowerment) be developed and validated? • How does DP influence existing conceptions of privacy constructs and phenomena (i.e., privacy concerns, privacy awareness, privacy paradox)?

a foreign government's access to users' personal information and the *highly manipulative and customized influence* exerted by the app's complex content-curation algorithms (Chan, 2023; Fung, 2023). TikTok's profound ability and potential to exert personalized influence, exploit consumers' cognitive biases and vulnerabilities, and exert large-scale covert influence and harmful misinformation are well documented. The collective backlash against TikTok illustrates that decisional privacy concerns related to interference exist and that people resent the idea of undue influence.

To address decisional privacy concerns, companies' privacy policies should continue to address the acquisition and handling of consumers' information, but importantly also decisional interference. This priority should also guide the design and interface of online platforms. Furthermore, to accommodate consumers' decisional privacy in the future, practitioners should promote rational and overt persuasion rather than manipulation and covert influence, as an integral part of corporations' future digital responsibility strategies (Wirtz et al., 2023). As the negative consequences of undue marketing are becoming more evident, for example with the "Hall of Shame" (Brignull et al., 2023), more regulation is expected in the future. Hence, adapting such a positioning, business model, and advertising strategy could become a competitive advantage (Day & Stemler, 2020; Eggers et al., 2022; Wirtz et al., 2023).

Future research and limitations

We currently lack insights regarding the contexts in which consumers value decisional privacy. To enable empirical research on decisional privacy,—including its antecedents and consequences—requires conceptual development, including the establishment and validation of a definition and scale for decisional privacy. Such a scale should reflect the identified key themes: (1) the absence of interference and undue influence in all stages of the decision-making process and (2 and 3) enabling self-determination in individuals' decisions, choices, and actions. As the proxy used to measure privacy, *decisional* privacy concerns require further investigation, which should capture consumers' worries related to external agents interfering in their preference construction and decision-making, being covertly influenced or manipulated into making a certain choice, or being unable to make autonomous decisions.

Devoting research attention to decisional privacy should also shed new light on existing privacy-related phenomena. The notion that consumers' information disclosure may be influenced by manipulative design tactics that exploit cognitive biases (Day & Stemler, 2020; Thaler & Sunstein, 2009) may provide a new perspective on the "privacy paradox," noting how people disclose information despite concerns about their privacy (Norberg et al., 2007; Waldman, 2020). In sum, the proposed research agenda indicates how decisional privacy can yield valuable insight for marketing scholars and practitioners in the future (Table 5).

While the inclusion of descriptions and explanations of privacy in the systematic literature review, in addition to explicit definitions, could be considered a limitation, this choice aligns with the aim of identifying the range of understandings and definitions of privacy and conveying how privacy has been understood and communicated in the marketing field. These "non-explicit definitions" were also considered essential due to the recognized difficulty of defining privacy (Bleier et al., 2020; Martin & Murphy, 2017; Martin et al., 2017; Peltier et al., 2009). Moreover, while the focus on higher-level marketing journals could also reinforce a publication bias, this concern was balanced against these journals' influence on the privacy discourse in terms of reach and impact. Hence, studying these journals' understandings of privacy was considered valuable.

Conclusion

AI systems' unobtrusive and covert influence obfuscates the lines between persuasion and manipulation, compromising consumers' ability to determine their own course of action and engage in deliberate, well-informed decision-making (Deci & Ryan, 2000; Ryan & Deci, 2000). As consumers' identities are shaped by the attitudes and preferences they develop, and ultimately the decisions they make, outsourcing formative and identity-defining processes to algorithms may severely impact consumers' autonomy. While these changes have implications for individual consumers' privacy online, the collective-scale consequences of undermining consumer autonomy are more serious than the minute choice of one product over the other, since democracy is premised on the free choice of individuals.

By preventing interference, decisional privacy promotes consumers' right and ability to not be manipulated or unduly influenced, as well as their right and ability to make self-determined decisions. Introducing and explicating the decisional privacy construct and developing this conceptually, the paper contributes to the conceptual realignment of consumer privacy in the context of online decision-making. Extending previous research on consumer privacy and existing definitions of decisional privacy, this work also provides a starting point for developing a decisional privacy scale to enable future empirical research. While consumer privacy continues to entail protecting consumers' personal information regarding past decisions and behavior, I propose that it also relates to protecting their future decisions from interference.

The novelty of the paper lies in explicating and explaining decisional privacy and its relevance for consumer privacy. I have proposed that information privacy is a necessary but insufficient condition for consumer privacy, implying that despite perfect information privacy, consumer privacy can still be breached through decisional privacy. Facing a whole new range of interference, it thus remains fundamental to understand how privacy influences

consumers and their decisions and to capture and understand consumers' current privacy concerns. Hence, definitions and operationalizations of privacy and privacy concerns should reflect both decisional privacy and information privacy as dimensions of consumer privacy.

The paper aims to reinvigorate the discussion on consumer privacy in light of the radical changes in what privacy means for consumers today. Aligned with the aims of transformative consumer research (TCR), advocating that marketing should be seen in a larger societal context, the paper supports the notion of "better marketing for a better world" (Chandy et al., 2021) and marketing research as "a force for good" (Mende & Scott, 2021). In addition to being unethical, covert and manipulative influence is deteriorating the reputation of marketing practices and making marketing activities seem exploitative altogether.

In conclusion, I hope that this article will contribute to awareness of decisional privacy among researchers, practitioners, consumers, and policymakers and motivate future research. As emphasized by decisional privacy research in other fields, corporations' use of algorithms poses the largest threat to consumers' decisional privacy today (Fairfield & Reynolds, 2022). As marketing scholars, we should not neglect the constructs closest to us—influence and decision-making—or leave the important task of understanding the implications of pervasive technological changes on

consumers' privacy and decision-making up to other academic disciplines. Hence, as a field focused on influence, marketing should recognize decisional privacy as a significant dimension of consumer privacy, which supplements information privacy.

Appendix A: Literature review of privacy in marketing

According to Table 6, the journals with the highest volume of papers explaining privacy or a privacy-related construct included the Journal of Public Policy and Marketing (49 papers), Psychology and Marketing (41 papers), Journal of Interactive Marketing (33 papers), Marketing Science (30 papers), and Journal of Retailing (24 papers). Journals with the highest percentage of articles offering a definition, explanation, and/or operationalization of privacy, or a privacy-related construct, included Journal of Consumer Research (100%), Journal of Interactive Marketing (63.6%), Journal of the Academy of Marketing Science (61.1%), Psychology and Marketing (61%), Journal of Retailing (54.2%), and Industrial Marketing Management (53.3%). Below is a brief review of relevant privacy constructs identified in the review. Table 6 provides an overview of the volume of papers identified that contained "privacy" in the title, keywords, abstract, or topic, noting in parentheses how many papers provide a definition or explanation for a privacy or privacy-related construct.

Table 6 Review of privacy, sorted by 2021 chartered association of business schools' academic journal guide

ABS Level	Journal name	Privacy in title, key words, abstract, or topic	Contains explanation, definition, or operationalization
4*	Journal of Consumer Psychology	8 (2)	25 %
4*	Journal of Consumer Research	4 (4)	100 %
4*	Journal of Marketing	17 (5)	29.4 %
4*	Journal of Marketing Research	12 (0)	0 %
4*	Journal of the Academy of Marketing Science	18 (11)	61.1 %
4*	Marketing Science	30 (1)	3.3 %
4	International Journal of Research in Marketing	11 (4)	36.4 %
4	Journal of Retailing	24 (13)	54.2 %
3	European Journal of Marketing	17 (6)	35.3 %
3	Industrial Marketing Management	15 (8)	53.3 %
3	International Marketing Review	5 (2)[1]	50 %
3	Journal of Advertising	20 (9)	45 %
3	Journal of Advertising Research	13 (6)	46.2%
3	Journal of Interactive Marketing	33 (21)	63.6 %
3	Journal of International Marketing	2 (0)	0 %
3	Journal of Public Policy and Marketing	49 (25)	51 %
3	Marketing Letters	12 (3)	25 %
3	Marketing Theory	4 (2)	0 %
3	Psychology and Marketing	41 (25)	61 %
3	Quantitative Marketing and Economics	2 (1)	50 Un

[1]Unable to access two articles. These papers are hence excluded from the calculated percentage

Literature review of Privacy in Marketing - Method

I first searched Web of Science for articles in ABS level 4*, 4, and 3 marketing journals containing 'privacy' in the title, resulting in 73 papers in total. The majority of these fulfilled the review criteria, providing a definition, explanation, explicit interpretation, or operationalization of privacy or privacy-related constructs (i.e., consumer privacy, privacy concern, and information privacy). Seven papers were excluded due to a lack of this and were hence considered unable to aid in answering the research question, resulting in a review of 66 papers. 90.4% of papers identified in the first round fulfilled the review criteria and were included in further analysis. In the second round, the search was extended. Again, I systematically searched Web of Science for all ABS level 4*, 4, and 3 marketing journals for articles containing "privacy" either in the title, abstract, keywords, or as the topic. The decision to only search for "privacy" (e.g., not "private" or "privatize") was found to yield the most relevant search results, based on a preliminary stage employing a "trial and error" strategy. The choice of these recognized premier outlets for marketing research was based on their influential potential in terms of scope and reach, serving as benchmarks for the field.

The first search was conducted in June 2021, and the second search was concluded in September 2022, imposing no time restrictions on either search period. In total, 292 articles were reviewed in the second round. This involved an additional 212 papers, adding to the original 73 papers in the first round. Out of the 292 reviewed papers, only 129 fulfilled the review criteria of offering a definition, explicit interpretation, explanation, or operationalization of privacy, or a privacy-related construct. Thus, extending the search to include articles that contained "privacy" in the abstract, keywords, or topic reduced the definition/explanation rate to 43.6%, however, a much larger volume of articles was reviewed.

To ensure that the review reflected the most up-to-date research, a third round of searches was conducted in April 2023. The same journals were searched in the same manner as in the second round. Out of the 22 additional papers identified and reviewed in this round, ten fulfilled the review criteria by offering a definition or explanation of privacy. A fourth and final search was conducted in December 2023, in the time period between April 2023 and December 2023, following the same procedure as previous rounds. Out of the 19 papers identified in this round, seven fulfilled the review criteria. In total, 333 papers were reviewed, and 148 of the reviewed papers fulfilled the review criteria across the four rounds.

Privacy

In general, most definitions of privacy in marketing are centered around personal information and data (i.e., Culnan,

2000; Martin & Murphy, 2017; Martin et al., 2020; Rust et al., 2002; Stewart 2017). Most definitions emanate from the seminal definition of privacy as "the right or ability to control information about oneself" (Westin, 1967). Moreover, definitions largely reflect the extent to which information is disclosed to, or known by, others (Luo, 2002; Rust et al., 2002), awareness of information being collected (Culnan, 2000; Krafft et al., 2017; Luo, 2002; Visentin et al., 2021), use of information, and knowledge about how it is used (Ioannou et al., 2021; Krafft et al., 2017; Milne & Culnan, 2004; Visentin et al., 2021). Together, these definitions and understandings of privacy reflect the information privacy dimension.

A second theme emerging from definitions is privacy as "The right or ability to be let alone" (Warren & Brandeis, 1890) and avoid intrusions (Bleier et al., 2020; Foxman & Kilcoyne, 1993; Luo, 2002; Massara et al., 2021; Peltier et al., 2009; Petty, 2000; Phelps et al., 2000; Rapp et al., 2009; Roznowski, 2003). Similarly, some consider privacy to be the right to not be subjected to intrusions (Foxman & Kilcoyne, 1993; Goodwin, 1991; Mayer & White, 1969; Peltier et al., 2009; Phelps et al., 2000; Rapp et al., 2009; Roznowski, 2003). Definitions are, however, quite elusive regarding the meaning of and from what one should be "let alone". While some contend that the object of intrusion refers to "an individual's private affairs, his solitude or his seclusion" (Mayer & White, 1969, p. 2), others suggest that "intrusion" can encompass "unwanted marketing solicitations" (Petty 2000, p. 42). Together, "the right to be let alone" and "the right to be protected from intrusions" can relate to decisional privacy due to its focus on interference; however, decisional privacy is not addressed explicitly.

Most definitions of privacy focus on either "information privacy" or "the right to be let alone or avoid intrusions", interpreted here as decisional privacy. However, the notion that privacy rests on both principles has also been proposed (Jones, 1991). Similarly, a view of privacy as "the selective control of access to the self" (Altman, 1975) promotes the importance of control over privacy. Access to the self may be interpreted both as access to information about the self (information privacy) and as access to influence or thereby steer decision-making (decisional privacy). However, the review only identified appropriation or control of the flow of information, leaving the appropriation or control of decisional influence and intrusions mostly unaddressed. See Web Appendix A for an overview of privacy definitions.

Consumer privacy

In the early 1990s, efforts were made to understand and describe the implications of privacy for consumers. Consumer privacy was originally defined as «the consumer's ability to control the (a) presence of other people in the

environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behavior to those who were not present» (Goodwin, 1991, p. 152). This two-dimensioned approach to privacy was corroborated by a pronounced need to focus on both the right to "be let alone" and "control personal information" (Jones, 1991, p. 135). Together, this supports the notion that consumer privacy provides protection on two dimensions: access to information (information privacy) and against intrusions, i.e., interference in the decision-making process (decisional privacy). These dimensions carry direct links to the dimensions of privacy outlined by the formative definitions of Westin (1967) and Warren and Brandeis (1890), respectively. This concurs that consumer privacy has traditionally entailed the aspect of undue influence, central to autonomous decision-making.

In line with this, consumers' knowledge and control as appropriate dimensions to conceptualize consumer privacy have also been emphasized (Milne, 2000). Other definitions are restricted to knowledge and control of information, omitting control and knowledge of undue influence, decisional interference, or decisional privacy. It was later noted that much of the privacy debate appeared to focus on the collection and dissemination of personal information (Horppu, 2023; Petty, 2000). Upholding that "unwanted marketing solicitations" should be included in the right to be, let alone is supported by previous research (Jones, 1991; Goodwin, 1991). See Web Appendix B for an overview of consumer privacy definitions.

Information privacy

Information privacy was originally defined as «The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others» (Westin, 1967, p. 7). Definitions of information privacy are centered around personal information and data and the claims, rights, or abilities of individuals to control how personal information is acquired, collected, or used (Bandara et al., 2020; Inman & Nikolova, 2017; Martin & Murphy, 2017; Miyazaki & Fernandez, 2000; Peltier et al., 2009). Control is a recurring theme in definitions, including consumers' or individuals' ability, rights, or claims to control, or appropriate, flows of personal information (Bleier et al., 2020; Inman & Nikolova, 2017; Massara et al., 2021; Nissenbaum, 2011; Okazaki et al., 2009; Roznowski, 2003; Song et al., 2021; Westin, 1967). This includes the extent to which such information is communicated, disclosed, or transferred to others (Martin & Murphy, 2017; Okazaki et al., 2009; Peltier et al., 2009; Roznowski, 2003 Song et al., 2021) and how this information is used (Bandara et al., 2020; Inman & Nikolova, 2017;

Martin & Murphy, 2017). See Web Appendix C for an overview of definitions of information privacy.

Privacy concerns

The review reveals that the definitions and interpretations of consumers' privacy concerns reflect a pronounced focus on information privacy, with only one exception (Zwebner & Schrift, 2020). This includes a focus on information and data reflected in identifying the antecedents and consequences of consumers' privacy concerns (Phelps et al., 2000). Some propose that "consumer privacy concerns relate mainly to personal data, including name, address, demographics, lifestyle, interests, shopping preferences, and purchase history (Lwin et al., 2008, p. 207; Nowak & Phelps, 1992)". Furthermore, the concepts "privacy concern" and "information privacy concern" are often used interchangeably (e.g., Bandara et al., 2020; Martin & Murphy, 2017; Okazaki et al., 2009). Due to this, claims to address "consumer privacy concerns" mostly only address concerns pertaining to information privacy (i.e., Bandara et al., 2020; Malhotra et al., 2004). Out of 49 papers providing a definition or explanation of privacy concerns, 48 confine these concerns to information privacy. Altogether, this illustrates a prevalent focus on information privacy in the literature on consumers' privacy concerns. See Web Appendix D for an overview of definitions of privacy concerns.

Operationalization of privacy concern

Privacy concern is the operationalization applied when marketing scholars aim to study privacy empirically, recognized as "the best proxy to understand consumers' feelings about their information privacy" (Martin & Murphy, 2017, p. 145). The review uncovers that operationalizations of privacy concerns are confined entirely to "information privacy concerns" for privacy, consumer privacy, and particularly for privacy concerns. Out of 35 papers operationalizing privacy concerns, 32 address only informational privacy concerns, two refer to privacy concerns simply as concerns for privacy, and only one latently addresses decisional privacy concerns: concerns related to interference or intrusions (Zwebner & Schrift, 2020). See Web Appendix E for an overview of the operationalization of privacy concerns.

Other privacy concepts identified

Apart from the four main privacy concepts, additional privacy concepts were identified, however far less frequently, i.e., "privacy control", "privacy risk", "privacy calculus", "privacy protection behaviors", "privacy empowerment", and "privacy invasiveness". All share a focus on information

privacy. See Web Appendix F for an overview of definitions of privacy concepts.

Declarations

Conflicts of interest The author declares no conflict of interest.

References

Acikgoz, F., Perez-Vega, R., Okumus, F., & Stylos, N. (2023). Consumer engagement with AI-powered voice assistants: A behavioral reasoning perspective. *Psychology & Marketing, 40*(11), 2226–2243.

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society.* Rowman & Littlefield.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding.* Brooks/Cole Publishing Company.

André, Q., Carmon, Z., Wertenbroch, K., Crum, A., Frank, D., Goldstein, W., Huber, J., van Boven, L., Weber, B., & Yang, H. (2018). Consumer choice and autonomy in the age of artificial intelligence and big data. *Customer Needs and Solutions, 5*(1), 28–37.

Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of Advertising, 41*(1), 59–76.

Bakir, V., & McStay, A. (2023). Harms to the civic body from false information online. In *Optimising emotions, incubating falsehoods: How to protect the global civic body from disinformation and misinformation*, pp. 175–203. Cham: Springer International Publishing.

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services, 52*, 1–9.

Banker, S., & Khetani, S. (2019). Algorithm overdependence: How the use of algorithmic recommendation systems can increase risks

to consumer well-being. *Journal of Public Policy & Marketing, 38*(4), 500–515.

Becher, S. I., & Feldman, Y. (2016). Manipulating, fast and slow: The law of non-verbal market manipulations. *Cardozo Law Review, 38*, 1–48.

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.

Bergdahl, J. (2020). Are 14 people really looking at that product? Retrieved Dec 9, 2021, from https://blog.devgenius.io/are-14-people-currently-looking-at-this-product-e7fe8412f16b

Bjørlo, L., Moen, Ø., & Pasquine, M. (2021). The role of consumer autonomy in developing sustainable AI: A conceptual framework. *Sustainability, 13*(4), 1–18.

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.

Bolin, S. (1998). E-commerce: A market analysis and prognostication. *StandardView, 6*(3), 97–105.

Borenstein, J. (2008). Privacy: A non-existent entity. *IEEE Technology and Society Magazine, 27*(4), 20–26.

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.

Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023). Deceptive patterns – user interfaces designed to trick you. deceptive.design. Retrieved Nov 25, 2023, from https://www.deceptive.design/

Brough, A. R., Kamleitner, B., & Martin, K. D. (2023). Physical and digital privacy: How developed and developing countries differ in both vulnerability and protection. *Journal of International Marketing, 31*(4), 76–79.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157–165.

Calvo, R. A., Peters, D., Vold, K., & Ryan, R. M. (2020). Supporting human autonomy in AI systems: A framework for ethical enquiry. *Ethics of Digital Well-Being* (pp. 31–54). Springer.

Campbell, C., & Marks, L. J. (2015). Good native advertising isn't a secret. *Business Horizons, 58*(6), 599–606.

Castmo, M., & Persson, R. (2018). The alliance of digital nudging & persuasive design: The complementary nature of the design strategies. [Master's thesis, Lund University]. Retrieved 03 Sep 2022 https://lup.lub.lu.se/student-papers/record/8950219/file/8950235.pdf

Chan, K. (2023, April 4). Here are the countries that have bans on TikTok. *AP News.* https://apnews.com/article/tiktok-ban-privacy-cybersecurity-bytedance-china-2dce297f0aed056efe53309bbcd44a04

Chandy, R. K., Johar, G. V., Moorman, C., & Roberts, J. H. (2021). Better marketing for a better world. *Journal of Marketing, 85*(3), 1–9.

Chartered Association of Business Schools. (2021). Academic Journal Guide 2021: Methodology. Retrieved August, 2022, from https://charteredabs.org/academic-journal-guide-2021-view/

Chen, J. V., Ross, W., & Huang, S. F. (2008). Privacy, trust, and justice considerations for location-based mobile telecommunication services. *info, 10*(4), 30–45.

Cheung, C., Lee, Z. W., & Chan, T. K. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research, 25*(2), 279–299.

Churchill, G. A., Jr. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64–73.

Cohen, J. E. (2000). Examined lives: Informational privacy and the subject as object. In *Law and Society Approaches to Cyberspace,* pp. 473–538. Routledge.

Cohen, J. L. (2009). *Regulating intimacy*. Princeton University Press.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review, 126*(7), 1904–1933.

Contissa, G., Lagioia, F., Lippi, M., Micklitz, H. W., Palka, P., Sartor, G., & Torroni, P. (2018). Towards consumer-empowering artificial intelligence. *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Evolution of the contours of AI*, 5150–5157.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing, 19*(1), 20–26.

Solove, DJ. (2006). A taxonomy of privacy. University of *Pennsylvania law review, 154*(3), 477–560.

Davis, B., Ozanne, J. L., & Hill, R. P. (2016). The transformative consumer research movement. *Journal of Public Policy & Marketing, 35*(2), 159–169.

Davis, B., & Pechmann, C. (2020). The characteristics of transformative consumer research and how it can contribute to and enhance consumer psychology. *Journal of Consumer Psychology, 30*(2), 365–367.

Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science, 48*, 24–42.

Day, G., & Stemler, A. (2020). Are Dark Patterns Anticompetitive? *Alabama Law Review, 72*, 1.

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press.

Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin, 125*(6), 627–668.

Deci, E. L., & Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry, 11*(4), 227–268.

Demandsage. (2023). TikTok Statistics 2023 — (Users, Revenue and Trends). Accessed April 10, 2023. https://www.demandsage.com/tiktok-user-statistics/

DeVellis, R. F. (1991). *Scale development: Theory and applications* (Applied Social Research Methods Series, Vol. 26). Sage Publications.

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. In *Proceedings of the 2020 CHI conference on human factors in computing systems.* Association for Computing Machinery, New York, NY, USA, pp. 1–14.

Dimopoulos, G. (2022). *Decisional privacy and the rights of the child*. Taylor & Francis.

Eggers, F., Beke, F. T., Verhoef, P. C., & Wieringa, J. E. (2022). The market for privacy: Understanding how consumers trade off privacy practices. *Journal of Interactive Marketing, 58*(4), 341–360.

Essén, A. (2008). The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices. *Social Science & Medicine, 67*(1), 128–136.

Etzioni, A. (1999). *The limits of privacy*. Basic Books.

Fairfield, J., & Reynolds, N. (2022). Griswold for Google: Algorithmic determinism and decisional privacy. *The Southern Journal of Philosophy, 60*(1), 5–37.

Felsen, G., Castelo, N., & Reiner, P. B. (2013). Decisional enhancement and autonomy: Public attitudes towards overt and covert nudges. *Judgment & Decision Making, 8*(3), 202–213.

Ferrell, O. (2017). Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science, 45*(2), 160–163.

Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information Technology, 8*(3), 109–119.

Foucault, M. (1991). *Discipline and punish: The birth of the prison.* Allen Lane.

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing, 12*(1), 106–119.

Frankfurt, H. (1971). Freedom of the will and the concept of a person. *Journal of Philosophy, 68*(1), 5–20.

Fung, B. (2023, March 24). TikTok collects a lot of data. But that's not the main reason officials say it's a security risk. *CNN Business.* https://edition.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing/index.html

Ganley, P. (2002). Access to the individual: Digital rights management systems and the intersection of informational and decisional privacy interests. *International Journal of Law and Information Technology, 10*(3), 241–293.

Gilbert, H. L. (2007). Minors' constitutional right to informational privacy. *The University of Chicago Law Review, 74*(4), 1375–1410.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing, 10*(1), 149–166.

Grafanaki, S. (2016). Autonomy challenges in the age of big data. *The Fordham Intellectual Property, Media and Entertainment Law Journal, 27*, 803–868.

Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* Association for Computing Machinery, New York, NY, USA, pp. 1–18.

Gutwirth, S., Leenes, R., & Hert, P. D. (2014). *Reloading data protection*. Springer.

Hacker, P. (2021). Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal, 29*, 142–175.

Harris, C. E., Jr., Pritchard, M. S., Rabins, M. J., James, R., & Englehardt, E. (2013). *Engineering ethics: Concepts and cases*. Cengage Learning.

Hausman, D. M., & Welch, B. (2010). Debate: To nudge or not to nudge. *Journal of Political Philosophy, 18*(1), 123–136.

Henkin, L. (1974). Privacy and autonomy. *Columbia Law Review, 74*(8), 1410–1433.

Hildebrandt, M., & Gutwirth, S. (2007). (Re) presentation: PTA citizens' juries and the jury trial. *Utrecht Law Review, 3*(1), 24–40.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85.

Hong, W., Chan, F. K., & Thong, J. Y. (2021). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics, 168*, 539–564.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Mis Quarterly, 37*(1), 275–298.

Horppu, J. (2023). Sensing privacy: Extending consumer privacy research through a consumer culture theory approach. *Marketing Theory, 23*(4), 661–684.

Hughes, M., & Lacy, C. J. (2016). "The sugar'd game before thee": Gamification revisited. *Portal: Libraries and the Academy, 16*(2), 311–326.

Hulland, J. (2020). Conceptual review papers: Revisiting existing research to develop and refine theory. *AMS Review, 10*(1–2), 27–35.

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., & Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection

motivation theory perspective. *Psychology & Marketing, 38*(10), 1766–1778.

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*(1–2), 18–26.

Jaccard, J., & Jacoby, J. (2019). *Theory construction and model-building skills: A practical guide for social scientists*. Guilford Publications.

Jones, M. G. (1991). Privacy: A significant marketing issue for the 1990s. *Journal of Public Policy & Marketing, 10*(1), 133–148.

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist, 58*(9), 697.

Kapsner, A., & Sandfuchs, B. (2015). Nudging as a threat to privacy. *Review of Philosophy and Psychology, 6*(3), 455–468.

Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2013). Information privacy and data control in cloud computing: Consumers, privacy preferences, and market efficiency. *Washington & Lee Law Review, 70*, 341–472.

Koops, B. J., Newell, B., Timan, T., Skorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law, 38*(2), 483–575.

Kopalle, P. K., Gangwar, M., Kaplan, A., Ramachandran, D., Reinartz, W., & Rindfleisch, A. (2022). Examining artificial intelligence (AI) technologies in marketing via a global lens: Current trends and future research opportunities. *International Journal of Research in Marketing, 39*(2), 522–540.

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

Krishna, A. (2020). Privacy is a concern: An introduction to the dialogue on privacy. *Journal of Consumer Psychology, 30*(4), 733–735.

Kugler, M. B. (2014). *Affinities in privacy attitudes: A psychological approach to unifying informational and decisional privacy*. Northwestern University.

Lanzing, M. (2019). "Strongly recommended" Revisiting decisional privacy to judge hypernudging in self-tracking technologies. *Philosophy & Technology, 32*(3), 549–568.

Loh, W. (2018). A practice–theoretical account of privacy. *Ethics and Information Technology, 20*(4), 233–247.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*(2), 111–118.

Lwin, M. O., & Williams, J. D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters, 14*(4), 257–272.

Lwin, M. O., Stanaland, A. J. S., & Miyazaki, A. D. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing, 84*(2), 205–217.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293–334.

Maheshwari, S. & Holpuch, A. (2023, April 12). Why countries are trying to ban TikTok. *The New York Times.* https://www.nytimes.com/article/tiktok-ban.html

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, S. T. (1974). Privacy as a behavioral phenomena: Coming of age. In D. H. Carson (Ed.), *Man-Environment Interactions: Evaluations and Applications Part II* (pp. 101–123). Hutchinson & Ross.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5–21.

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411–429.

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

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., Wang, Y., & Weaven, S. K. (2020). Data privacy in retail. *Journal of Retailing, 96*(4), 474–489.

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.

Massara, F., Raggiotto, F., & Voss, W. G. (2021). Unpacking the privacy paradox of consumers: A psychological perspective. *Psychology & Marketing, 38*(10), 1814–1827.

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems.* Association for Computing Machinery, New York, NY, USA, pp. 1–18.

Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current Opinion in Psychology, 31*, 116–121.

Mayer, C. S., & White, C. H., Jr. (1969). The law of privacy and marketing research. *Journal of Marketing, 33*(2), 1–4.

Mende, M., & Scott, M. L. (2021). May the force be with you: Expanding the scope for marketing research as a force for good in a sustainable world. *Journal of Public Policy & Marketing, 40*(2), 116–125.

Mick, D. G., Pettigrew, S., Pechmann, C., & Ozanne, J. L. (2012). Origins, qualities, and envisionings of transformative consumer research. In Mick, D. G., Pettigrew, S., Pechmann, C., & Ozanne, J. L. (Eds.), In *Transformative consumer research for personal and collective well-being*, pp. 3–24. Taylor & Francis.

Mill, J. S. (2006). [1869]. *On liberty and the subjection of women.* Alan Ryan (Ed.), Penguin Classics.

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing, 19*(1), 1–6.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*(1), 54–61.

Moradi, M., & Dass, M. (2022). Applications of artificial intelligence in B2B marketing: Challenges and future directions. *Industrial Marketing Management, 107*, 300–314.

Moskop, J. C., Marco, C. A., Larkin, G. L., Geiderman, J. M., & Derse, A. R. (2005). From Hippocrates to HIPAA: Privacy and confidentiality in emergency medicine—Part I: Conceptual, moral, and legal foundations. *Annals of Emergency Medicine, 45*(1), 53–59.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society a: Mathematical, Physical and Engineering Sciences, 374*, 1–17.

Mulligan, D. K., Regan, P. M., & King, J. (2020). The fertile dark matter of privacy takes on the dark patterns of surveillance. *Journal of Consumer Psychology, 30*(4), 767–773.

Murphy, P. E., Laczniak, G. R., & Harris, F. (2012). *Ethics in marketing: International cases and perspectives.* Taylor & Francis.

Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: Past, present, and future: The evolution of tricky user interfaces. *Queue, 18*(2), 67–92.

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications.* Sage Publications.

Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology, 15*(2), 87–104.

Newman, C. L., Finkelstein, S. R., & Davis, B. (2021). Transformative consumer research and public policy and marketing research: Distinct, yet complementary, approaches. *Journal of Public Policy & Marketing, 40*(3), 331–335.

Niker, F., Felsen, G., Nagel, S. K., & Reiner, P. B. (2021). Autonomy, evidence-responsiveness, and the ethics of influence. In M. J. Blitz & J. C. Bublitz (Eds.), *The Law and Ethics of Freedom of Thought, Volume 1: Neuroscience, Autonomy, and Individual Rights,* pp. 183–212. Palgrave Macmillan Cham.

Nill, A., & Aalberts, R. J. (2014). Legal and ethical challenges of online behavioral targeting in advertising. *Journal of Current Issues & Research in Advertising, 35*(2), 126–146.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

Nowak, G. J., & Phelps, J. E. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing, 6*(4), 28–39.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising, 38*(4), 63–77.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy.* Crown.

Ottlewski, L., Rokka, J., & Schouten, J. W. (2023). How consumer-initiated platforms shape family and consumption. *Marketing Theory, 0*(0), 1–29.

Packard, V. (1957). *The hidden persuaders.* David McKay Company.

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

Petty, R. D. (2000). Marketing without consent: Consumer choice and costs, privacy, and public policy. *Journal of Public Policy & Marketing, 19*(1), 42–53.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27–41.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2–17.

Plangger, K., Marder, B., Montecchi, M., Watson, R., & Pitt, L. (2023). Does (customer data) size matter? Generating valuable customer insights with less customer relationship risk. *Psychology & Marketing, 40*(10), 2016–2028.

Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). Advertising and consumer privacy. *Journal of Advertising, 38*(4), 51–61.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. University of North Carolina Press.

Roest, H., & Pieters, R. (1997). The nomological net of perceived service quality. *International Journal of Service Industry Management, 8*(4), 336–351.

Roznowski, J. L. (2003). A content analysis of mass media stories surrounding the consumer privacy issue 1990–2001. *Journal of Interactive Marketing, 17*(2), 52–69.

Rust, R. T., Kannan, P., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science, 30*(4), 455–464.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68.

Ryan, R. M., & Deci, E. L. (2006). Self-regulation and the problem of human autonomy: Does psychology need choice, self-determination, and will? *Journal of Personality, 74*(6), 1557–1586.

Ryan, R. M., & Deci, E. L. (2017). *Self-determination theory: Basic psychological needs in motivation, development, and wellness.* Guilford Publications.

Rössler, B. (2005). *The value of privacy*. Polity Press.

Rössler, B. (2018). *The value of privacy*. John Wiley & Sons.

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media+ Society, 3*(1), 1–14.

Skinner-Thompson, S. (2015). *Outing Privacy. Northwerstern University Law Review, 110*(1), 159–222.

Solove, D. J. (2000). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*, 1393–1462.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*, 477–560.

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.

Stanford Digital Civil Society Lab. (n.d.). *Dark patterns tip line*. Retrieved 01 Dec 2023. https://darkpatternstipline.org/

Stewart, D. W. (2017). A comment on privacy. *Journal of the Academy of Marketing Science, 45*(2), 156–159.

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Consumer view on personalized advertising: Overview of self-reported benefits and concerns. In: Bigne, E., Rosengren, S. (Eds.), *Advances in Advertising Research X: Multiple Touchpoints in Brand Communication*, pp. 53–66. Springer Gabler.

Strycharz, J., & Segijn, C. M. (2022). The future of dataveillance in advertising theory and practice. *Journal of Advertising, 51*(5), 574–591.

Sunstein, C. R. (2015). *Fifty shades of manipulation.* Journal of Behavioral Marketing.

Supreme Court Of The United States. (1965) U.S. Reports: Griswold v. Connecticut, 381 U.S. 479. [Periodical] Retrieved from the Library of Congress, https://www.loc.gov/item/usrep381479/. Retrieved on 03 Mar 2023.

Susser, D., Roessler, B., & Nissenbaum, H. (2019a). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review, 4*(1), 1–45.

Susser, D., Roessler, B., & Nissenbaum, H. (2019b). Technology, autonomy, and manipulation. *Internet Policy Review, 8*(2).

Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. *The handbook of information and computer ethics*, pp. 131–164. John Wiley & Sons.

Tene, O., & Polonetsky, J. (2013). A theory of creepy: Technology, privacy and shifting social norms. *Yale Journal of Law & Technology, 16*, 59–102.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology, 11*(2), 105–112.

Van der Sloot, B. (2017). Decisional privacy 2.0: The procedural requirements implicit in Article 8 ECHR and its potential impact on profiling. *International Data Privacy Law, 7*(3), 190–201.

Vargo, S. L., & Koskela-Huotari, K. (2020). Advancing conceptual-only articles in marketing. *AMS Review, 10*, 1–5.

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.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review, 2*, 494–620.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox.' *Current Opinion in Psychology, 31*, 105–109.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63–70.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*, 193–220.

Wertenbroch, K., Schrift, R. Y., Alba, J. W., Barasch, A., Bhattacharjee, A., Giesler, M., Knobe, J., Lehmann, D. R., Matz, S., Nave, G., Parker, J. R., Puntoni, S., Zheng, Y., & Zwebner, Y. (2020). Autonomy in consumer choice. *Marketing Letters, 31*(4), 429–439.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Wilkinson, T. M. (2013). Nudging and manipulation. *Political Studies, 61*(2), 341–355.

Willis, L. E. (2017). Performance-based remedies: Ordering firms to eradicate their own fraud. *Law & Contemporary Problems, 80*(3), 7–41.

Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research, 26*(2), 173–190.

Wood, A. W. (2014). Coercion, manipulation, exploitation. *Manipulation: Theory and Practice,* 17–50.

Zarsky, T. Z. (2002). Mine your own business: Making the case for the implications of the data mining of personal information in the forum of public opinion. *Yale Journal of Law & Technology, 5*, 1–56.

Zhang, J. Z., & Watson, G. F., IV. (2020). Marketing ecosystem: An outside-in view for sustainable advantage. *Industrial Marketing Management, 88*, 287–304.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Zwebner, Y., & Schrift, R. Y. (2020). On My own: The aversion to being observed during the preference-construction stage. *Journal of Consumer Research, 47*(4), 475–499.