VILNIUS UNIVERSITY

FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION

MARKETING AND INTEGRATED COMMUNICATION

Danielius Aliaševičius

MASTER THESIS

TITLE IN LITHUANIAN	TITLE IN ENGLISH
PASITIKĖJIMO ĮTAKA VARTOTOJŲ NORUI PERDUOTI ASMENS DUOMENIS PREKIŲ ŽENKLAMS LEIDIMAIS GRĮSTOJE RINKODAROJE	**THE IMPACT OF TRUST ON CONSUMER'S WILLINGNESS TO DISCLOSE PERSONAL DATA TO BRANDS IN PERMISSION-BASED MARKETING**

Supervisor assoc. prof. dr. Mindaugas Degutis

Vilnius, 2026

TABLE OF CONTENTS

FIGURES

TABLES

INTRODUCTION

Relevance of the Study. In today's digital environment, personal data play a key role in how companies communicate with consumers. Permission-based marketing relies on individuals voluntarily sharing their data in exchange for more relevant and personalized messages. For such approaches to work, consumers must be willing to disclose personal information. However, many remain hesitant due to ongoing concerns about privacy and data misuse. Although regulations such as the General Data Protection Regulation (GDPR) aim to increase transparency and protect consumers' rights, they have not fully eliminated doubts about how personal data are collected and used (Tesseras, 2019).

Previous research has shown that trust plays an important role in reducing privacy concerns and encouraging data sharing, particularly trust in brands that collect and use personal data (Urbonavicius et al., 2021; Zimaitis et al., 2022). At the same time, data disclosure does not occur in isolation. Consumers interact with digital services through technological systems and within regulatory environments, suggesting that trust in technologies and trust in government may also influence how privacy risks are perceived. These trust dimensions are often examined separately in the literature, and their combined effect on privacy concerns, perceived control, and willingness to disclose personal data remains insufficiently explored. In addition, many studies treat personal data as a single category, even though consumers clearly differentiate between less sensitive information, such as contact details, and highly sensitive data, such as medical or financial information.

This thesis addresses these gaps by examining how trust in brand, trust in technologies, and trust in government relate to privacy concerns, perceived control over personal data, and perceived benefits of personalization in shaping consumers' willingness to disclose personal data in permission-based marketing contexts. Furthermore, the study explicitly considers differences in data sensitivity by analyzing disclosure behavior across multiple types of personal data. The results provide insights that are relevant for businesses, policymakers, and technology developers seeking to design data practices that are both effective and respectful of consumer expectations.

Theoretical Contribution. This study draws on established theoretical perspectives, including Privacy Calculus Theory and its extensions, Commitment–Trust Theory, Trust Transfer Theory, and the Technology Acceptance Model, to better understand how consumers make decisions about personal data disclosure. While existing research mainly emphasizes trust in

brand, this thesis broadens the perspective by also considering trust in government and trust in technologies as factors that shape privacy concerns and perceived control.

In addition, the study contributes to privacy calculus research by showing that disclosure decisions depend on the type of personal data involved. By distinguishing between low-, moderate-, and high-sensitivity data, the thesis demonstrates that consumers weigh risks and benefits differently depending on the context. This sensitivity-based approach helps explain why willingness to disclose varies across data types and adds depth to existing models of data disclosure behavior.

Level of Exploration of the Topic. Although permission-based marketing is widely used in practice, it remains relatively underexplored in academic research. A review by Swain (2023) identified only 38 peer-reviewed studies on permission-based marketing published between 2000 and 2021, indicating a clear need for further empirical work. This thesis contributes to addressing this gap by combining theoretical analysis with quantitative research focused on consumer perceptions and behavior.

The study is conducted within the Lithuanian context and is based on survey data collected from consumers familiar with a well-known urban mobility brand "Bolt". By examining trust in brand, trust in government, trust in technologies, privacy concerns, and data sensitivity, the research extends existing empirical insights and provides practical implications for the development of ethical and trust-oriented data-sharing practices.

Research Problem. Despite regulatory efforts and the growing adoption of permission-based marketing, consumers' hesitation to disclose personal data remains a significant challenge. This reluctance is largely driven by privacy concerns and varying levels of trust in brands, governmental institutions, and digital technologies. While trust in brand has been widely studied, the roles of trust in government and trust in technologies, particularly in relation to different types of personal data, are still not fully understood.

Aim of the Thesis. The aim of this thesis is to examine how trust in government, trust in technologies, trust in brand, and the sensitivity of personal data types interact to shape consumers' willingness to disclose personal data for permission-based marketing.

Objectives of the Thesis

1. To analyze theoretical frameworks relevant to permission-based marketing, including Privacy Calculus Theory, Commitment–Trust Theory, and Trust Transfer Theory, with a focus on trust-related mechanisms.
2. To examine factors influencing consumers' willingness to disclose personal data, emphasizing trust in brand, trust in government, trust in technologies, privacy concerns, and perceived control.
3. To conduct empirical research using survey data to assess how trust dimensions and data sensitivity affect disclosure behavior.
4. To develop recommendations for businesses, policymakers, and technology developers aimed at strengthening trust and promoting responsible data-sharing practices.

Research methods. A quantitative research design was used to test the proposed research model. Data were collected through an online survey administered to Lithuanian consumers familiar with "Bolt Services", an urban mobility brand. Measurement scales for trust, privacy concerns, perceived control, perceived benefits, and willingness to disclose personal data were adapted from validated instruments used in previous studies. Data analysis was conducted using IBM SPSS Statistics and included descriptive statistics, reliability analysis, simple and multiple regression analysis, moderation analysis, and exploratory cluster analysis.

1. FUNDAMENTALS OF TRUST AND DATA SHARING DECISIONS IN THE CONTEXT OF PERMISSION-BASED MARKETING

1.1. Building Trust in Permission-Based Marketing

1.1.1. Origin of Trust and Consumer Behaviour in Data Disclosing Decisions

Permission-based marketing emphasizes obtaining explicit consumer consent before sending marketing communications, fostering personalized and interactive relationships. This marketing method emphasizes respect for consumer autonomy and aims to foster trust by ensuring that marketing efforts are both relevant and non-intrusive. By aligning with the principles of relationship marketing and one-to-one marketing, this approach focuses on long-term engagement rather than single transactions, leveraging consumer preferences for relevance and control (Brey et al., 2007; Im & Ha, 2013; Zhang et al., 2017). This strategy not only reduces clutter and enhances targeting precision, but also respects consumer privacy and responds to growing demands for tailored communication, particularly in digital environments overwhelmed with unsolicited messages (Brey et al., 2007; DuFrene et al., 2005).

Trust is a foundational element in both social and economic interactions, serving to reduce complexity and uncertainty in human behavior (Bansal et al., 2016). In marketing, trust is not only essential for reducing perceived risks but also plays a strategic role in transitioning from transactional exchanges to long-term relationships. Its origins can be traced back to psychology and sociology, where it was initially viewed as a unidimensional construct centered on predictability and the absence of opportunism (Raimondo, 2000). Over time, marketing scholars adopted a more multidimensional perspective, recognizing trust as a combination of cognitive beliefs (e.g., competence and reliability) and affective elements (e.g., benevolence and care), which together foster stronger emotional bonds between brands and consumers (Hajli et al., 2017).

This evolving understanding of trust is particularly relevant in the context of permission-based marketing, where consumers must actively consent to sharing personal data with brands. In digital environments, where face-to-face interaction is absent, consumers rely heavily on their perception of a brand's trustworthiness when deciding whether to disclose personal information. Specific trust, developed through direct brand experience, complements general trust, which is rooted in individual predispositions and past social learning (Kenning, 2008). Studies have shown that higher levels of trust correlate with an increased willingness to provide personal information, suggesting that trust can mitigate privacy concerns and enhance consumer engagement, as well as data misuse (Norberg et al., 2007; Zsigmondová et al., 2021). This relationship is particularly important in online contexts, where trust can be operationalized through a company's reputation and the perceived integrity of its brand (Norberg et al., 2007). As such, fostering trust through

transparent communication, consistent behavior, and secure data practices is vital for encouraging consumer engagement and long-term loyalty in permission-based marketing strategies.

Trust transfer theory explains how trust can move from one entity to another through association, making it highly relevant in digital marketing and e-commerce settings where direct interactions are limited. In this framework, trust is transferred from a trusted third party to a new, less familiar entity when the two are closely connected and the third party strongly endorses the new entity (Zhao et al., 2019). For example, in consumer-to-consumer (C2C) commerce, trust in a platform or a third-party broker – such as one offering certificates or guarantees – can transfer to individual sellers or brands through this association, enhancing consumers' willingness to engage (Zhao et al., 2019). This mechanism is especially powerful in social commerce contexts where trust can be built through interpersonal connections and perceived social endorsement. In organizational settings, trust also acts as a moderator that enhances the positive effects of self-efficacy on job performance and satisfaction, suggesting that a high-trust environment amplifies beneficial behavioral outcomes (Ozyilmaz et al., 2018). As such, trust transfer theory not only highlights the importance of trust endorsements in marketing but also provides valuable insights into how trust can be cultivated and leveraged in both consumer and workplace environments.

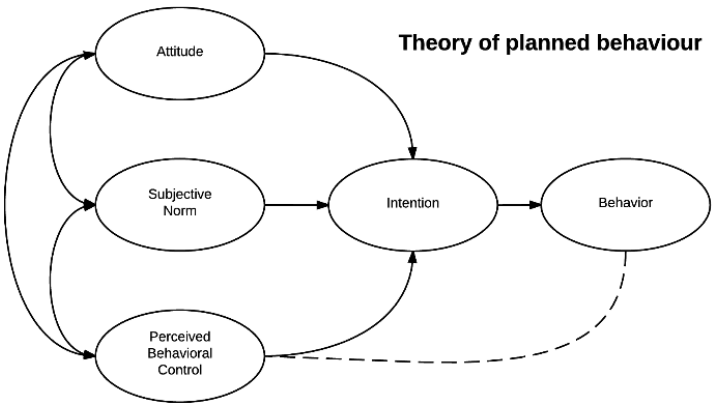
Social cognitive theory offers a dynamic perspective for understanding how trust emerges and evolves in marketing contexts by emphasizing the interplay between cognitive, behavioral, and environmental influences (Yakut, 2019). Unlike models that view trust as a fixed trait or solely rational decision, this theory frames trust as a product of learning through social interaction and experience. Factors such as self-efficacy, perceived control, and environmental feedback are central to how individuals evaluate the trustworthiness of brands and marketing messages (Schunk & DiBenedetto, 2020). In the context of permission-based marketing, this perspective allows researchers to investigate how consumers' internal motivations and past experiences with brands shape their willingness to disclose personal data. As individuals observe others engaging with trustworthy brands or receive consistent and positive feedback, their trust in those brands is likely to increase over time (Castelfranchi & Falcone, 2011).

When applied to marketing, social cognitive theory highlights the importance of reciprocal influence in trust formation. Consumers are not passive recipients of brand messaging; rather, they actively interpret and react to marketing cues based on personal and social experiences. This understanding enables marketers to craft strategies that reinforce trust through behavioral modeling, peer validation, and credible brand actions (Yakut, 2019). For instance, user-generated content and testimonials can act as social proof, aligning with consumers' observational learning processes. Moreover, environmental cues - such as privacy settings, transparent communication,

and data protection assurances - can serve as external reinforcers that support trust development. By aligning trust-building efforts with the principles of social cognitive theory, businesses can foster deeper consumer relationships and enhance voluntary data disclosure in digital environments.

Some researches used Theory of Reasoned Action to demonstrate that obtaining consent for mobile advertising fosters a favorable consumer attitude, which in turn enhances consumers' willingness to accept mobile advertisements, ultimately influencing their actual behavior (Tsang et al., 2004). Some other authors employed the foundations of the Theory of Planned Behavior (figure 1) to investigate the significance of perceived behavioral control within the realm of permission-based marketing research (Bamba & Barnes, 2007; Jayawardhena et al., 2009). They contend that when consumers feel they have more authority over opt-in parameters, such as timing, location, and advertisement frequency, they are more inclined to authorize the reception of SMS advertisements.

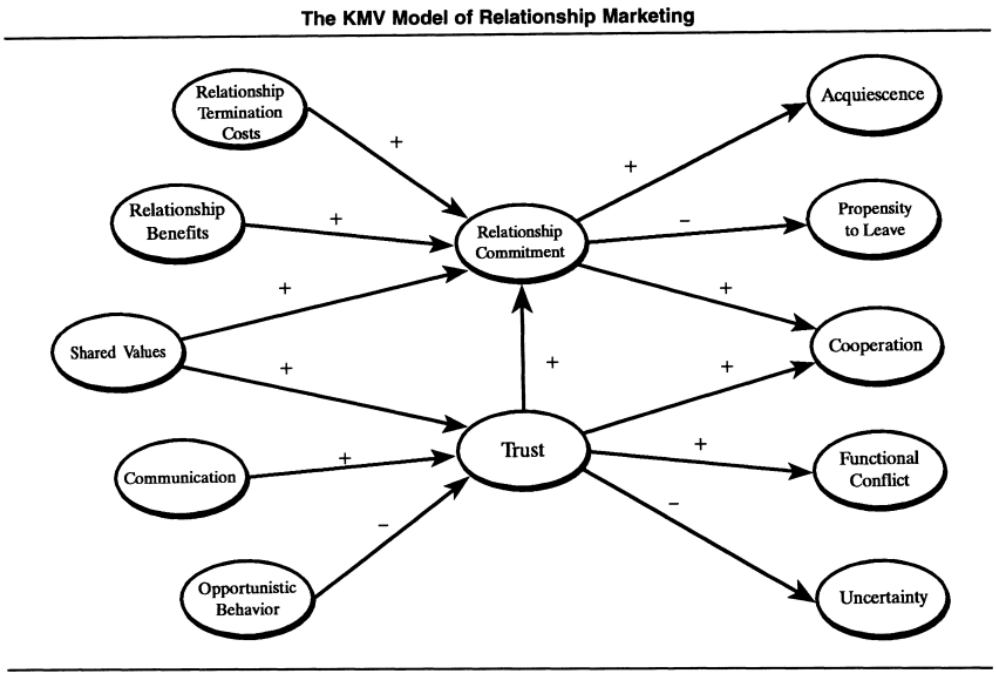
Figure 1. *Theory of planned behaviour model by Ajzen (1985)*



Other authors used Commitment-Trust Theory (figure 2) and proposed that successful relationship marketing, which focuses on long-term interactions and mutual benefit, requires two fundamental elements: commitment and trust (Morgan & Hunt, 1994). Commitment is defined as a desire to maintain a valued relationship, while trust is seen as the confidence in the exchange partner’s reliability and integrity. Author‘s findings underscore the central role of commitment and trust in fostering successful relationships, emphasizing their impact on efficiency, productivity, and effectiveness in marketing exchanges. They as well emphasize the importance of confidence in the trust construct, suggesting that confidence arises from a firm belief in the exchange partner's

reliability and integrity, which are associated with qualities like consistency and competence. So while trust is crucial for commitment (Morgan & Hunt, 1994), over-commitment might have negative impacts on trust (Brown et al., 2019).

***Figure 2**. Morgan and Hunt's (1994) Model Based on Commitment-Trust model*



Morgan and Hunt (1994) argue that conceptualization of trust underscores its importance in relationship marketing, where the focus is on long-term interactions and mutual benefit – trust directly impacts customer willingness to maintain a relationship with a brand. Consequently, the hypotheses proposed by Morgan and Hunt (1994) regarding the existence of a positive correlation between shared values and trust, a positive correlation between communication and trust, a negative correlation between opportunistic behavior and trust, a positive correlation between trust and relationship commitment, a positive correlation between trust and cooperation, and a positive correlation between trust and functional conflict were substantiated during their investigation (Morgan & Hunt, 1994). However, there is a call for further empirical work to confirm the applicability of the commitment-trust theory across various forms of relationship marketing beyond the current sample. While the model of Commitment-Trust Theory implies a linear relationship between trust, commitment, and successful marketing relationships - however, real-world business relationships can be more complex and non-linear, influenced by a multitude of fluctuating factors, such as, for example, trust in government and perceived data privacy.

The success of permission-based marketing also hinges on the design of its processes, such as simplifying registration and clearly communicating data usage policies. These measures help alleviate privacy concerns, a common barrier to consumer participation. Trust, perceived relevance, and the value of communications are key drivers of data-sharing willingness, outweighing financial incentives like monetary rewards or lotteries (Fernandes et al., 2017, 2021). Tailored communication, enabled by interactive and customizable platforms, empowers consumers, mitigates privacy concerns, and fosters a trusting relationship between consumers and marketers (Watson et al., 2013a).

According to Swain et al. (2023), the effectiveness of marketing communication in permission marketing relies on several factors (figure 3). Well-crafted and relevant promotional messages foster positive consumer relationships, while informative content enhances perception without being intrusive. Proper frequency and timing of message delivery are as well crucial for engagement. Consumer-related factors such as trust and credibility in the marketer, innovativeness, ease of technology use, and perceived behavioral control significantly influence attitudes toward permission marketing (Swain et al., 2023). Innovative consumers, especially those comfortable with technology, are more likely to respond favorably when they feel in control of communication parameters. However, privacy concerns and the risk of personal data misuse remain substantial barriers, underscoring the importance of addressing these issues in marketing campaigns (Swain et al., 2023). Lastly, enjoyment, entertainment value, and the tangible utility of marketing messages play a vital role in driving consumer engagement, with messages offering clear benefits being more positively received (Swain et al., 2023).

Figure 3. *Conceptual framework for permission marketing by Swain et al. (2023)*

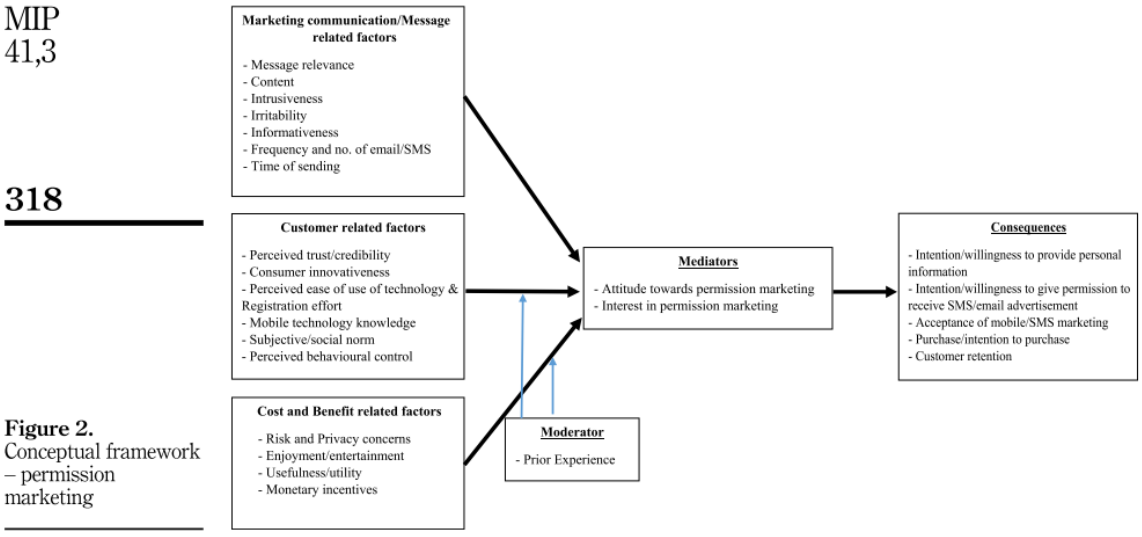


Figure 2.
Conceptual framework – permission marketing

Ultimately, permission-based marketing represents a paradigm shift toward consumer-centric strategies. By emphasizing consent and trust, marketers can enhance engagement and loyalty while addressing the delicate balance between privacy concerns and the benefits of data sharing. As digital marketing evolves, transparency, consumer empowerment, and trust will remain fundamental to effective marketing strategies (Brey et al., 2007; Krafft et al., 2017; Zhang et al., 2017). Therefore trust in brand, risk and privacy concerns and perceived benefits, as well as environmental-influential factors such as trust in government and technologies are the main subjects of this literature review.

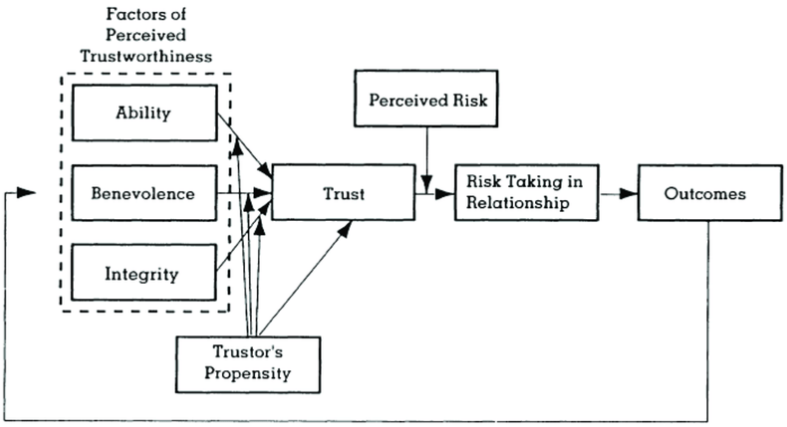
1.1.2. Trust in Brand and Permission-Based Marketing

Trust is a cornerstone of permission-based marketing, fundamentally shaping consumers' willingness to disclose personal information and opt in to receive brand communications. This trust can be both personal-stemming from direct experiences or recommendations, and institutional-rooted in a company's transparency, privacy policies, and demonstrated integrity (Watson et al., 2013). In mobile and online environments, where interactions are highly personal and privacy concerns are amplified, trust becomes even more critical (DuFrene et al., 2005; Theocharidis et al., 2020a; Watson et al., 2013). For permission marketing to be effective, brands must consistently deliver relevant and engaging content while ensuring that communications remain respectful and non-intrusive. This includes providing clear explanations about data usage and giving users control over their information. The notion that consumers are cautious about how their personal information is managed and prefer to engage with brands they trust is echoed in more studies. Some authors highlight that trust, both personal and institutional, significantly influences consumers' willingness to grant permission for mobile marketing, as consumers are wary of data misuse and the potential for their information to be shared with third parties (Jayawardhena et al., 2009; Watson et al., 2013). By fostering trust through transparency and responsible data handling, marketers can encourage consumers to actively participate in permission-based marketing and build lasting relationships.

An Integrative Model of Organizational Trust by Mayer et al. (1995) examines the factors that contribute to the development of trust within organizations (figure 3). They propose that trust is primarily influenced by three key attributes: ability, benevolence, and integrity. „Ability is that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain.“, „Benevolence is the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive“, „The relationship between integrity and trust involves the trustor's perception that the trustee adheres to a set of principles that the trustor finds

acceptable.“ (Mayer et al., 1995). These factors collectively shape the foundation of trust in organizations, influencing interpersonal and institutional dynamics.

***Figure 4**. Integrative Model of Organizational Trust by Mayer et al. (1995)*



Their model importantly delineates the difference between the willingness to take risks (trust) and the actual act of taking risks (trusting behavior) – this delineation is essential as it underscores that trust is not just about taking risks, but also about the confidence in relying on another party. So according to Mayer et al. (1995), this distinction is key to understanding organizational interactions, as trust influences decision-making, collaboration, and overall functionality within institutions. However, their model was developed within the context of organizational behavior, which may limit its direct applicability to other contexts or environments where trust dynamics might differ, such as customer-brand relationships. They also suggest that future research should focus on the evolving nature of permission marketing, particularly in the context of rapidly changing online communication technologies. This includes examining how these technologies impact consumer behavior and the effectiveness of permission marketing strategies.

The contextualization of trust theories highlights the importance of understanding the specific environments in which trust operates. In permission marketing, the context can significantly affect the antecedents and consequences of trust. For instance, trust in a brand may be influenced by the sensitivity of the information being requested and the consumer's previous experiences with privacy invasions (Bansal et al., 2016). Theories such as the Theory of Reasoned Action and Prospect Theory (figure 1) suggest that trust and privacy concerns are context-

dependent, with certain antecedents of trust being more significant in specific contexts, such as financial transactions or health-related disclosures (Bansal et al., 2016). This context sensitivity implies that brands must tailor their trust-building strategies to the specific circumstances of their marketing efforts, ensuring that they address the unique concerns and expectations of their target audience.

Moreover, the interplay between trust and personality traits can further complicate the dynamics of permission marketing. Research shows that individual differences, such as extroversion and agreeableness, can influence how consumers perceive and respond to trust cues in marketing communications(Bansal et al., 2016). Trust is not only a function of the brand's actions but also of the consumer's personality and the context in which the interaction occurs. This suggests that brands should consider both the context of their marketing efforts and the personality traits of their audience when designing trust-building strategies. By doing so, they can enhance the effectiveness of their permission marketing campaigns, fostering deeper consumer relationships and encouraging more meaningful engagement with their brand.

As mentioned before, trust in a brand plays a crucial role in shaping consumer behavior and fostering brand loyalty. However, trust extends beyond the tangible aspects of product quality, encompassing the emotional and psychological bonds that consumers form with a brand. These connections influence their willingness to continue engaging with the brand, even in the face of competition. Some authors highlight that trusted brands not only enjoy repeat purchases but also foster a deeper level of consumer commitment, contributing to both purchase loyalty (behavioral loyalty) and attitudinal loyalty (emotional attachment) (Chaudhuri & Holbrook, 2001). Same authors further elaborate on the role of trust in reducing uncertainty. By creating a sense of commitment and security, trust encourages consumers to engage in repeated interactions with the brand (Chaudhuri & Holbrook, 2001). This process often involves behaviors that imply vulnerability, such as relying on the brand for essential services or sharing personal data. Positive emotional engagement, referred to as brand affect, is equally critical in strengthening this relationship. Emotions such as joy, satisfaction, or pleasure create a bond that increases consumer willingness to support the brand. These affective responses not only drive attitudinal loyalty but also foster behaviors such as data-sharing, especially when consumers believe that the brand has their best interests at heart (Chaudhuri & Holbrook, 2001). In contexts like digital marketing and governmental policies, these emotional and trust-based connections are vital for encouraging consumers to disclose personal data or engage with online platforms.

An additional factor in building brand trust is the alignment of values and differentiation. Some authours underscore the importance of perceived uniqueness and shared values in

establishing trust (Chaudhuri & Holbrook, 2001). When consumers view a brand as offering unique benefits or reflecting their personal values, they are more likely to trust and engage with it (Chaudhuri & Holbrook, 2001; Urbonavicius et al., 2021b)(Chaudhuri & Holbrook, 2001). This dynamic extends to data-sharing behaviors, where trust serves as the foundation for consumer willingness to provide personal information.

The importance of trust becomes even more pronounced in the context of e-commerce, where uncertainty and risk are inherent. Online environments lack the tactile and visual cues that consumers rely on in physical stores, making trust a crucial element in consumer-marketer relationships. Some researchers argue that trust mitigates perceived risks and behavioral uncertainty, creating a more secure environment for consumers to engage in online transactions (Pavlou, 2003). So in e-commerce, trust in web retailers is essential for influencing purchase intentions and alleviating fears of opportunistic behavior by sellers. This makes trust-building an indispensable strategy for brands operating in digital marketplaces, where consumers often face heightened skepticism.

Beyond direct interactions with products or services, trust also involves broader perceptions of a brand's values, intentions, and overall reputation. It is a psychological state that includes vulnerability and positive expectations regarding the brand’s behavior. These expectations are shaped by several factors, including the brand’s communication strategies, transparency, and the perceived competence of the brand in delivering high-quality content (Colesca, 2009; Karjaluoto et al., 2008). For instance, brands that communicate consistently and honestly about their values and commitments are more likely to gain and maintain consumer trust (Brown et al., 2019; Hajli et al., 2017; Popova et al., 2019).

Moreover, the effectiveness of permission marketing is closely tied to the brand's ability to maintain a positive relationship with consumers. This involves not only obtaining initial permission, but also continuously reaffirming it through relevant and engaging communications. As consumers become overwhelmed with marketing messages, they may begin to perceive permission-based marketing emails as spam unless the content remains valuable and personalized. Therefore, brands must focus on delivering messages that resonate with consumers' interests and expectations to sustain trust and engagement over time (DuFrene et al., 2005).

1.2.Balancing Trade-offs in Data Disclosure Decisions

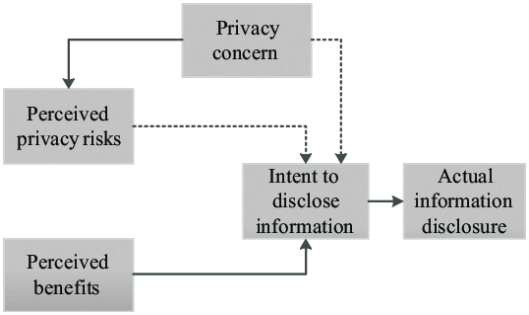
1.2.1. Insights from Privacy Calculus Theory and Trust Dynamics

Privacy concerns arise from a complex interplay of factors, including the unauthorized collection, disclosure, or use of personal information, particularly in the context of online transactions and digital interactions. The erosion of anonymity facilitated by the internet has heightened these concerns, making it increasingly difficult for consumers to engage in online activities without revealing personal data (Penaloza, 2006). The perception of privacy risks is influenced by various elements, such as the type of personal information collected, the level of control consumers have over their data, and the potential consequences of data misuse (Penaloza, 2006).

Additionally, privacy concerns are shaped by individual characteristics, such as a person's disposition to value privacy, which can vary based on cultural, social, and personal factors (Xu et al., 2008). These concerns are dynamic and context-dependent, often influenced by situational cues like the reputation of a website or the presence of privacy assurances such as third-party certifications (Li, 2014). External factors, including user interface design and the framing of privacy policies, can also manipulate privacy preferences, either heightening or alleviating concerns (Acquisti et al., 2015). Moreover, sensitivity to the type of information requested plays a critical role. Individuals are generally more hesitant to share sensitive information such as financial or health data compared to less sensitive demographic information (Rohunen et al., 2020). Addressing these multifaceted privacy concerns is crucial for companies aiming to foster consumer trust and encourage data-sharing behaviors.

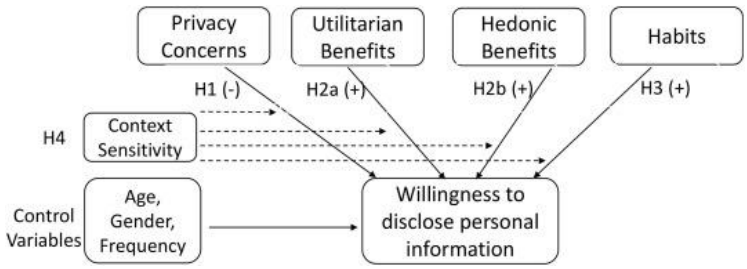
The concept of privacy calculus plays a pivotal role in understanding how privacy concerns are formed. According to this theory (figure 5), individuals conduct a cost-benefit analysis when deciding whether to disclose personal informal risks (Fernandes & Pereira, 2021; T. Wang et al., 2016). Privacy calculus theory suggests that disclosure is more likely when the perceived benefits, such as personalized offers or services, outweigh the anticipated privacy risks. Kurtz et al. (2021) employed this framework to explain consumers' willingness to disclose information in response to permission-based mobile advertising.

***Figure 5**. Privacy Calculus Theory by Laufer, R.S. and Wolfe, M. (1977)*



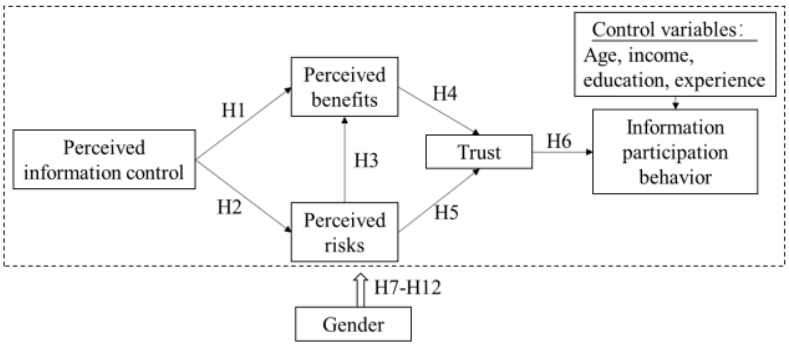
Building on this, Fernandes (2021a) proposed a framework where privacy concerns negatively impact willingness to disclose, while utilitarian and hedonic benefits, along with habitual behaviors, positively influence disclosure intentions (Figure 6). Context sensitivity plays a moderating role, affecting the strength of these relationships. Control variables such as age, gender, and interaction frequency further influence disclosure behaviors.

***Figure 6.** Modified Privacy Calculus Theory Framework with Emotional and Behavioural aspects (Fernandes & Pereira, 2021)*



Similarly, Luo (2023) presented a framework where perceived information control reduces perceived risks and enhances perceived benefits, both of which influence trust (Figure 7). Trust, in turn, significantly predicts individuals' information participation behavior. The model also shows that gender moderates several relationships, while demographic characteristics such as age, income, education, and experience serve as important control variables.

Figure 7. *Modified Privacy Calculus Theory Framework with Focus on Trust (Luo et al., 2023)*



However, privacy calculus is not purely rational. Kehr et al. (2015) and Treiblmaier and Chong (2011) criticized the Privacy Calculus Theory for overemphasizing rationality, neglecting psychological and emotional factors such as heuristics, bounded rationality, and affective states. This aligns with the "privacy paradox," which highlights the discrepancy between individuals' expressed concerns about privacy and their actual data-sharing behaviors (Norberg et al., 2007). Often, individuals disclose more information than intended when motivated by perceived benefits or habitual behaviors.

Trust plays a crucial mediating role in the privacy calculus, influencing the perceived risks and benefits associated with information disclosure (Fernandes & Pereira, 2021; Penaloza, 2006). When trust is established, individuals are more likely to focus on the benefits of sharing data, thereby mitigating privacy concerns. Trust is particularly vital in digital environments, such as e-commerce, where interactions frequently involve unfamiliar vendors (Penaloza, 2006). Trust can be cultivated through various means, including a strong website reputation, third-party certifications, and positive consumer experiences (Penaloza, 2006). Establishing these trust signals reduces perceived risks and increases consumers' willingness to disclose personal information. Furthermore, the perception of control over personal data enhances trust, making consumers more comfortable with sharing information (Krafft et al., 2017; Luo et al., 2023; Theocharidis et al., 2020; Watson et al., 2013).

The decision-making process surrounding privacy is also heavily influenced by emotional and irrational factors. Habitual behaviors can lead to automatic, non-conscious disclosure decisions that override deliberate cost-benefit assessments (Fernandes & Pereira, 2021). Emotional responses such as fear of data misuse and loss of control can heighten privacy concerns and deter information sharing (Krafft et al., 2017). Conversely, positive emotional experiences - such as perceiving benefits like personalized content and entertainment value - can encourage data sharing (Krafft et al., 2017). Permission-based marketing, which requires explicit consumer

consent before sending promotional messages, hinges significantly on emotional factors. Trust, perceived control, and emotional engagement are critical in reducing privacy concerns and increasing the likelihood of consumer consent (Carroll et al., 2007; Krafft et al., 2017; Watson et al., 2013).

Context sensitivity significantly moderates the privacy calculus, as individuals weigh costs and benefits differently depending on situational and environmental factors (Fernandes & Pereira, 2021; Luo et al., 2023; Penaloza, 2006). Trust and privacy concerns fluctuate based on specific contexts and individual characteristics. For example, gender differences also impact privacy decision-making processes. Research indicates that females are generally more sensitive to perceived risks and more risk-averse, while males focus more on perceived benefits and task-oriented outcomes (Luo et al., 2023). Age is another relevant demographic factor. Teenagers, for example, are more willing to disclose profile data (e.g., age, gender, hobbies) than sensitive contact information (e.g., home addresses, phone numbers) (Walrave & Heirman, 2013). Their willingness to disclose personal information is often influenced by perceived benefits and mitigated by privacy concerns. Similarly, adults in e-commerce settings may become more comfortable disclosing information over time as they perceive less risk (Robinson, 2016) . These findings further highlight the importance of understanding demographic differences when addressing privacy concerns.

Effective management of privacy concerns is essential for businesses seeking to increase consumer willingness to disclose personal information. Communicating data protection measures, providing transparent privacy policies, and granting consumers control over their personal data are critical strategies (Boerman et al., 2021; Krafft et al., 2017; Tezinde et al., 2002). For instance, allowing consumers to manage message frequency and type fosters a sense of control, enhancing trust and acceptance of mobile marketing communications (Carroll et al., 2007; Watson et al., 2013).

Addressing the privacy paradox also requires efforts to reduce the perceived risks associated with data sharing. Sensitivity to the nature of requested information and offering clear, credible assurances about data usage can significantly impact consumers' willingness to disclose (Norberg et al., 2007; Olivero & Lunt, 2004; Rohunen et al., 2020). Ultimately, fostering trust, ensuring transparency, and maintaining consumer control are crucial for mitigating privacy concerns and encouraging open information-sharing practices. Robust data protection measures, coupled with effective communication, can enhance marketing effectiveness and build stronger, more sustainable consumer relationships (Beldad et al., 2011; Bhatia, 2020; Krafft et al., 2017).

1.2.2. Types of Consumer‘s Personal Data Disclosed in Permission-based Marketing

Consumers' willingness to disclose their personal data with brands for permission-based marketing largely depends on two key factors: the type of data requested and the context in which the data is being requested. Addressing these factors effectively is crucial for marketers seeking to gain consumer permission while respecting privacy concerns. Gaining consumer permission involves addressing several critical elements, including building trust, ensuring personalization, adhering to regulatory standards, and providing consumers with a sense of control over their information. Trust in the company requesting the data plays a central role. Consumers are significantly more likely to disclose personal information when they trust the brand’s reputation and perceive transparency in how their data will be used (Theocharidis et al., 2020; Watson et al., 2013). Moreover, control mechanisms, such as privacy settings and clear consent options, further empower consumers, making them feel more secure when sharing their data (Anic et al., 2019; Bhatia, 2020).

Personalization and relevance are major advantages of permission-based marketing. By collecting and analyzing consumer data, companies can tailor communications to better align with individual interests and needs (Bhatia, 2020; Rowley, 2004). Increased relevance enhances the effectiveness of marketing campaigns and reduces the perception of intrusiveness (DuFrene et al., 2005; Jolley et al., 2013). However, when data collection feels intrusive or fails to offer a clear consumer benefit, individuals become less willing to disclose their information (Bhatia, 2020; Norberg et al., 2007). Despite general concerns about privacy, many consumers still disclose personal data when they perceive immediate benefits, such as discounts, access to exclusive content, or personalized offers – a phenomenon known as the "privacy paradox" (Wakefield, 2013). This behavior reflects the complex interplay between privacy concerns, perceived rewards, and trust in the data-collecting entity.

In permission-based marketing, various types of personal data are typically requested to facilitate personalized communication and offers. Commonly collected information includes contact details like email addresses and phone numbers, demographic data such as age, gender, and location (Abashidze, 2023; Im & Ha, 2013; Krafft et al., 2017; Rowley, 2004). Contact information, such as email addresses and phone numbers, is crucial for delivering personalized marketing messages directly to the consumer's preferred communication channel (Jolley et al., 2013; Theocharidis et al., 2020). Additionally, demographic data, such as age, gender, and location, helps marketers understand their audience and tailor marketing efforts accordingly, allowing for better audience segmentation and more targeted campaigns (Theocharidis et al., 2020a; Watson et al., 2013). Moreover, behavioral data, such as past purchase history and

browsing patterns, allows marketers to predict future consumer behavior and preferences, thereby enhancing the relevance of marketing communications (Rowley, 2004). Consumers may also share preference data, including explicit preferences about the type of content they wish to receive, the frequency of communications, and the preferred channels, which helps ensure that marketing messages align with consumer expectations and avoid being perceived as intrusive (Theocharidis et al., 2020; Watson et al., 2013). Social networking data, including user interests, followers, and engagement metrics, allows brands to better understand consumer behavior and engage with users on their preferred platforms, further enhancing marketing relevance (Theocharidis et al., 2020). Live location data (geolocation) offers the ability to target consumers in real-time, providing immediate benefits such as local promotions or notifications based on a consumer's current location (Im & Ha, 2013).

However, consumers' willingness to disclose personal information varies depending on the sensitivity of the data. Studies have shown that individuals are generally more willing to disclose demographic and lifestyle information, such as age, hobbies, or favorite products, compared to more sensitive information like home addresses or phone numbers (Walrave & Heirman, 2013). Particularly among younger demographics, such as teenagers, there is a noticeable preference for sharing profile-related information over direct contact data, reflecting a broader trend observed across different age groups (Walrave & Heirman, 2013).

Therefore, we can clasify these types of personal data, that are disclosed for permission-based marketing (Table 1). These types of personal data are integral to permission-based marketing, allowing businesses to create targeted and personalized marketing campaigns while respecting consumer privacy preferences.

Table 1. *Types of Consumer's Personal Data in Permission-Based Marketing. Made by the Author of the Thesis*

Types of Data	Examples	Purpose in Permission-Based Marketing	Data Sensitivity
Contact Information	Name, Email address, Phone number, Home adress	Used to identify and contact consumers; essential for account creation, transactions, and personalized offers. Often required as a prerequisite for service delivery	Low to moderate – consumers view this data as necessary for accessing services or participating in online activities (Ashworth & Free, 2006; Robinson, 2016; Swain et al., 2023)

Demographic Data	Age, Gender, Education level, Location from	To understand the audience and tailor marketing efforts, segment audiences, and create targeted campaigns	Low to moderate – often lower for less sensitive data like age and gender (Bamba & Barnes, 2007)
Online Behavioral Data / Cookies	Browsing History, Purchase History, Website Visits	Allows for tracking and analyzing consumer habits to refine marketing strategies. Drives behavioral advertising and dynamic content delivery	High to moderate – decreases with perceived benefits and personalized offers (Im & Ha, 2013)
Social Networking Data	Interests, Likes, Social Connections	Enables highly personalized advertising and targeted recommendations. Often used to strengthen brand-consumer relationships through relevant social interactions	Low to moderate – freely shared due to reciprocal nature of social platforms and perceived control over visibility (Urbonavicius et al., 2021; Zimaitis et al., 2022)
Preferences Data of Receiving Content methods	Content preferences, Frequency of communication preferences, Preferred communication channels	To ensure marketing messages align with consumer expectations and avoid intrusiveness	Low – it helps to ensure relevance and reduces perceived intrusiveness (Krishnamurthy, 2001; Olivero & Lunt, 2004; Watson et al., 2013)
Profile and views data	Hobbies, Faith orientation, Political orientation, Relationship status, Favourite brands	Enables deeper audience segmentation and personalization by understanding consumer values, interests, and preferences; supports tailored messaging and brand positioning	Moderate – perceived as less moderatly, but may trigger concerns when related to political or faith orientation (Heirman et al., 2013)
Medical data	Health conditions, Medical history, Medications	Useful for highly tailored health-related marketing and recommendations (e.g., wellness apps, fitness plans, pharmaceutical offers)	High – seen as highly sensitive; users fear misuse or discrimination based on health data (Ashworth & Free, 2006; Olivero & Lunt, 2004)
Financial data	Income level, Loans information, Transaction history, Investment portfolio details	Essential for financial services, personalized offers, and credit evaluations; allows precise targeting for financial products	High – highly sensitive; often triggers strong privacy concerns and reluctance to share (Ashworth & Free, 2006; Olivero & Lunt, 2004)

Live Location Data	Geolocation, Location-based Marketing Data	Used for targeted mobile marketing campaigns or some services	High – it can be interpreted as privacy invasion (Im & Ha, 2013)

In conclusion, the decision to disclose personal data in permission-based marketing results from a careful evaluation of trust, perceived benefits and risks, control over personal information, and the sensitivity and context of the data request. Businesses aiming to implement successful permission-based marketing strategies must prioritize transparency, offer meaningful value, and respect consumer privacy preferences to foster stronger, trust-based relationships with their audiences. As technology and regulatory landscapes evolve, businesses must continue adapting their practices to maintain consumer trust and encourage data sharing.

1.3. Environmental-influential Factors on Privacy concerns and Data Disclosing Decisions

1.3.1. The Influence of Trust in Government (perceived regulatory effectiveness) on Privacy Concerns and Willingness to Disclose Data for Marketing Purposes

Trust in government, defined as the belief that government institutions and regulators effectively protect personal information, plays a crucial role in shaping individuals' privacy concerns and their willingness to disclose personal data for marketing purposes (Miltgen & Smith, 2015; Trein & Varone, 2024; N. Wang et al., 2022). Perceived regulatory effectiveness, or the belief that legal safeguards – such as data protection laws and policies – are strong and reliable, reduces individuals' fears that their data will be misused or mishandled (Degutis et al., 2020; Urbonavicius et al., 2021; Zimaitis et al., 2022). Empirical studies consistently demonstrate that higher trust in government correlates with lower privacy concerns, as individuals feel more secure when regulations are seen as effective (Herian et al., 2014; Miltgen & Smith, 2015; Trein & Varone, 2024). This trust acts as a psychological buffer, allowing individuals to feel protected and to believe that their privacy will be respected and safeguarded (Trein & Varone, 2024; N. Wang et al., 2022).

When people believe that government regulations, such as the General Data Protection Regulation (GDPR), are robust and enforced effectively, they are more comfortable sharing personal information, including for marketing purposes (Urbonavicius et al., 2021; Zimaitis et al., 2022). For instance, Zimaitis et al. (2022b) found that perceived regulatory effectiveness significantly alleviates privacy concerns, fostering greater willingness to participate in digital activities and disclose data. Similarly, Trein & Varone (2024) emphasized that trust in government

enhances individuals' willingness to share personal data for public policy purposes, as people assume risks are minimized when regulations are seen as strict and well-enforced.

Privacy concerns arise from fears of data misuse, identity theft, and unauthorized access, which are heightened when individuals lack confidence in the government's ability to protect their information (Degutis et al., 2020; Miltgen & Smith, 2015; N. Wang et al., 2022). Conversely, when trust is high, people are less likely to engage in defensive behaviors, such as withholding information or avoiding digital services (Degutis et al., 2020; Miltgen & Smith, 2015). This reduction in privacy concerns translates into greater openness to data sharing, including for marketing and other commercial purposes, as trust functions as a heuristic that reduces the perceived need for constant risk assessment (Norberg et al., 2007).

Several authors highlight that trust in government, as an expression of perceived regulatory effectiveness, creates a sense of security, encouraging individuals to share their data without fear of misuse (Herian et al., 2014; Trein & Varone, 2024; N. Wang et al., 2022). For example, Herian (2014) found that high trust in government leads to greater support for data-sharing initiatives, particularly in sensitive areas like healthcare. Trein (2024) similarly argued that effective regulatory oversight reduces citizens' worries and increases their willingness to engage in data sharing for public purposes.

Moreover, transparency and communication from government institutions play a critical role in building trust and reducing privacy concerns (Song & Lee, 2016; Trein & Varone, 2024). Song (2016) demonstrated how transparency through social media enhances trust in government by making citizens feel informed and secure, although the study did not directly examine the link to privacy concerns. Nonetheless, Trein (2024) and Wang, N. (2022) argue that transparency, coupled with strong regulatory frameworks, strengthens trust and alleviates fears about data misuse.

While most studies emphasize that trust in government lowers privacy concerns, some caution that the effect of trust may vary depending on the type of data involved (Degutis et al., 2020). Degutis et al. (2020) noted that trust in government may reduce concerns for less sensitive data, but this relationship may weaken when it comes to more intimate information, such as social network details. Thus, while perceived regulatory effectiveness generally reduces privacy concerns and encourages data sharing, its impact can differ depending on the context and data type.

In summary, the literature consistently highlights that trust in government, operationalized through perceived regulatory effectiveness, is a key factor in mitigating privacy concerns and

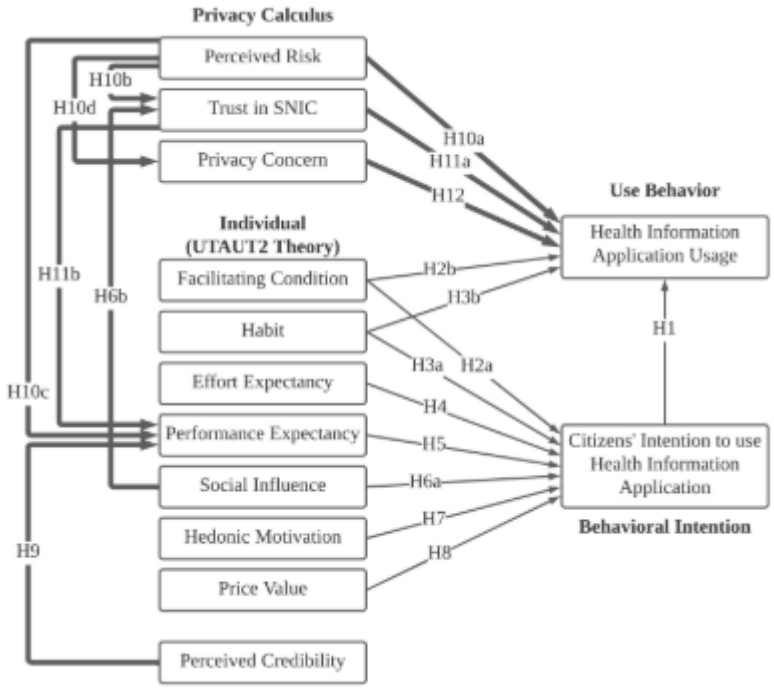
fostering individuals' willingness to disclose data for marketing purposes (Miltgen & Smith, 2015; Trein & Varone, 2024; N. Wang et al., 2022; Zimaitis et al., 2022b). Strong, transparent, and enforceable regulatory frameworks build confidence in data protection systems, reducing fears of misuse and encouraging greater engagement in data-driven services (Degutis et al., 2020; Herian et al., 2014; Urbonavicius et al., 2021). Consequently, fostering trust through effective regulatory measures is critical for creating a digital environment where individuals feel safe to share personal data for marketing and other purposes.

1.3.2. The Role of Trust in Technologies on Privacy Concerns and Willingness to Disclose Data

Trust in technologies plays a critical and multifaceted role in shaping users' privacy concerns and their willingness to disclose personal data. According to Lankton et al. (2016), trust develops dynamically as users' initial expectations about technology are confirmed or disconfirmed through experience, shaping their intentions to continue using the system. Although this process explains technology reliance, Lankton et al. (2016) note that it does not directly address privacy concerns or data disclosure outcomes.

Building on this foundation, Hassan et al. (2022) define trust as the belief that technology will function correctly and protect user information, examining its impact within a model alongside privacy concerns and perceived risks (Figure 8). Their findings suggest that trust alone may not significantly reduce privacy concerns or directly influence technology use behavior, emphasizing that privacy worries negatively affect willingness to use technology and disclose data (Hassan et al., 2022). This indicates that trustworthy system design must be complemented by transparent data policies and robust legal protections to foster data disclosure (Hassan et al., 2022).

Figure 8. *Extended UTAUT2 Model with a Privacy Calculus Model by Hassan et al. (2022)*



Conversely, Venkatesh et al. (2012) highlight that when users perceive technologies as reliable and secure, their privacy concerns decrease, leading to greater willingness to share personal data. Trust, therefore, acts as a psychological bridge, reducing privacy wariness and encouraging disclosure, with mixed methods research recommended to comprehensively capture these effects (Venkatesh et al., 2012). Krafft (2017) similarly finds that while trust may not directly increase willingness to disclose data, it mitigates privacy concerns, indirectly supporting data-sharing decisions when consumers expect responsible data handling.

Im & Ha (2013) underscore the role of social influence alongside trust, showing that peer acceptance enhances trust, which in turn reduces perceived privacy risks and increases willingness to share sensitive data, such as location information, vital for permission-based marketing. Similarly, Colesca (2009) notes that trust in the reliability and security of technology correlates positively with reduced privacy concerns and greater readiness to share personal information in online services, though the link between trust and reduced privacy risk is mostly inverse and implied.

Kumar et al. (2014) argue that prior positive interactions and trust-building measures – such as privacy audits and transparency – reduce privacy concerns and enhance users' confidence to disclose data, thereby improving marketing outcomes. Metcalfe et al. (2023) expands this view by emphasizing that trust encompasses perceptions of organizational competence, honesty, and

empathy, which reduce fears of misuse and encourage data sharing across domains, from aviation safety to digital platforms. Transparency and ethical behavior are key in reinforcing this trust and its beneficial cycle (Metcalfe et al., 2023).

Hajli et al. (2017) and Theocharidis et al. (2020) further illustrate how trust reduces perceived risks on social commerce platforms and online hotelier services, respectively, by fostering confidence in data protection, supported by regulatory compliance such as GDPR. Their work highlights that transparent privacy policies and trustworthy service provider behavior increase users' willingness to consent to personal data use for marketing.

Pavlou (2003) similarly states that trust diminishes perceived economic, personal, and privacy risks by signaling security commitments like encryption and clear data policies, which reassures users and promotes personal data disclosure in e-commerce contexts. Robinson (2016, 2018) corroborates these findings by showing that trusted platforms reduce users' mental burden of evaluating privacy risks, balance perceived benefits over risks, and increase willingness to share personal data. Certification marks and institutional trust also play important roles in this process, collectively encouraging positive attitudes toward data disclosure online (Robinson, 2016, 2018).

In summary, the literature consistently reveals that trust in technologies reduces privacy concerns and increases willingness to disclose personal data, though its direct effect on privacy concerns may vary depending on context and measurement (Hassan et al., 2022; Krafft et al., 2017; Lankton et al., 2016). Trust is often built and reinforced through transparent practices, social influence, regulatory compliance, and demonstrated organizational integrity (Hajli et al., 2017; Im & Ha, 2013; Metcalfe et al., 2023; Theocharidis et al., 2020). This trust lowers perceived risks and fosters safer, more confident data-sharing behaviors essential for effective permission-based marketing and e-commerce (Pavlou, 2003; Robinson, 2018; Venkatesh et al., 2012).

2. METHODOLOGY AND RESEARCH DESIGN FOR ASSESSING RELATIONSHIP OF TRUST WITH THE CONSUMER‘S WILLINGNESS TO DISCLOSE PERSONAL DATA TO BRANDS

2.1. Purpose of the Research, Research Model and Hypotheses of the Study

This section presents the methodological approach of the study, which is grounded in the theoretical insights discussed in the preceding chapters. The research model was developed based on a structured review of the relevant literature and draws primarily on Privacy Calculus Theory and its extensions, as well as Commitment–Trust Theory (Morgan & Hunt, 1994) and related trust-based frameworks applied in digital and marketing contexts (Fernandes & Pereira, 2021; Luo et al., 2023). These theoretical perspectives provide the foundation for examining how trust-related, contextual, and psychological factors shape consumers’ willingness to disclose personal data in permission-based marketing environments.

The proposed research model integrates trust in brand, trust in technologies, and trust in government, alongside privacy concerns, perceived control over personal data, and perceived benefits of personalization. The author’s research model is presented in **Figure 9**. The empirical investigation adopts a quantitative research design, using a structured online survey. Measurement constructs and questionnaire items were adapted from previously validated scales to ensure reliability and validity.

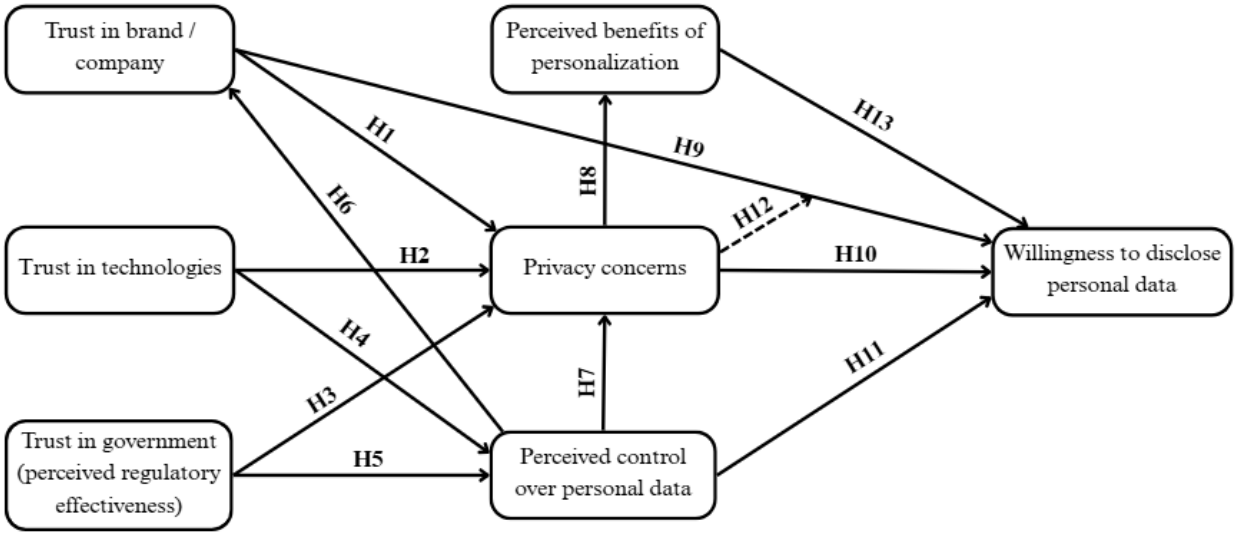
Research problem – How trust-related factors, privacy concerns, perceived benefits of personalization, and perceived control influence consumers’ willingness to disclose personal data in the context of permission-based marketing.

Aim of the research – To examine how trust in technologies, trust in government, and trust in brand, together with perceived control, privacy concerns, and perceived benefits, shape consumers’ willingness to disclose personal data to brands.

Research object – The personal data disclosure behavior of users interacting with UAB “Bolt Services” as an urban mobility service provider offering personalized services and communications.

In the theoretical part of the thesis, scientific literature and peer-reviewed studies related to trust, privacy, and personal data disclosure in permission-based marketing were analyzed. Based on this theoretical foundation, the research model was developed and hypotheses were formulated. The empirical part of the study was subsequently conducted using an online questionnaire to test the proposed relationships.

Figure 9. *Researh Model by Author of the Thesis*



H1: Higher trust in the brand reduces privacy concerns.

Research shows that when consumers trust a brand more, their worries about privacy go down because they feel confident that their personal data will be handled openly, honestly, and safely (Ashworth & Free, 2006; Beldad et al., 2011; Watson et al., 2013). Trusted brands are seen as reliable and fair, which makes consumers less anxious about their data being misused or accessed without permission (Ashworth & Free, 2006; Beldad et al., 2011; Watson et al., 2013). This trust helps reduce fears even if some data practices seem unclear and makes people more forgiving of occasional mistakes, trusting the brand will fix problems (Ashworth & Free, 2006). Giving consumers control over how their data is used, as in permission-based marketing, builds even more trust and lowers privacy concerns (Beldad et al., 2011; Watson et al., 2013). Positive experiences and consistent, ethical behavior from the brand over time strengthen trust, making consumers feel safer and more willing to disclose their personal data (Watson et al., 2013). Overall, the research supports the idea that higher trust in a brand lowers privacy concerns and encourages consumers to share their data in permission-based marketing.

H2: Higher trust in technologies reduces privacy concerns.

Several empirical studies provide partial or indirect support for the hypothesis that higher trust in technologies reduces privacy concerns. Pavlou (2003) reported a strong negative relationship between trust and perceived risk, suggesting that increased trust lowers concerns related to privacy. Similarly, Li (2014) found that website reputation, serving as a proxy for trust,

significantly reduces privacy concerns, especially for low-reputation websites, and that reduced privacy concerns enhance behavioral intentions. Penaloza (2006) also found that perceived ease of use and third-party security certificates significantly reduce privacy concerns, implying that trust-enhancing features lower user anxiety. S. C. Robinson (2018) showed that trust in the internet and institutions positively affects data disclosure attitudes, while privacy concerns reduce them, indirectly supporting the hypothesis. However, some studies report no significant direct link; for example, Hassan et al. (2022) found no statistically significant path from trust in a national ID system to reduced privacy concerns. Luo et al. (2023) confirmed that higher perceived risk decreases trust, but did not test the inverse relationship. Colesca (2009) treated trust and privacy concerns as independent influences on e-government trust, without establishing a causal link. Metcalfe et al. (2023) suggested that transparency and reliability reduce user hesitation. Overall, the hypothesis is supported by studies showing significant inverse relationships between trust and privacy concerns, though some studies only imply or partially support this connection.

H3: Higher trust in government (perceived regulatory effectiveness) reduces privacy concerns.

Empirical evidence consistently supports the hypothesis that higher trust in government – measured as perceived regulatory effectiveness – reduces privacy concerns. Beldad et al. (2011) found a strong negative relationship, showing that trust in the government's competence significantly lowers perceived privacy risks. Similarly, Hong et al. (2021) reported a smaller but significant effect, linking trust in privacy legislation to reduced internet privacy concerns. Lwin et al. (2007) demonstrated that manipulating perceived regulatory effectiveness significantly reduced privacy concerns, with most of the regulatory impact mediated by decreased concern. Urbonavičius et al. (2021) confirmed a negative indirect effect of perceived regulatory effectiveness on privacy concern via perceived lack of control, while Miltgen & Smith (2015) and Perdereaux-Weekes (2021) showed a direct negative effect between trust in regulators and lower risk perceptions. Pandey (2023) as well found statistically significant paths linking trust in government to improved privacy perceptions. Although some effects are modest, the overall findings affirm that trust in competent, protective regulation lowers consumer privacy concerns across contexts.

H4: Higher trust in technologies increases perceived control over personal data.

The literature suggests that trust in technologies reduces uncertainty and perceived risks, which strengthens users' sense of control over their personal information. When technological systems are seen as reliable, secure, and transparent, individuals feel less anxious about potential

data misuse and more confident in how their information is handled (Colesca, 2009; Penaloza, 2006; Venkatesh et al., 2012). Trust-enhancing elements such as third-party certifications and clear privacy assurances further lessen perceived vulnerability, reinforcing the perception that users can oversee and manage their data (Li, 2014; Penaloza, 2006). Trusted platforms also reduce the cognitive burden of evaluating privacy risks, allowing users to feel more empowered in overseeing their data (Robinson, 2016, 2018). Taken together, these findings indicate that higher trust in technologies supports a greater perception of control over personal data.

H5: Higher trust in government (perceived regulatory effectiveness) increases perceived control over personal data.

Urbonavičius et al. (2021) found that while trust in government enhances feelings of data safety, it may simultaneously reduce consumers' perceived control, as individuals shift responsibility to regulatory institutions. In contrast, Wang N. et al. (2022) emphasize that perceived regulatory effectiveness fosters security and confidence, enhancing consumers' sense of control over their data. Similarly, Wang H. et al. (1998) argues that when consumers trust the government to enforce privacy regulations, they feel more in charge of their personal information due to reinforced protections. Acquisti et al. (2015) support this by showing that visible government oversight increases individuals' agency and willingness to disclose data. Pandey (2023) further confirms that trust in transparent, secure e-governance systems boosts perceived control, with trust-related paths showing strong statistical significance.

H6: Higher perceived control over personal data increases trust in brand.

Research shows that perceived control over personal data is a central driver of trust in permission-based marketing. When consumers are able to manage how their information is used – such as adjusting message frequency or selecting preferred communication channels – they feel more empowered, which strengthens trust in the marketing relationship (Carroll et al., 2007; Watson et al., 2013). This sense of control also reduces perceived risks, supporting trust formation, as models demonstrate that perceived information control lowers risk perceptions and reinforces trust (Luo et al., 2023). More broadly, perceptions of control over personal data foster trust by increasing feelings of security and reducing privacy-related uncertainty (Krafft et al., 2017; Theocharidis et al., 2020; Watson et al., 2013). Additionally, research on regulatory effectiveness shows that reducing feelings of lacking control diminishes privacy concerns, which helps establish a more trusting relationship between consumers and organizations (Urbonavicius et al., 2021). Across these studies, perceived control consistently emerges as a condition that encourages trust, underscoring its importance in brand–consumer data interactions.

H7: Higher perceived control over personal data reduces privacy concerns.

Research findings largely support the hypothesis that more control over personal data reduces privacy concerns – perceived information control decreases perceived risks, uncertainty, and privacy invasion, encouraging data sharing (Luo et al., 2023). Similalry, in Penaloza (2006) research, one of the key hypotheses examined the relationship between factors that include aspects similar to "control" (i.e. perceived convenience, which can be interpreted as reflecting the ease and perceived control users experience) and the level of privacy concerns – the results indicated a significant negative relationship. Studies also show that transparent data practices and user autonomy – such as regulating communication frequency or opting out – lower anxiety and increase trust (Ashworth & Free, 2006; Watson et al., 2013). While most findings confirm this link, Bhatia (2020) challenges the assumption, reporting no significant effect of consumer empowerment on privacy concerns in permission-based marketing, suggesting that deeper fears may override perceived control.

H8: Lower privacy concerns increase perceived benefits of personalization.

Research consistently supports the hypothesis that lower privacy concerns increase the perceived benefits of personalization, as consumers who are less worried about data misuse tend to focus more on the utility and relevance of personalized offers (Krafft et al., 2017; Norberg et al., 2007). Reduced privacy concerns remove psychological barriers and enhance comfort with data sharing, which in turn boosts trust and leads to a greater appreciation of personalized marketing features such as tailored recommendations or time-saving promotions (Krafft et al., 2021; Norberg et al., 2007). Luo et al. (2023) confirmed this relationship empirically in the context of AI-based services, showing a significant negative effect of perceived risks on perceived benefits, further validating that minimizing privacy concerns allows users to experience personalization as helpful rather than intrusive.

H9: Higher trust in brand increases willingness to disclose data.

Research consistently supports the hypothesis that higher trust in a brand increases consumers' willingness to disclose personal data for permission-based marketing. Theocharidis et al. (2020) reports a statistically significant positive effect of trust in online hoteliers – conceptually akin to brand trust – on data-sharing willingness. Luo et al. (2023) finds an even stronger positive relationship between trust in AI-based medical platforms and users' information disclosure, highlighting trust's key role across contexts. Jayawardhena et al. (2009) further substantiates this, showing institutional trust significantly predicts willingness to disclose data in mobile marketing, especially among female consumers, emphasizing trust's influence through brand reputation and

transparency. Watson et al. (2013) and Popova et al. (2019) conceptually reinforce that trust – built via transparency, data handling, and quality content – increases perceived security and willingness to disclose, though without statistical validation. Krafft et al. (2017) also highlight trust's theoretical importance in reducing privacy concerns and promoting engagement but do not provide direct empirical effect sizes or p-values. Together, these findings demonstrate a robust link between brand trust and data-sharing willingness, with multiple studies providing significant effect sizes and p-values that validate trust as a critical driver in permission-based marketing.

H10: Higher privacy concerns reduce the willingness to disclose personal data.

Empirical research consistently demonstrates that higher privacy concerns directly reduce individuals' willingness to share personal data. Krafft et al. (2017) found that privacy concerns were the strongest negative predictor of permission-granting behavior in permission-based marketing. Their findings showed that as privacy concerns increase, the likelihood of consumers consenting to share their data decreases significantly. Similarly, Robinson (2016) confirmed that individuals who perceive a higher risk to their privacy are less inclined to disclose information online, particularly when the data in question is sensitive, such as financial or health-related details. Robinson (2018) also showed a direct negative relationship between privacy concerns and willingness to share, concluding that heightened concern leads to a more negative attitude toward disclosure. Acquisti et al. (2015) reinforced this conclusion, reporting that individuals with strong privacy concerns often reduce data sharing behavior, even opting to pay more to avoid disclosing information. Across these studies, the evidence consistently supports the conclusion that privacy concerns are a key deterrent to voluntary data disclosure.

H11: Higher perceived control over personal data increases willingness to disclose data.

Higher perceived control over personal data significantly increases consumers' willingness to disclose information by reducing privacy concerns and fostering trust (Ashworth & Free, 2006; Penaloza, 2006). When individuals believe they can determine who accesses their data and how it is used, they feel more comfortable and confident in disclosure (Ashworth & Free, 2006; Boerman et al., 2017). Transparent procedures such as explicit permission requests, opt-in and opt-out options, and clear privacy settings empower consumers, making them feel respected and in control, which lowers anxiety about misuse and vulnerability (Ashworth & Free, 2006; Carroll et al., 2007; Watson et al., 2013). This user control enhances perceptions of procedural fairness and safety, encourages openness to personalized marketing, and strengthens trust in brands and platforms (Boerman et al., 2017; Carroll et al., 2007; Watson et al., 2013). Consequently, policies

and technologies that prioritize user-centric data management increase perceived control, thereby promoting greater willingness to disclose personal data in permission-based marketing contexts (Penaloza, 2006; Watson et al., 2013).

H12: Privacy concerns moderate the effect of trust in brand on willingness to disclose personal data.

Trust in a brand – built through reputation, ease of use, and clear security signals like third-party certifications – increases consumers' willingness to disclose personal data, but this effect is moderated by privacy concerns arising from past experiences, media reports, or uncertainty about data use (Penaloza, 2006). Privacy worries can weaken the positive impact of trust on data sharing, indicating that trust alone is insufficient without addressing these concerns through transparent policies, visible security measures, and user control (Penaloza, 2006; Watson et al., 2013). Consumers generally share more data when they believe the brand will handle it fairly and securely, yet high privacy concerns, such as fears of misuse or third-party sharing, can override trust and reduce willingness to disclose information (Norberg et al., 2007; Watson et al., 2013). This balance between trust and privacy concerns is particularly important in sensitive digital contexts, like AI-based healthcare, where trust encourages data sharing but privacy fears diminish it, making transparent communication and strong data protection essential to foster consumer engagement in permission-based marketing (Luo et al., 2023; Norberg et al., 2007).

H13: Higher perceived benefits of personalization increase willingness to disclose data.

Research consistently shows that higher perceived benefits of personalization – such as convenience, relevance, tailored recommendations, discounts, and improved service efficiency – increase consumers' willingness to disclose personal data (Anic et al., 2019; DuFrene et al., 2005; Li, 2012, 2014; Luo et al., 2023; Rowley, 2004; Tezinde et al., 2002; Watson et al., 2013). These benefits motivate users by providing clear, tangible rewards that outweigh privacy concerns through a privacy calculus or cost-benefit analysis (Anic et al., 2019; Li, 2012). Personalization builds trust as users believe their data will be handled responsibly to enhance their experience, which further reduces hesitation and encourages disclosure (Li, 2014; Luo et al., 2023; Watson et al., 2013). Empirical evidence supports that perceived benefits positively predict willingness to disclose data by demonstrating that users value the personalized service and feel the trade-off between privacy risks and rewards is favorable (Anic et al., 2019; Li, 2014; Rowley, 2004). In sum, perceived benefits act as a key driver in permission-based marketing by fostering trust and motivating consumers to share personal information (DuFrene et al., 2005; Luo et al., 2023).

2.2.Data Collection Method and Instruments

A quantitative survey was selected as the primary data collection method for this study, as it aligns well with the research objectives, the chosen theoretical framework, and the scope of the thesis. **The survey method** is widely recognized in marketing and consumer behavior research for its ability to gather standardized data from a large sample efficiently, particularly when examining complex models with multiple constructs. Given the study's focus on investigating trust-related factors, privacy concerns, perceived control, and their influence on willingness to disclose personal data, a survey provides a structured format for capturing these variables simultaneously and in a consistent manner across respondents. The flexibility of surveys allows for the measurement of a diverse range of factors, such as attitudes, perceptions, and behavioral intentions, which is essential for testing the developed research model. Furthermore, the online survey format enabled the study to reach a broad audience across Lithuania, specifically targeting UAB „Bolt Services" users or people familiar with their urban mobility services, ensuring a diverse and relevant sample. This approach also ensured that data could be collected within the limited timeframe and resources typical for a master's thesis project. By relying on established and validated constructs adapted from previous research, the survey method ensured both the reliability and validity of the findings, contributing to the overall robustness of the empirical investigation.

For the purposes of this study, **several validated constructs were adapted and applied** to measure key variables related to personal data disclosure and user behavior in the context of permission-based marketing. The questionnaire items were derived from established scales in the academic literature and adjusted as necessary to align with the study's objectives. In instances where the original scales utilized a 5- or 9-point Likert scale, items were adapted to a standardized 7-point Likert format to ensure consistency across the instrument.

The questionnaire was initially developed in English and subsequently translated into Lithuanian. Only Lithuanian version was distributed online, primarily through social media platforms and public community groups, allowing respondents to participate anonymously at their convenience. Anonymity was emphasized to encourage honest and candid responses, thereby enhancing the reliability and validity of the data.

Trust in technologies was measured using an adapted construct from Robinson (2018), as no direct measures for general trust in technologies were identified in the literature. Robinson's (2018) construct, which focuses on perceptions of the internet as a safe, reliable, and dependable

environment for information exchange and transactions, was deemed an appropriate proxy for this study's objectives. In the context of this research, trust in the internet is considered a closely related concept to trust in technologies, as brands such as Bolt rely on internet-based platforms and digital technologies to provide their services. Thus, users' trust in the internet as an infrastructure for transactions and communication is assumed to reflect their broader trust in the technological systems underlying permission-based marketing practices.

Trust in government (perceived regulatory effectiveness) was measured using a construct adapted from Urbonavičius et al. (2021). This construct includes three items that assess participants' perceptions of national and international authorities' effectiveness in protecting online privacy through regulations such as the General Data Protection Regulation (GDPR). A construct by Robinson (2018) was also considered but ultimately not adopted, as it focused only on the direct trust on different types of institutions (e.g., national, local governments, corporate businesses) rather than the regulatory effectiveness of the government bodies.

Perceived control over personal data was measured using a construct adapted from Wang et al. (2016), which had also been successfully employed in prior research by Urbonavičius et al. (2021) with sligh adaptations. This construct comprises three items designed to capture respondents' sense of autonomy and control over how their personal data is used and shared by brands. Additionally, a construct developed by Luo et al. (2023) was considered for inclusion; however, it required extensive modifications to measure perceived control over personal data in our situation.

Privacy concerns were assessed using a construct adapted from Krafft et al. (2017) with very slight modifications. This construct includes four items that evaluate participants' concerns about potential misuse of their personal data, including unauthorized sharing and purposes beyond the original intent.

Trust in brand was measured using an adapted construct from O'Cass and Carlson (2012), consisting of four items assessing whether participants feel safe in transactions, trust the brand to protect their data, believe the company is generally trustworthy, and feel that any information shared by the brand is secure. Jayawardhena et al.'s (2009) construct was reviewed but excluded, as it required prior personal experience with the brand, which was not necessary for this study – respondents only needed to be aware of the brand.

Willingness to disclose personal data was measured using an adapted construct originally developed by Urbonavičius et al. (2021). The final list of nine categories of personal data – such as contact information, demographic details, online behavior, and health data – was refined and

extended by the author of this study based on a comprehensive literature review (see Table 1). Participants were asked to indicate their willingness to disclose each type of data, offering insights into their perceptions of privacy sensitivity across different categories. While alternative constructs from Gupta et al. (2010) and Heirman et al. (2013) were considered, they were ultimately excluded: Gupta et al.'s (2010) construct covered a broad and diverse set of data types that overlapped with the author's framework, while Heirman et al.'s (2013) and Urbonavičius et al.'s (2021) measures were deemed too limited for the wider context of permission-based marketing. Nevertheless, relevant elements from these constructs were integrated into the author's final measure to ensure a comprehensive and robust assessment of willingness to disclose various types of personal data.

Perceived benefits of personalization were measured using a construct from Krafft et al. (2017) with slight adaptations, consisting of eight items assessing how participants perceive the relevance, usefulness, and customization of a brand's personalized communication. The construct captures whether communication is tailored to individual needs, provides meaningful and interesting recommendations, and enables participants to order products suited to their preferences. While Robinson's (2018) construct, focused on purchasing benefits like discounts and merchandise variety, it was excluded due to its narrower focus on tangible goods rather than services, which is a main subject in our survey.

An overview of all constructs and their corresponding scale formats is provided in Table 2. This structured measurement approach ensures a comprehensive assessment of the factors influencing personal data disclosure in the context of permission-based marketing. The complete questionnaire, including all measurement items, are available in Annex 3 (English language) and Annex 4 (Lithuanian language) – only Lithuanian language version was distributed.

Table 2. *Constructs of the measurement. Made by Author of the Thesis*

Variable	Construct **modified*	Type of scale	Authors
Trust in technologies	1. Technologies and* the internet is a safe environment in which to exchange information with others. 2. Technologies and* the internet is a reliable environment in which to conduct business transactions or personal purchases.	7 point Likert scale	Adapted from (Robinson, 2018): 1. The Internet is a safe environment in which to exchange information with others. 2. The Internet is a reliable environment in which to

	3. Technology and* internet merchants are dependable. 4. Technologies and* the internet can be trusted.		conduct business transactions or personal purchases. 3. Internet merchants are dependable. 4. The Internet can be trusted.
Trust in government (perceived regulatory effectiveness)	1. The existing laws in my country and internationally, (such as General Data Protection Regulation, GDPR) are sufficient to protect consumers' online privacy. 2. There are stringent international laws to protect personal information of individuals on the Internet. 3. The government is doing enough to ensure that consumers are protected against online privacy violations.	7 point Likert scale	(Urbonavicius et al., 2021)
Perceived control over personal data	1. I am usually bothered when I do not have control over personal information that I provide to this company/brand*. 2. I am usually bothered when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by this company/brand*. 3. I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction with this company/brand*.	7 point Likert scale	Adapted from (T. Wang et al., 2016): 1. I am usually bothered when I do not have control over personal information that I provide to mobile applications. 2. I am usually bothered when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by mobile applications. 3. I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction with mobile applications
Privacy concerns	I am concerned that this company/brand* will: 1. ... gather too much personal information about me. 2. ... use my personal data for purposes other than the reason I provided the information for. 3. ... share my personal information with other parties.	7 point Likert scale	Adapted from (Krafft et al., 2017): I am concerned that the company will: 1. … gather too much personal information about me. 2. … use my personal data for purposes other than the reason I provided the information for. 3. … share my personal information with other parties.

	4. I am concerned about my privacy at this company/brand*.		4. I am concerned about my privacy at this company.
Trust in brand / company	1. I feel safe in my transactions with this company/brand*. 2. I trust this company/brand* to keep my personal information safe. 3. Overall this company/brand* is trustworthy. 4. I feel that any information communicated by this company/brand* is secure.	7 point Likert scale	Adapted from (O'Cass & Carlson, 2012): 1. I feel safe in my transactions with the retailer's website. 2. I trust the retailer's website to keep my personal information safe. 3. Overall the retailer's website is trustworthy. 4. I feel that any information communicated by the retailer's website is secure.
Willingness to disclose personal data	While purchasing or ordering services at this company/brand*, you are often asked to provide to them your personal data. Please, specify, how much are you willing to provide personal data of each type of data: 1. Contact Information (Name, Email address, Phone number, Home adress)* 2. Demographic Data (Age, Gender, Education level, Location from)* 3. Online Behavioral Data / Cookies (Browsing History, Purchase History, Website Visits)* 4. Social Networking Data (Interests, Likes, Social Connections)* 5. Receiving Content Preferences Data (Content preferences, Frequency of communication preferences, Preferred communication channels)* 6. Profile and views data (Hobbies, Faith orientation, Political orientation, Relationship status, Favourite brands)* 7. Medical data (Health conditions, Medical history, Medications)*	7 point Likert scale	Adapted from (Urbonavicius et al., 2021): While purchasing goods or services in online, you are often asked to provide to them your personal data. Please, specify, how much are you willing to provide personal data of each type: 1. Home address 2. Mobile phone number 3. Email address 4. Date of birth 5. Marital status 6. Name 7. Last name 8. Gender

	8. Financial data (Income level, Loans information, Transaction history, Investment portfolio details)* 9. Live Location Data (Geolocation, Location-based Marketing Data)*		
Perceived benefits of personalization	The personalized communication of this company/brand* will: 1. ... be supposedly relevant to my needs. 2. ... be supposedly meaningful to me. 3. ... be supposedly useful to me. 4. ... be supposedly interesting to me. 5. ... be supposedly provide purchase recommendations that match my needs. 6. I think this personalized communication of this company/brand* enables me to order products that are tailor-made for me. 7. Overall, this personalized communication of this company/brand* is tailored to my situation. 8. I believe this personalized communication of this company/brand* is customized to my needs.	7 point Likert scale	Adapted from (Krafft et al., 2017): The personalized communication of the company will: 1. … be supposedly relevant to my needs. 2. … be supposedly meaningful to me. 3. … be supposedly useful to me. 4. … be supposedly interesting to me. 5. … supposedly provide purchase recommendations that match my needs. 6. I think this personalized communication of the company enables me to order products that are tailor-made for me. 7. Overall, this personalized communication of the company is tailored to my situation. 8. I believe this personalized communication of the company is customized to my needs.

2.3.Selection of respondents and methods for analysis

First, in order to define the sampling technique, the population of the study was determined. Given the research focus on consumers who disclose personal data to brands for personalized offers, the population of interest consists only of consumers who are familiar with the Bolt brand. Since the aim was to examine factors such as trust, privacy concerns, and perceived benefits in relation to data disclosure behavior, **the main inclusion criteria for respondents were:**

1) being **18 years or older** (to ensure respondents have the legal capacity to make independent decisions about data sharing)
2) being **aware of the Bolt brand** as urban mobility provider in order to evaluate their level of trust towards it.

No specific limitations regarding gender, age beyond 18+, or education were applied to ensure a diverse sample of respondents.

The data collection process involved distributing an **online questionnaire** via multiple channels. These included sharing the survey made on Google Forms on social media platforms such as Facebook, Instagram, Discord, and LinkedIn in the relevant forums where people discuss experiences related to the Bolt brand and other similar urban mobility services. Given the absence of a direct sampling frame (as no full list of Bolt users was accessible), the study employed a **non-probability convenience sampling method**. This approach was chosen due to practical constraints in obtaining access to a full population list and to enable the collection of insights from a relevant group of participants in a time-efficient manner.

To determine an appropriate sample size for the survey, two complementary estimation techniques were applied. First, a comparable studies approach was used to benchmark the sample against similar quantitative research on consumer privacy, trust, and willingness to disclose personal data. A review of such studies indicated that typical sample sizes in this field range from approximately **300 to 400 respondents**. Aligning with this established practice ensures that the resulting dataset is sufficiently large to support reliable inference and meaningful statistical analysis. The study therefore targeted a similar number of valid responses, maintaining consistency with methodological norms in related research domains.

A second sample size estimation method relied on the Paniotto formula, which provides a statistical calculation of required sample size based on the acceptable margin of error and the size of the target population. Applying this formula with a 5 percent margin of error indicated that **a minimum of 400 respondents** would be needed to achieve results with an adequate level of precision. This estimate is consistent with the benchmark derived from comparable studies and reinforces the methodological soundness of the chosen sample size. The target population for this research comprises 2,393,536 adult residents of Lithuania. According to data from the Lithuanian Official Statistics Portal, the total population at the beginning of 2025 was 2,890,664 people, of whom 2,393,536 were adults aged 18 and older (Lithuanian Official Statistics Portal, 2025), which was the only age group eligable to participate in this research.

$$n = \frac{1}{\Delta^2 + \frac{1}{N}}$$

n is the required sample size,

Δ is the acceptable margin of error,

N is the population size.

When N = 2,393,536 and n = 5%:

$$n = \frac{1}{0{,}05^2 + \frac{1}{2393536}} = \textbf{400 respondents}$$

Table 3. *Comparable Researches Sampling Methods, made by Author of the Thesis*

Author	Type of questionnaire	Sampling	Number of respondents (valid responses)
(Beldad et al., 2011)	Online questionnaire	Non-probability sampling – Multi-phase convenience sampling	208
(Bhatia, 2020)	Online and offline questionnaire	Non-probability sampling – Convenience sampling	271
(Degutis et al., 2020)	Online questionnaire	Non-probability sampling – Convenience sampling	439
(Hajli et al., 2017)	Online and offline questionnaire	Non-probability sampling – Convenience sampling	201
(Jolley et al., 2013)	Web-based experimental questionnaire	Non-probability sampling – Purposive sampling	168
(Kehr et al., 2015)	Online questionnaire	Non-probability sampling – Convenience sampling	414
(Luo et al., 2023)	Online questionnaire	Non-probability sampling – Purposive sampling with pre-screening	494
(Pandey, 2023)	Online and offline questionnaire	Non-probability sampling – Snowball sampling	210
(Robinson, 2018)	Online questionnaire	Non-probability sampling – Quota sampling	248
(T. Wang et al., 2016)	Online questionnaire	Non-probability sampling – Convenience / Purposive sampling	327
(Urbonavicius et al., 2021b)	Online questionnaire	Non-probability sampling – Convenience sampling	480

(Watson et al., 2013)	Online questionnaire	Non-probability sampling – Convenience / Snowball sampling	214
AVERAGE VALID RESPONSES			**306**

The collected survey data were prepared and analyzed using **IBM SPSS** Statistics. Prior to analysis, all variable names, item labels, and value labels were translated from Lithuanian to English to ensure consistency and accuracy. Initial data screening was conducted to identify missing values, verify correct coding of responses, and examine the demographic profile of respondents using frequency distributions and percentages for variables such as age, gender, geographic location, and education level.

Reliability analysis was performed using Cronbach's alpha to assess the internal consistency of all multi-item constructs, with values above 0.70 considered acceptable. Following confirmation of reliability, composite scores for each construct were computed by averaging their corresponding items to create aggregate indicators for subsequent analyses.

Descriptive statistics, including means, standard deviations, minimums, and maximums, were generated for all composite variables, providing an overview of key constructs such as trust in brand, trust in government, trust in technology, privacy concerns, perceived benefits of personalization, perceived control over personal data, and willingness to disclose personal data. Distributional properties were examined using skewness, kurtosis, and Shapiro–Wilk tests, which indicated deviations from normality for several variables. Consequently**, non-parametric statistical techniques** were applied where appropriate.

Hypotheses involving direct relationships between two variables (H6 and H8) were tested using **simple linear regression** analysis. Hypotheses involving multiple theoretically interrelated predictors (H1-H5, H7, H9-H11, H13) were examined using **multiple linear regression** analysis, assessing the effects of trust-related factors, perceived control over personal data, privacy concerns, and perceived benefits of personalization on the respective dependent variables. **Moderation analysis** was conducted using **Hayes' PROCESS macro** (Model 1) to test whether privacy concerns moderated the relationship between trust in brand and willingness to disclose personal data (H12).

In addition to general analyses, willingness to disclose different types of personal data was examined to account for heterogeneity in data sensitivity. Differences in willingness to disclose across data categories were tested using **Friedman's test**, while **Kruskal–Wallis tests** were employed to compare disclosure behavior across consumer segments. To identify distinct consumer groups based on privacy-related psychological characteristics, a cluster analysis was

conducted using standardized variables. Hierarchical clustering with **Ward's method** was first applied to determine the optimal number of clusters, followed by **K-means** clustering to finalize cluster membership.

Where relevant, non-parametric group comparison tests were used to explore differences in disclosure behavior across demographic groups. The results of these analyses form the empirical basis for testing the study's hypotheses and for identifying distinct patterns of permission-based marketing personal data disclosure, which are presented in the following chapter.

3. EMPIRICAL ANALYSIS OF CONSUMER DATA DISCLOSURE BEHAVIOR

3.1. Respondent Profile and General Personal Data Sharing Behaviour

A total of 508 respondents completed the survey. However, given the research focus on consumers who disclose personal data to brands for personalized offers, only those familiar with the urban mobility brand Bolt were included. 93.3% of the respondents use or used urban mobility services "Bolt", 5.7% of the respondents have never used it but is familiar with the brand, and 1% was not aware of this brand. As a result, 5 respondents did not meet the qualification criteria and were excluded from the study, leaving **a final sample of 503 valid respondents.**

As seen in Table 4, the sample was predominantly female (78.9%), with males representing 18.3% and 2.8% identifying as other or not disclosing their gender. The largest age groups were 18–24 (32.6%) and 25–34 (31.4%), followed by 35–44 (22.1%), indicating a relatively young sample. Most respondents held a Bachelor's degree (42.7%) or Master's degree (26.4%), while smaller shares had secondary (23.9%) or vocational education (3.8%). In terms of location, the majority lived in larger Lithuanian cities with populations above 80,000 (88.1%), with smaller cities and villages accounting for 11.9% of the sample. Compared to national statistics from Lithuanian Official Statistics Portal (2025), the survey sample is slightly younger, more urban, and more highly educated, while women are somewhat overrepresented. Although the sample does not fully reflect the Lithuanian population, the **study employed a non-probability convenience sampling method**. This approach aligns with the research objective, focusing specifically on perception-based dependencies among the selected variables rather than generating generalizable population estimates.

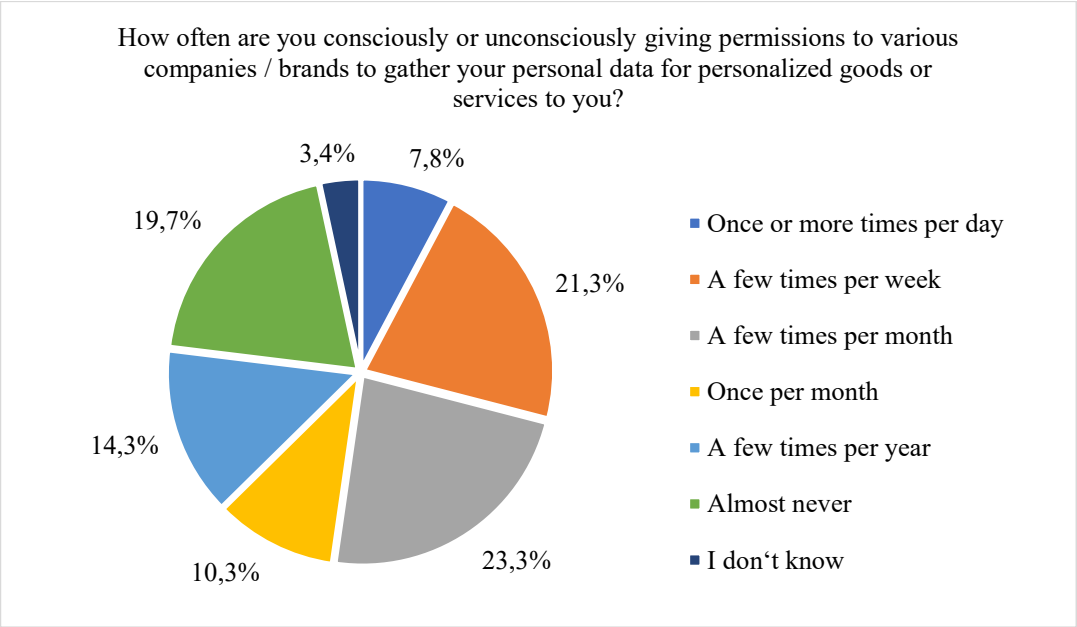
Table 4. *Survey respondents' demographical data vs Lithuanian demographical data (Lithuanian Official Statistics Portal, 2025).*

Respondents' demographical data (age >=18, aware of „Bolt")		N	%		%	Lithuanian demographical data (2025)	
Gender	Male	92	18.3		47.45	Male	Gender
	Female	397	78.9		52.55	Female	
	Did not disclose or chose "other"	14	2.8		-	-	
Age group	18-24	164	32.6		6.6	18-24	Age group
	25-34	158	31.4		12.5	25-34	
	35-44	111	22.1		14.7	35-44	
	45-54	53	10.5		13.6	45-54	
	55-64	14	2.8		14.6	55-64	
	64+	3	0.6		20.9	65+	
Education	Primary education	8	1.6		61.4	Other level of education or unknown	Education
	Secondary education	120	23.9				
	Vocational education	19	3.8				
	Bachelor's degree	215	42.7		38.6	Higher education degree	
	Master's degree	133	26.4				
	Doctoral degree	8	1.6				
Geography	Big cities (exceeding 80,000 population)	443	88.1		68.5	Urban areas	Geography
	Smaller cities (with a population between 3,000 and 80,000)	44	8.7				
	Villages (with population under 3,000)	16	3.2		31.5	Rural areas	

To explore general consumer behavior regarding permission-based marketing, respondents were asked how often they consciously or unconsciously allow companies or brands to collect their personal data for personalized goods or services. As seen in Figure 10, the responses reveal that while some consumers actively manage their data sharing, a substantial portion engages in this behavior with moderate frequency: 7.8% reported giving permissions once or more times per day, 21.3% a few times per week, and 23.3% a few times per month. Fewer respondents indicated once per month (10.3%), a few times per year (14.3%), or almost never (19.7%), while 3.4% were uncertain.

The relatively even distribution of answers may indicate that many individuals may not fully recognize the extent to which they are sharing personal data. Digital interactions with the brands, such as visiting websites and accepting cookies, using apps that request location access, or subscribing to newsletters, often involve granting permissions without conscious awareness. This suggests that while consumers regularly provide personal information, a significant portion of this behavior occurs passively, highlighting the importance of transparency and trust in permission-based marketing practices.

Figure 10. *Respondents' self-evaluated personal data disclosure to brands general behavior*



3.2.Questionnaire Validity and Reliability

Before proceeding with the detailed analysis of the research results, it is necessary to assess the suitability and reliability of the questionnaire used in this study. Evaluating instrument quality ensures that the statements within each construct measure the intended concept consistently and can be used confidently in further statistical analyses. Cronbach's alpha was applied as the primary method for assessing internal consistency, as it is widely recognized as an appropriate indicator of reliability in multi-item scales. Accordingly, Table 5 presents the reliability evaluation of the constructs included in the survey based on Cronbach's alpha.

Table 5. *Cronbach's Alpha Values for Study Constructs*

Construct	Number of Items	Cronbach's Alpha
Trust in technologies	4	0.866
Trust in government (perceived regulatory effectiveness)	3	0.847
Perceived control over personal data	3	0.923
Privacy concerns	4	0.918
Trust in brand / company	4	0.916
Willingness to disclose personal data	9	0.855
Perceived benefits of personalization	8	0.961

As shown in Table 5, all constructs demonstrated acceptable to excellent internal consistency, with **Cronbach's alpha values ranging from 0.847 to 0.961**. This indicates that the items within each construct reliably measure the same underlying concept, and the questionnaire is suitable for further statistical analyses, including correlation and regression analyses. Before computing composite scores, the items measuring **perceived control over personal data were reverse-coded** so that higher values reflect higher perceived control. This adjustment was necessary to ensure theoretical alignment across constructs, as the original item wording assigned higher numerical values to lower perceived control. All other constructs were coded in their original direction.

Following the reliability analysis and computation of composite scores, it is essential to examine the descriptive statistics of the main study constructs. Descriptive statistics provide an initial understanding of the central tendencies, variability, and distributional characteristics of the variables under investigation. Assessing measures such as the mean, standard deviation, skewness, and kurtosis allows us to identify general response patterns, evaluate the range of participant perceptions, and verify assumptions for subsequent parametric analyses, including correlations and regression analyses.

As seen in Table 6, the mean scores for most constructs indicate moderate to moderately high levels among respondents. Trust in technologies (M = 3.66, SD = 1.20), trust in government (M = 3.78, SD = 1.28), perceived control over personal data (Reversed: M = 4.12, SD = 1.47), privacy concerns (M = 4.10, SD = 1.41), trust in the brand (M = 4.42, SD = 1.18), and perceived benefits of personalization (M = 3.78, SD = 1.33) show relatively balanced responses across the 1–7 Likert scale. Willingness to disclose personal data displayed a slightly lower average (M = 2.90, SD = 1.07) with a maximum of 6.33, reflecting some restraint in sharing personal information.

Normality was assessed using the Shapiro–Wilk test, where a p-value < 0.05 indicates a significant deviation from normality. All constructs had $p < 0.05$, suggesting that the **assumption of normality was not met**. Skewness and kurtosis were also examined, with thresholds of |Skewness| < 1 and |Kurtosis| < 2. Although, as seen in Table 6, all constructs were within these limits, the Shapiro-Wilk results indicate that the data cannot be considered fully normal. Trust in the brand showed a slight negative skew (Skewness = -0.48), indicating that respondents tended to rate the brand more positively, while willingness to disclose personal data had a modest positive skew (Skewness = 0.64), reflecting some caution in sharing personal information.

Table 6. *Descriptive Statistics, Skewness, and Kurtosis for All Study Variables*

	Minimum	Maximum	Mean	Std. Deviation	Skewness	Kurtosis	Shapiro-Wilk
Trust in technologies	1.00	7.00	3.66	1.20	-0.053	-0.548	<0.001
Trust in government (perceived regulatory effectiveness)	1.00	7.00	3.79	1.28	-0.004	-0.542	<0.001
Perceived control over personal data	1.00	7.00	4.12	1.47	0.002	-0.716	<0.001
Privacy concerns	1.00	7.00	4.10	1.41	-0.097	-0.562	<0.001
Trust in brand / company	1.00	7.00	4.43	1.18	-0.476	0.297	<0.001
Willingness to disclose personal data	1.00	6.33	2.90	1.07	0.638	0.072	<0.001
Perceived benefits of personalization	1.00	7.00	3.78	1.33	-0.058	-0.597	<0.001

3.3.Consumer Behavior in Permission-Based Marketing Data Disclosure

3.3.1. Hypothesis Testing of Psychological Determinants of Permission-Based Marketing Data Disclosure

Following the assessment of questionnaire reliability, validity, and distributional properties, this section examines consumer behavior in permission-based marketing data

disclosure through empirical testing of the proposed hypotheses. The analysis focuses on how trust-related factors, perceived control over personal data, privacy concerns, and perceived benefits of personalization shape consumers' willingness to disclose personal data for marketing purposes. Depending on the structure of each hypothesis, linear regression and multiple regression analyses were applied. Simple linear regression was used for hypotheses involving a single predictor variable (H6 and H8), while multiple regression analysis was employed for hypotheses in which several theoretically interrelated predictors were expected to influence the same outcome variable.

In addition to testing relationships between psychological constructs, this study acknowledges that personal data are heterogeneous and differ substantially in perceived sensitivity and risk. Therefore, the analysis extends beyond aggregate willingness to disclose and examines willingness to share specific types of personal data. This allows for identifying disclosure patterns across data categories and provides a more nuanced understanding of consumer behavior. Finally, clustering and comparative analyses are applied to explore whether distinct disclosure patterns emerge across different data types, providing further insight into heterogeneity in permission-based marketing data-sharing behavior.

Predictors of Privacy Concerns (H1, H2, H3, H7)

Hypotheses H1, H2, H3, and H7 examined the effects of trust in brand, trust in technologies, trust in government (perceived regulatory effectiveness), and perceived control over personal data on privacy concerns using multiple linear regression analysis. The regression model was statistically significant, $F(4, 498) = 142.301$, $p < 0.001$, and explained a substantial proportion of variance in privacy concerns ($R^2 = 0.533$; adjusted $R^2 = 0.530$). Multicollinearity was not a concern, as variance inflation factor (VIF) values ranged from 1.188 to 1.557, well below commonly accepted thresholds (VIF < 5.0).

Perceived control over personal data emerged as the strongest predictor, exhibiting a large and statistically significant negative effect on privacy concerns ($\beta = -0.670$, $p < 0.001$). This result provides strong **support for H7**, indicating that greater perceived control is associated with markedly lower privacy concerns. Trust in brand also showed a significant negative relationship with privacy concerns ($\beta = -0.129$, $p < 0.001$), **supporting H1** and suggesting that brand-level trust independently contributes to reducing privacy-related fears.

In contrast, trust in technologies ($\beta = 0.013$, $p = 0.715$) and trust in government ($\beta = -0.021$, $p = 0.571$) did not significantly predict privacy concerns when included in the multivariate model. Consequently, **H2 and H3 are not supported**. These findings suggest that, when individual-level

perceptions such as perceived control and brand trust are accounted for, broader institutional and technological trust do not directly alleviate privacy concerns. This pattern is consistent with prior literature emphasizing the central role of perceived control and relational trust in shaping privacy-related evaluations (Ashworth & Free, 2006; Krafft et al., 2017; Watson et al., 2013).

Predictors of Perceived Control (H4, H5)

Hypotheses H4 and H5 examined whether trust in technologies and trust in government influence perceived control over personal data using multiple linear regression analysis. The regression model was statistically significant, $F(2, 500) = 4.030$, $p = 0.018$, although the explained variance was modest ($R^2 = 0.016$; adjusted $R^2 = 0.012$). Multicollinearity was not a concern, as variance inflation factor (VIF) values were 1.297 for both predictors

Trust in technologies demonstrated a small but statistically significant positive effect on perceived control ($\beta = 0.109$, $p = 0.032$), **supporting H4**. This indicates that confidence in technological systems enhances individuals' subjective sense of control over their personal data. In contrast, trust in government did not significantly predict perceived control ($\beta = 0.030$, $p = 0.553$), leading to the **rejection of H5**. These findings imply that perceived control is more closely linked to technological reliability and system-level assurances than to institutional trust in regulatory frameworks, reflecting patterns observed in prior research (Colesca, 2009; Li, 2014; Robinson, 2016).

Perceived Control, Trust, and Benefits (H6, H8)

Hypothesis H6 examined the effect of perceived control over personal data on trust in brand using simple linear regression analysis. The regression model was statistically significant, $F(1, 501) = 87.994$, $p < 0.001$, explaining 14.9% of the variance in trust in brand ($R^2 = 0.149$). Perceived control exerted a positive and statistically significant effect on trust in brand ($\beta = 0.387$, $p < 0.001$), providing strong **support for H6**. This finding indicates that individuals who feel a greater sense of control over how their personal data are managed tend to exhibit higher levels of trust in the brand. The result is consistent with prior research suggesting that consumer empowerment and perceived control play a central role in strengthening trust within permission-based marketing contexts (Carroll et al., 2007; Krafft et al., 2017; Watson et al., 2013).

Hypothesis H8 examined the effect of privacy concerns on perceived benefits of personalization using simple linear regression analysis. The regression model was statistically significant, $F(1, 501) = 16.330$, $p < 0.001$, explaining 3.2% of the variance in perceived benefits of personalization ($R^2 = 0.032$). Privacy concerns exerted a negative and statistically significant effect on perceived benefits of personalization ($\beta = -0.178$, $p < 0.001$), providing **support for H8**.

This result indicates that higher levels of privacy concern are associated with a reduced ability to perceive the value and advantages of personalized marketing, such as relevance and convenience. The finding is consistent with privacy calculus theory, which posits that elevated perceptions of risk diminish the salience of perceived benefits in data disclosure decisions (Krafft et al., 2017; Luo et al., 2023; Norberg et al., 2007).

Predictors of Willingness to Disclose Personal Data (H9, H10, H11, H13)

Hypotheses H9, H10, H11, and H13 examined the effects of trust in brand, privacy concerns, perceived control over personal data, and perceived benefits of personalization on consumers' willingness to disclose personal data using multiple linear regression analysis. The regression model was statistically significant, $F(4, 498) = 38.258$, $p < 0.001$, and explained a meaningful proportion of variance in willingness to disclose personal data ($R^2 = 0.235$; adjusted $R^2 = 0.229$). Multicollinearity was not a concern, as variance inflation factor (VIF) values ranged from 1.271 to 2.142.

Among the predictors, only perceived benefits of personalization exerted a statistically significant effect ($\beta = 0.391$, $p < 0.001$), **supporting H13**. Trust in brand ($\beta = 0.087$, $p = 0.068$), privacy concerns ($\beta = -0.051$, $p = 0.375$), and perceived control ($\beta = 0.080$, $p = 0.162$) did not show significant independent effects when all predictors were considered simultaneously, leading to the **rejection of H9, H10, and H11** in the full model.

To further examine the risk–benefit mechanism proposed by privacy calculus theory, an additional multiple regression analysis including only privacy concerns and perceived benefits of personalization was conducted. This model was also statistically significant, $F(2, 500) = 72.848$, $p < 0.001$, and multicollinearity was not observed, with VIF values equal to 1.033 for both predictors. Both variables exerted statistically significant effects on willingness to disclose personal data: privacy concerns showed a negative effect ($\beta = -0.135$, $p < 0.001$), while perceived benefits of personalization demonstrated a strong positive effect ($\beta = 0.432$, $p < 0.001$).

These findings reinforce the central role of perceived risk-benefit trade-offs in shaping data disclosure decisions, consistent with privacy calculus arguments that perceived benefits often outweigh privacy concerns and trust-related considerations in actual disclosure behavior (Norberg et al., 2007). Moreover, the dominance of perceived benefits aligns with prior research in permission-based marketing, which emphasizes the importance of personalization value and relevance in motivating voluntary data disclosure (Krafft et al., 2017).

Moderation Analysis (H12)

H12 examined whether privacy concerns moderate the relationship between trust in brand and willingness to disclose personal data. A moderation analysis using Hayes' PROCESS Macro (Model 1) revealed that the interaction effect was not statistically significant ($\Delta R^2 = 0.003$, $p = 0.213$). Therefore, **H12 is not supported**, suggesting that the effect of brand trust on disclosure intentions does not depend on the level of privacy concern. This outcome contrasts with some prior findings (Penaloza, 2006; Watson et al., 2013), but is consistent with the present results emphasizing perceived benefits as the dominant driver of disclosure decisions.

Table 7. *Summary of Hypotheses Testing Results*

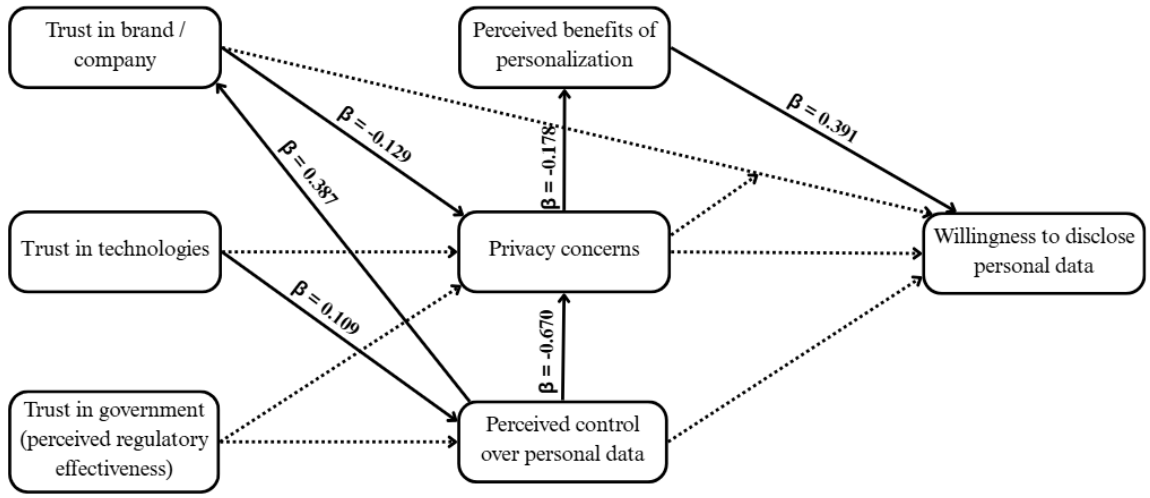
Hypothesis	**Relationship Tested**	**Analysis Method**	**Key Result (β / ΔR²)**	**p-value**	**Supported**
H1	Trust in brand → Privacy concerns	Multiple regression	β = -0.129	<0.001	Yes
H2	Trust in technologies → Privacy concerns	Multiple regression	β = 0.013	0.715	No
H3	Trust in government → Privacy concerns	Multiple regression	β = -0.021	0.571	No
H4	Trust in technologies → Perceived control over personal data	Multiple regression	β = 0.109	0.032	Yes
H5	Trust in government → Perceived control over personal data	Multiple regression	β = 0.030	0.553	No
H6	Perceived control over personal data → Trust in brand	Simple linear regression	β = 0.387	<0.001	Yes
H7	Perceived control over personal data → Privacy concerns	Multiple regression	β = -0.670	<0.001	Yes
H8	Privacy concerns → Perceived benefits	Simple linear regression	β = -0.178	<0.001	Yes
H9	Trust in brand → Willingness to disclose	Multiple regression	β = 0.087	0.068	No
H10	Privacy concerns → Willingness to disclose	Multiple regression	β = -0.051	0.375	No
H11	Perceived control over personal data → Willingness to disclose	Multiple regression	β = 0.080	0.162	No
H12	Trust in brand × Privacy concerns → Willingness to disclose	Moderation (PROCESS Model 1)	$\Delta R^2 = 0.003$	0.213	No

H13	Perceived benefits → Willingness to disclose	Multiple regression	β = 0.391	<0.001	Yes

Note. β coefficients are standardized regression coefficients. Significance was assessed at $p < 0.05$.

Overall, the hypothesis testing results provide partial support for the proposed research model and highlight the central mechanisms underlying permission-based marketing data disclosure. The findings demonstrate that perceived control over personal data and trust in brand play a critical upstream role by significantly reducing privacy concerns, while trust in technologies contributes modestly to strengthening perceived control. In contrast, trust in government did not exhibit significant effects on either privacy concerns or perceived control. With regard to disclosure behavior, perceived benefits of personalization consistently emerged as the strongest and most reliable predictor of willingness to disclose personal data, whereas trust in brand, privacy concerns, and perceived control showed limited or indirect effects when considered simultaneously. These results support the privacy calculus perspective by indicating that disclosure decisions are primarily driven by a perceived risk–benefit trade-off, with trust and control shaping this process indirectly through their influence on privacy-related evaluations. Based on these findings, the final research model reflects a streamlined structure in which perceived benefits function as the dominant direct driver of disclosure, while trust- and control-related constructs operate through more complex, mediated pathways. Figure 11 summarizes the final research model with standardized coefficients for supported relationships.

Figure 11. *Final research model with standardized regression coefficients*



Note. Solid arrows indicate statistically significant relationships ($p < 0.05$). Dashed arrows represent hypothesized but non-significant paths. Only standardized regression coefficients (β) are displayed.

3.3.2. Sensitivity-Based Differences in Willingness to Disclose Personal Data

The analysis further extends beyond general disclosure intentions by examining consumers' willingness to disclose specific types of personal data, recognizing that disclosure behavior may vary substantially depending on data sensitivity. Descriptive statistics for the nine data categories reveal pronounced differences in willingness to disclose (Table 8), indicating that respondents clearly differentiate between types of personal information.

Contact information exhibited the highest mean willingness to disclose (M = 4.36, SD = 1.63), suggesting that respondents generally perceive this type of data as low-risk and are relatively comfortable sharing it. **Demographic data** (M = 3.58, SD = 1.72) and **preferences data of receiving content methods** (M = 3.35, SD = 1.70) were also disclosed at comparatively higher levels, indicating that these data types are viewed as useful for personalization while remaining relatively non-sensitive.

In contrast, willingness to disclose declined as perceived intrusiveness increased. **Live location data** (M = 2.90, SD = 1.71) and **online behavioral data** (M = 2.96, SD = 1.63) were shared less willingly, while **social networking data** (M = 2.67, SD = 1.62) and **profile and views data** (M = 2.48, SD = 1.56) demonstrated even lower mean scores. The lowest willingness to disclose was observed for **medical data** (M = 1.94, SD = 1.32) and **financial data** (M = 1.82, SD = 1.23), reflecting their high perceived sensitivity.

Based on these mean values, Table 8 additionally presents a classification of personal data types according to perceived sensitivity. Data categories with mean willingness scores of 3.00 and above were classified as low-sensitivity data, those with means between 2.00 and 2.99 as moderate-sensitivity data, and those with means below 2.00 as high-sensitivity data. This classification illustrates a clear hierarchy in disclosure preferences, distinguishing information that respondents readily share from data types approached with substantially greater caution.

Distributional characteristics further reinforce these findings. Skewness and kurtosis analyses indicate that most data types exhibit relatively symmetrical distributions; however, medical data (skew = 1.487) and financial data (skew = 1.640) were positively skewed, indicating that the majority of respondents reported low willingness to disclose these highly sensitive data types. In contrast, contact information displayed a slight negative skew (skew = -0.368), consistent with its high disclosure levels. Kurtosis values for medical (1.445) and financial data (2.032) were also more pronounced, reflecting response clustering around low willingness scores.

Normality tests using the Shapiro-Wilk procedure confirmed non-normal distributions across all data types ($p < 0.05$), necessitating the use of non-parametric statistical methods. A Friedman test revealed statistically significant differences in willingness to disclose across the nine categories ($p < 0.05$), confirming that respondents systematically differentiate between types of personal data.

Table 8. *Willingness to Disclose Personal Personal Data and Data Sensitivity (based on results and literature analysis)*

Types of Data	Data Sharing Sensitivity	Mean	Std. Deviation	Skewness	Kurtosis
Contact Information (Name, Email address, Phone number, Home adress)	Low	4.36	1.63	-0.368	-0.933
Demographic Data (Age, Gender, Education level, Location from)	Low	3.58	1.72	0.190	-1.102
Preferences Data of Receiving Content methods (Content preferences, Frequency of communication preferences, Preferred communication channels)	Low	3.35	1.70	0.305	-0.943
Online Behavioral Data / Cookies (Browsing History, Purchase History, Website Visits)	Moderate	2.96	1.63	0.530	-0.682
Live Location Data (Geolocation, Location-based Marketing Data)	Moderate	2.90	1.71	0.554	-0.846
Social Networking Data (Interests, Likes, Social Connections)	Moderate	2.67	1.62	0.830	-0.264
Profile and views data (Hobbies, Faith orientation, Political orientation, Relationship status, Favourite brands)	Moderate	2.48	1.56	0.934	-0.114
Medical data (Health conditions, Medical history, Medications)	High	1.94	1.32	1.487	1.445
Financial data (Income level, Loans information, Transaction history, Investment portfolio details)	High	1.82	1.23	1.640	2.032
OVERAL	**-**	**2.90**	**1.07**	**0.638**	**0.072**

To further explore consistency in disclosure behavior, a bivariate Spearman correlation analysis was conducted. Willingness to share contact information was moderately associated with

the disclosure of demographic data ($\rho = 0.369$, $p < 0.001$) and online behavioral data ($\rho = 0.273$, $p < 0.001$), but showed no significant association with highly sensitive data such as medical or financial information. This suggests that willingness to disclose low-sensitivity data operates largely independently from the disclosure of highly sensitive data.

In contrast, demographic data disclosure demonstrated moderate correlations with most other data types, including online behavioral data ($\rho = 0.461$, $p < 0.001$), social networking data ($\rho = 0.441$, $p < 0.001$), and profile and views data ($\rho = 0.443$, $p < 0.001$). Similarly, willingness to share online behavioral data was strongly correlated with social networking data ($\rho = 0.722$, $p < 0.001$) and profile and views data ($\rho = 0.574$, $p < 0.001$), but only weakly related to contact information and live location data.

A comparable pattern emerged for social networking and profile and views data, which were strongly interrelated ($\rho = 0.759$, $p < 0.001$) and also showed substantial correlations with highly sensitive data such as medical ($\rho = 0.536$, $p < 0.001$) and financial information ($\rho = 0.570$, $p < 0.001$). Preferences for receiving content were moderately to strongly associated with online behavioral data ($\rho = 0.536$, $p < 0.001$), social networking data ($\rho = 0.605$, $p < 0.001$), and profile and views data ($\rho = 0.543$, $p < 0.001$), but only weakly related to contact information ($\rho = 0.179$, $p < 0.001$). Finally, medical and financial data demonstrated a very strong interrelationship ($\rho = 0.829$, $p < 0.001$), while live location data showed moderate associations with both.

Overall, these findings indicate that disclosure behavior is highly sensitive to data type and partially consistent across related categories. Low-sensitivity data are treated distinctly from highly sensitive data, whereas moderate- and high-sensitivity data types tend to cluster together in participants' disclosure patterns. This differentiation underscores the importance of considering data type sensitivity when examining personal data disclosure behavior.

3.3.3. Predictors on Willingness to Disclose Different Types of Personal Data

Building on the descriptive, correlational, and general regression findings, the analysis now turns to a more fine-grained analysis of consumers' willingness to disclose specific types of personal data. While research model treated willingness to disclose as a general construct, the preceding results demonstrated substantial variation in disclosure behavior across data types with different levels of perceived sensitivity. This pattern suggests that the psychological mechanisms driving disclosure decisions may not operate uniformly across all categories of personal data.

To address this heterogeneity, a series of multiple regression analyses were conducted separately for each personal data category. For each model, **willingness to disclose a specific type**

of personal data served as the dependent variable, while **trust in brand, perceived control over personal data, privacy concerns, and perceived benefits of personalization** were entered simultaneously as predictors. This approach allows for assessing the independent contribution of each psychological determinant while controlling for the others and enables a direct comparison of how predictor importance varies across low-, moderate-, and high-sensitivity data types.

Analyzing each data category individually is methodologically justified for two reasons. First, prior results showed that disclosure behavior clusters differently across data types, indicating that consumers distinguish sharply between information perceived as low-risk (e.g., contact and demographic data) and highly sensitive information (e.g., medical and financial data). Second, the privacy calculus framework suggests that the balance between perceived risks and benefits may shift depending on the context and sensitivity of the data requested. Consequently, predictors such as perceived benefits may dominate disclosure decisions for low-sensitivity data, whereas privacy concerns and perceived control may play a stronger role for highly sensitive data.

The following tables present the results of the regression analyses for each personal data category, grouped by sensitivity level. This structure enables a systematic comparison of disclosure drivers and provides deeper insight into how trust in brand, perceived control over personal data, privacy concerns, and perceived benefits of personalization jointly shape consumers' willingness to disclose different types of personal data in permission-based marketing contexts. The regression results are presented separately for low-, moderate-, and high-sensitivity personal data categories. For each sensitivity group, standardized regression coefficients (β), significance levels (p-values), and model fit indicators (R^2 and adjusted R^2) are reported. All predictors were entered simultaneously using the enter method to assess their unique contribution to willingness to disclose each type of personal data while controlling for the remaining predictors.

Table 9. *Multiple Regression Results for Willingness to Disclose Low-Sensitivity Personal Data*

Predictor	**Contact Information Data**	**Demographic Data**	**Preferences Data of Receiving Content methods**
Trust in Brand (β)	0.293 (p<0.001)	0.200 (p<0.001)	0.005 (p=0.919)
Perceived Control over Personal Data (β)	-0.029 (p<0.627)	0.090 (p=0.135)	0.095 (p=0.125)
Privacy Concerns (β)	-0.091 (p=0.131)	0.012 (p=0.845)	-0.028 (p=0.646)
Perceived Benefits of Personalization (β)	0.136 (p=0.003)	0.231 (p<0.001)	0.295 (p<0.001)
R^2	0.163	0.161	0.116
Adjusted R^2	0.156	0.155	0.109
Model p (ANOVA)	<0.001	<0.001	<0.001

Note. Standardized regression coefficients (β) reported. Dependent variables: willingness to disclose each low-sensitivity personal data type.

As seen in Table 9, the results for low-sensitivity personal data reveal a differentiated pattern across data types, despite all models being statistically significant overall ($p < 0.001$). For contact information and demographic data, **trust in brand** emerged as a strong and significant positive predictor ($\beta = 0.293$ and $\beta = 0.200$, respectively; $p < 0.001$), indicating that brand-related trust plays an important role when consumers are asked to disclose basic identifying information. In contrast, trust in brand was not significant for preferences related to receiving content, suggesting that trust becomes less relevant when the requested data is perceived as less directly linked to personal identification.

Across all three low-sensitivity data types, **perceived benefits of personalization** showed consistent and statistically significant positive effects, with the strongest influence observed for preferences related to receiving content ($\beta = 0.295$, $p < .001$). This indicates that even for data perceived as relatively low risk, consumers' willingness to disclose is largely driven by value considerations. **Privacy concerns and perceived control over personal data** did not significantly predict disclosure in any of the low-sensitivity models, suggesting that risk-related considerations are less salient when consumers evaluate disclosure of information perceived as routine or minimally intrusive. Overall, the explanatory power of the models was moderate, with adjusted R^2 values ranging from 0.109 to 0.156.

***Table 10**. Multiple Regression Results for Willingness to Disclose Moderate-Sensitivity Personal Data*

Predictor	**Online Behavioral Data / Cookies**	**Live Location Data**	**Social Networking Data**	**Profile and views data**
Trust in Brand (β)	0.088 (p=0.081)	0.032 (p=0.538)	0.015 (p=0.771)	-0.011 (p=0.827)
Perceived Control over Personal Data (β)	0.025 (p=0.685)	-0.051 (p=0.417)	0.078 (p=0.203)	0.170 (p=0.005)
Privacy Concerns (β)	-0.107 (p=0.077)	-0.144 (p=0.023)	-0.013 (p=0.828)	0.054 (p=0.369)
Perceived Benefits of Personalization (β)	0.277 (p<0.001)	0.214 (p<0.001)	0.335 (p<0.001)	0.346 (p<0.001)
R^2	0.145	0.075	0.137	0.150
Adjusted R^2	0.138	0.068	0.130	0.143
Model p (ANOVA)	<0.001	<0.001	<0.001	<0.001

Note. Standardized regression coefficients (β) reported. Dependent variables: willingness to disclose each moderate-sensitivity personal data type.

As seen in Table 10, for moderate-sensitivity personal data, the regression results indicate a shift in the relative importance of predictors across data types. While all models were statistically significant ($p < 0.001$), **perceived benefits of personalization** emerged as the most consistent and strongest predictor across all four categories, with standardized coefficients ranging from $\beta = 0.214$ to $\beta = 0.346$ (all $p < .001$). This highlights that perceived value remains a central driver of disclosure even as data sensitivity increases, particularly for social networking data and profile or view data.

In contrast, **trust in brand** generally exhibited weak and non-significant effects across moderate-sensitivity data types, indicating that trust alone is insufficient to encourage disclosure of more intrusive data. **Privacy concerns** showed a significant negative effect only for live location data ($\beta = -0.144$, $p = 0.023$), suggesting heightened risk sensitivity when real-time or continuous tracking information is involved. Additionally, **perceived control over personal data** was significant only for profile and views data ($\beta = 0.170$, $p = 0.005$), indicating that feelings of control become relevant for certain types of moderately sensitive information. The models explained between 6.8% and 14.3% of variance (adjusted R^2), reflecting greater heterogeneity in disclosure drivers compared to low-sensitivity data.

Table 11. *Multiple Regression Results for Willingness to Disclose High-Sensitivity Personal Data*

Predictor	**Medical Data**	**Financial Data**
Trust in Brand (β)	-0.060 (p=0.249)	-0.092 (p=0.080)
Perceived Control over Personal Data (β)	0.035 (p=0.571)	0.095 (p=0.132)
Privacy Concerns (β)	0.011 (p=0.861)	0.023 (p=0.718)
Perceived Benefits of Personalization (β)	0.312 (p<0.001)	0.287 (p<0.001)
R^2	0.086	0.076
Adjusted R^2	0.079	0.068
Model p (ANOVA)	<0.001	<0.001

Note. Standardized regression coefficients (β) reported. Dependent variables: willingness to disclose each high-sensitivity personal data type.

In Table 11, the results for high-sensitivity personal data demonstrate a markedly constrained disclosure pattern. Although both models were statistically significant overall ($p < .001$), **perceived benefits of personalization** was the only predictor that consistently and significantly influenced willingness to disclose both medical data ($\beta = 0.312$, $p < .001$) and financial data ($\beta = 0.287$, $p < .001$). This suggests that even for highly sensitive information, perceived value can motivate disclosure, though within a generally lower explanatory framework.

Notably, **trust in brand, perceived control over personal data**, and **privacy concerns** did not reach statistical significance in either model. This finding indicates that for highly sensitive data, traditional trust- and risk-related predictors may no longer function as decisive factors once a certain sensitivity threshold is reached. Instead, consumers' willingness to disclose appears to be driven primarily by strong perceived benefits, while overall disclosure remains limited, as reflected in the relatively low adjusted R^2 values (0.068-0.079). These results point to a fundamentally different decision logic governing high-sensitivity data disclosure compared to lower-sensitivity categories.

The analyses of willingness to disclose different types of personal data reveal a clear sensitivity-based structure in disclosure behavior. Descriptive and correlational results indicate a hierarchical pattern, with low-sensitivity data disclosed more readily and highly sensitive data approached with substantial caution, while moderate- and high-sensitivity data types show stronger interrelationships. Regression analyses further demonstrate that the drivers of disclosure vary across data types: perceived benefits of personalization remain a consistent motivator, whereas trust in brand, perceived control, and privacy concerns display selective and context-

dependent effects. These findings confirm that personal data disclosure is a differentiated decision process shaped by data sensitivity and individual privacy evaluations, providing a strong empirical rationale for the subsequent clustering analysis aimed at identifying distinct disclosure-related consumer segments.

3.3.4. Cluster Analysis of Psychological Determinants of Personal Data Disclosure

To identify distinct consumer segments based on privacy-related psychological characteristics, a cluster analysis was conducted using **trust in brand, perceived control over personal data, privacy concerns, and perceived benefits of personalization**. All clustering variables were standardized (z-scores) prior to analysis to ensure equal contribution of each construct to the distance calculations used in the clustering procedure. The cluster analysis was conducted as an exploratory procedure to identify patterns of heterogeneity in disclosure behavior rather than to test additional hypotheses.

Trust in technologies and trust in government were not included in the clustering variables for two reasons. First, prior hypothesis testing showed that these constructs played a limited or indirect role in explaining privacy concerns, perceived control, and willingness to disclose personal data when individual-level perceptions were accounted for. Second, the clustering aimed to capture consumer segments based on proximal psychological drivers of disclosure decisions, in line with privacy calculus theory. Including broader institutional trust variables risked diluting cluster interpretability without adding explanatory value.

A hierarchical clustering procedure using Ward's method and squared Euclidean distance was first applied to determine the appropriate number of clusters. Inspection of the agglomeration schedule revealed a pronounced increase in fusion coefficients at the final merging stages, indicating that a **three-cluster solution** best represented the underlying data structure. Based on this result, a K-means cluster analysis specifying three clusters was subsequently conducted to finalize cluster membership. The final cluster centers served as the basis for interpreting and labeling the clusters.

Cluster 1: Trusting, empowered, low-concern users

This cluster is characterized by very low privacy concerns ($z = -0.97$), above-average trust in brand ($z = 0.49$), slightly above-average perceived benefits of personalization ($z = 0.14$), and very high perceived control over personal data ($z = 1.00$). Individuals in this group combine low privacy anxiety with strong feelings of control and trust, suggesting a confident disclosure

orientation. Their privacy calculus appears favorable, as low perceived risk and high control reduce resistance to data sharing.

Cluster 2: Benefit-driven but cautious users

Cluster 2 exhibits moderately elevated privacy concerns (z = 0.42), slightly above-average trust in brand (z = 0.24), strongly perceived benefits of personalization (z = 0.64), and moderately below-average perceived control (z = -0.41). This profile reflects a balanced privacy calculus, in which strong perceived benefits motivate disclosure despite some privacy concerns and a less pronounced sense of control. Disclosure decisions in this group are therefore likely to be deliberate and context-dependent rather than automatic.

Cluster 3: Privacy-concerned, low-trust, low-benefit users

This cluster is defined by high privacy concerns (z = 0.66), low trust in brand (z = -0.92), low perceived benefits of personalization (z = -1.02), and low perceived control over personal data (z = -0.71). This configuration represents a distinctly unfavorable privacy calculus, in which both perceived risks and perceived benefits are evaluated negatively. As a result, individuals in this group are likely to be highly reluctant to disclose personal data and to approach permission-based marketing with skepticism. Disclosure, if it occurs, is expected to be highly conditional and limited to situations involving strong guarantees of control, transparency, and minimal data sensitivity.

Table 12. *Final Cluster Centers (z-scores)*

	Cluster 1	**Cluster 2**	**Cluster 3**
Privacy Concerns	-0.97	0.42	0.66
Trust in Brand	0.49	0.24	-0.92
Perceived Benefits of Personalization	0.14	0.64	-1.02
Perceived Control over Personal Data	1.00	-0.41	-0.71

To assess whether these psychologically distinct clusters also differ in disclosure behavior, Kruskal-Wallis tests were conducted. This non-parametric approach was appropriate given the categorical nature of cluster membership and the non-normal distribution of willingness-to-disclose measures. Three disclosure indices were examined, corresponding to low-, moderate-, and high-sensitivity personal data categories identified in earlier analyses.

As seen in Table 13, the results revealed statistically significant differences across clusters for all three data sensitivity levels. For low-sensitivity personal data, Cluster 1 exhibited the highest willingness to disclose, followed by Cluster 2, while Cluster 3 showed substantially lower willingness. A similar pattern emerged for moderate-sensitivity data, with Clusters 1 and 2 demonstrating comparably high willingness and Cluster 3 remaining markedly more reluctant. For high-sensitivity data, overall differences across clusters were smaller but remained statistically significant, with Cluster 2 exhibiting the highest willingness to disclose medical and financial data, followed closely by Cluster 1, and Cluster 3 again displaying the lowest willingness.

Table 13. *Differences in Willingness to Disclose Personal Data Across Clusters by Data Sensitivity*

Data Sensitivity Level	**Kruskal-Wallis H**	**df**	**p-value**	**Mean Rank: Cluster 1**	**Mean Rank: Cluster 2**	**Mean Rank: Cluster 3**
Low sensitivity	67.971	2	<0.001	294.32	275.96	167.57
Moderate sensitivity	68.589	2	<0.001	287.36	283.54	166.26
High sensitivity	19.944	2	<0.001	261.82	274.66	209.85

Overall, the clustering analysis demonstrates that consumers differ systematically in how they evaluate privacy concern, perceived benefits of personalization, trust in brand, and perceived control over personal data, resulting in distinct disclosure behaviors across data sensitivity levels. High-trust, empowered, and low-concern users exhibit consistently high willingness to disclose personal data, particularly for low- and moderate-sensitivity information, making them well suited for personalization-driven marketing initiatives and loyalty programs. In contrast, privacy-concerned and low-trust users show markedly lower willingness to disclose across all data categories, indicating that data requests targeting this segment require enhanced transparency, stronger assurances of control, and clearly communicated value propositions. Benefit-driven but cautious users occupy an intermediate position, remaining receptive to data sharing, especially for highly sensitive information, when perceived benefits are sufficiently salient. Importantly, the findings highlight that disclosure strategies should be differentiated not only by consumer segment but also by data sensitivity, as the effectiveness of trust cues, benefit framing, and control mechanisms varies depending on the type of personal data requested. These results reinforce the view that permission-based marketing is most effective when both psychological profiles and data sensitivity are jointly considered.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions:

1. The analysis of scientific literature demonstrated that permission-based marketing relies fundamentally on consumers' willingness to disclose personal data, which is shaped by a trade-off between perceived risks and perceived benefits, as described by Privacy Calculus Theory. Prior research consistently highlights trust in brand as a key factor reducing privacy concerns, while trust in government and trust in technologies are discussed more inconsistently and often examined in isolation. The literature also indicates that personal data are not perceived uniformly, as consumers distinguish between data types based on sensitivity. These findings provided the theoretical foundation for developing the research model of this thesis.

2. Theoretical analysis further revealed that perceived control over personal data plays a central role in shaping privacy-related evaluations and trust formation. Commitment–Trust Theory and Trust Transfer Theory support the assumption that trust is multidimensional and embedded within broader technological and institutional contexts. However, the literature lacks consensus regarding how different trust dimensions jointly influence disclosure decisions in permission-based marketing. This gap justified the empirical focus of the study on integrating trust in brand, government, and technologies within a single analytical framework.

3. Empirical results confirmed that perceived control over personal data is the strongest predictor of privacy concerns, indicating that individuals who feel empowered to manage their data experience significantly lower privacy anxiety. Trust in brand also contributes independently to reducing privacy concerns, whereas trust in government and trust in technologies do not exhibit direct effects when individual-level perceptions are considered. These findings suggest that personal perceptions of control and relational trust are more influential than broader institutional trust in shaping privacy concerns, with perceived control also reinforcing trust in brand at the individual level.

4. The results further showed that perceived benefits of personalization are the primary driver of consumers' willingness to disclose personal data. When multiple predictors were considered simultaneously, trust in brand, privacy concerns, and perceived control did not exert significant direct effects on disclosure intentions, whereas perceived benefits remained a strong and consistent predictor. This supports the core mechanism of Privacy Calculus Theory, emphasizing a risk–benefit evaluation rather than trust alone as the dominant driver of disclosure behavior.

5. Analysis of willingness to disclose different types of personal data revealed a clear sensitivity-based hierarchy. Consumers were most willing to disclose low-sensitivity data, such as contact information and demographics, while medical and financial data were approached with substantial caution. Correlation patterns indicated that low-sensitivity data disclosure operates largely independently from highly sensitive data, whereas moderate- and high-sensitivity data tend to cluster together, confirming that personal data disclosure is not a uniform behavior.

6. Regression analyses across data sensitivity levels demonstrated that predictors of disclosure vary depending on the type of data requested. Perceived benefits of personalization remained a consistent motivator across all data categories, while trust in brand, perceived control, and privacy concerns exerted selective and context-dependent effects. These findings indicate that consumers' privacy calculus is adjusted according to data sensitivity rather than applied uniformly across all disclosure decisions.

7. The cluster analysis identified three distinct consumer segments characterized by systematically different configurations of brand trust, privacy concerns, perceived private data control, and perceived benefits of personalization. These psychological profiles translated into meaningful differences in willingness to disclose personal data across sensitivity levels. The results highlight substantial heterogeneity in permission-based data disclosure and demonstrate that consumers cannot be treated as a homogeneous group when designing data collection strategies.

Recommendations:

1. Businesses implementing permission-based marketing should prioritize enhancing perceived benefits of personalization, as this factor consistently motivates data disclosure across all data types. Personalized value propositions should clearly communicate relevance, convenience, and usefulness to consumers. Emphasizing tangible benefits may be more effective than relying solely on trust cues.

2. Organizations should strengthen consumers' perceived control over personal data by offering transparent consent mechanisms, clear data management options, and easily accessible privacy settings. Increasing users' sense of control can significantly reduce privacy concerns and indirectly support data-sharing intentions. Control-oriented design should be treated as a core component of ethical data practices.

3. Marketing strategies should differentiate data requests based on sensitivity levels rather than applying uniform opt-in approaches. Low-sensitivity data may be requested with minimal resistance, while requests for highly sensitive data should be accompanied by stronger assurances,

clear justifications, and additional safeguards. Sensitivity-based communication can help align data practices with consumer expectations.

4. Firms should tailor permission-based marketing strategies to different consumer segments identified through psychological profiling. Trusting and empowered users may be suitable for more advanced personalization, while privacy-concerned users require enhanced transparency and reduced data demands. Segment-specific approaches can improve both consumer trust and campaign effectiveness.

5. Policymakers and regulators should focus not only on formal compliance measures but also on initiatives that enhance individuals' perceived control and understanding of data practices. Clear communication of data rights and practical enforcement mechanisms may help translate regulatory protection into subjective consumer confidence. Strengthening perceived effectiveness of regulation may support long-term trust development.

6. Future research should extend this study by examining permission-based data disclosure across different cultural and national contexts to assess the generalizability of the findings. Comparative studies could reveal whether trust and privacy mechanisms operate similarly under different regulatory and technological environments. Cross-country research would enrich the understanding of contextual influences on data disclosure behavior.

7. Further studies could employ longitudinal designs to examine how trust, privacy concerns, and disclosure behavior evolve over time, particularly in response to regulatory changes or data breaches. Additionally, experimental approaches could be used to test causal effects of perceived benefits and control mechanisms. Such research would deepen insights into the dynamic nature of privacy calculus in digital marketing context.

LIST OF REFERENCES

Abashidze, I. (2023). Permission Marketing Strategy Shaping Consumer Behaviour Through Online Communication Channels. *Baltic Journal of Economic Studies*, *9*(2), 8–18. https://doi.org/10.30525/2256-0742/2023-9-2-8-18

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. *Action Control*, 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Anic, I. D., Budak, J., Rajh, E., Recher, V., Skare, V., & Skrinjaric, B. (2019). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281/FULL/PDF

Ashworth, L., & Free, C. (2006). Marketing Dataveillance and Digital Privacy : Using Theories of Justice to Understand Consumers ' Online Privacy Concerns. *Journal of Business Ethics*, 107–123. https://doi.org/10.1007/s10551-006-9007-7

Bamba, F., & Barnes, S. J. (2007). SMS advertising, permission and the consumer: a study. *Business Process Management Journal*. https://doi.org/10.1108/14637150710834578

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1–21. https://doi.org/10.1016/J.IM.2015.08.001

Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, *27*(6), 2233–2242. https://doi.org/10.1016/J.CHB.2011.07.002

Bhatia, V. (2020). Drivers and barriers of permission-based marketing. *Journal of Research in Interactive Marketing*, *14*(1), 51–70. https://doi.org/10.1108/JRIM-07-2018-0088/FULL/PDF

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, *46*(3), 363–376. https://doi.org/10.1080/00913367.2017.1339368

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Brey, E. T., So, S. I. (Amy), Kim, D. Y., & Morrison, A. M. (2007). Web-based permission marketing: Segmentation for the lodging industry. *Tourism Management*, *28*(6), 1408–1416. https://doi.org/10.1016/J.TOURMAN.2007.01.002

Brown, J. R., Crosno, J. L., & Tong, P. Y. (2019). Is the theory of trust and commitment in marketing relationships incomplete? *Industrial Marketing Management*, *77*, 155–169. https://doi.org/10.1016/J.INDMARMAN.2018.10.005

Carroll, A., Barnes, S. J., Scornavacca, E., & Fletcher, K. (2007). Consumer perceptions and attitudes towards SMS advertising: recent evidence from New Zealand. *International Journal of Advertising*, *26*(1), 79–98. https://doi.org/10.1080/02650487.2007.11072997

Castelfranchi, C., & Falcone, R. (2011). Socio-Cognitive Theory of Trust. *Wiley*, *October 2011*, 58–89.

Chaudhuri, A., & Holbrook, M. B. (2001). The chain of effects from brand trust and brand affect to brand performance: The role of brand loyalty. *Journal of Marketing*, *65*(2), 81–93. https://doi.org/10.1509/jmkg.65.2.81.18255

Colesca, S. E. (2009). Increasing E-Trust: a Solution to Minimize Risk in E-Government Adoption. *Journal of Applied Quantitative Methods*, *4*(1).

Degutis, M., Urbonavicius, S., Zimaitis, I., Skare, V., & Laurutyte, D. (2020). Willingness to Disclose Personal Information: How to Measure it? *Engineering Economics*, *31*(4), 487–494. https://doi.org/10.5755/J01.EE.31.4.25168

DuFrene, D. D., Engelland, B. T., Lehman, C. M., & Pearson, R. A. (2005). Changes in Consumer Attitudes Resulting from Participation in a Permission E-mail Campaign. *Journal of Current Issues & Research in Advertising*, *27*(1), 65–77. https://doi.org/10.1080/10641734.2005.10505174

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, *65*(September 2020), 101717. https://doi.org/10.1016/j.tele.2021.101717

Gupta, B., Lyer, L., & Weisskirch, R. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the U.S. and in India. *Journal of Electronic Commerce Research*.

Hajli, N., Sims, J., Zadeh, A. H., & Richard, M. O. (2017). A social commerce investigation of the role of trust in a social networking site on purchase intentions. *Journal of Business Research*, *71*, 133–141. https://doi.org/10.1016/J.JBUSRES.2016.10.004

Hassan, I. B., Azrifah, M., Murad, A., El-shekeil, I., & Liu, J. (2022). Extending the UTAUT2 Model with a Privacy Calculus Model. *Informatics (Mdpi)*, *9*(31).

Heirman, W., Walrave, M., Ponnet, K., & Van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology Journal of Psychosocial Research on Cyberspace*, *7*(3). https://doi.org/10.5817/CP2013-3-3

Herian, M. N., Shank, N. C., & Abdel-Monem, T. L. (2014). Trust in government and support for governmental regulation: the case of electronic health records. *Health Expectations*, *17*(6), 784–794. https://doi.org/10.1111/J.1369-7625.2012.00803.X

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics*, *168*(3), 539–564. https://doi.org/10.1007/S10551-019-04237-1/TABLES/10

Im, H., & Ha, Y. (2013). Enablers and inhibitors of permission-based marketing: A case of mobile coupons. *Journal of Retailing and Consumer Services*. https://doi.org/10.1016/j.jretconser.2013.05.002

Jayawardhena, C., Kuckertz, A., Karjaluoto, H., & Kautonen, T. (2009). Antecedents to permission based mobile marketing: An initial examination. *European Journal of Marketing*, *43*(3–4), 473–499. https://doi.org/10.1108/03090560910935541/FULL/PDF

Jolley, W., Lee, A., Mizerski, R., & Sadeque, S. (2013). Permission email messages significantly increase gambler retention. *Journal of Business Research*, *66*(9), 1617–1622. https://doi.org/10.1016/J.JBUSRES.2012.12.006

Karjaluoto, H., Lehto, H., Leppa¨niemi, M., Leppa¨niemi, L., & Jayawardhena, C. (2008). Exploring Gender Influence on Customer's Intention to Engage Permission-based Mobile Marketing. *Electronic Markets*, *18*(3). https://doi.org/10.1080/10196780802265793

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/ISJ.12062

Kenning, P. (2008). The influence of general trust and specific trust on buying behaviour. *International Journal of Retail and Distribution Management*, *36*(6), 461–476. https://doi.org/10.1108/09590550810873938

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission Marketing and Privacy Concerns - Why Do Customers (Not) Grant Permissions? *Journal of Interactive Marketing*. https://doi.org/10.1016/j.intmar.2017.03.001

Krafft, M., Kumar, V., Harmeling, C., Singh, S., Zhu, T., Chen, J., Duncan, T., Fortin, W., & Rosa, E. (2021). Insight is power: Understanding the terms of the consumer-firm data exchange. *Journal of Retailing*, *97*(1), 133–149. https://doi.org/10.1016/J.JRETAI.2020.11.001

Krishnamurthy, S. (2001). A comprehensive analysis of permission marketing. *Journal of Computer-Mediated Communication*, *6*(2). https://doi.org/10.1111/J.1083-6101.2001.TB00119.X/4584249

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

Kurtz, O. T., Wirtz, B. W., & Langer, P. F. (2021). An Empirical Analysis of Location-Based Mobile Advertising—Determinants, Success Factors, and Moderating Effects. *Journal of Interactive Marketing*, *54*, 69–85. https://doi.org/10.1016/J.INTMAR.2020.08.001

Lankton, N. K., Harrison McKnight, D., Wright, R. T., & Thatcher, J. B. (2016). Using expectation disconfirmation theory and polynomial modeling to understand trust in technology. *Information Systems Research*, *27*(1), 197–213. https://doi.org/10.1287/ISRE.2015.0611

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*(1), 343–354. https://doi.org/10.1016/J.DSS.2013.09.018

Lithuanian Official Statistics Portal. (2025, November 30). *Lithuanian Official Statistics Portal* .

Luo, Y., Li, X., & Ye, Q. (2023). the Impact of Privacy Calculus and Trust on User Information Participation Behavior in Ai-Based Medical Consultation-the Moderating Role of Gender. *Journal of Electronic Commerce Research*, *24*(1), 48–67.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. https://doi.org/10.1007/S11747-006-0003-3

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792

Metcalfe, M., Nager, J., & Hacker, C. S. (2023). Trust Framework for Data Sharing between Industry and Government. *Integrated Communications, Navigation and Surveillance Conference, ICNS*, *2023-April*. https://doi.org/10.1109/ICNS58246.2023.10124290

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi.org/10.1016/J.IM.2015.06.006

Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, *58*(3), 20. https://doi.org/10.2307/1252308

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. https://doi.org/10.1111/J.1745-6606.2006.00070.X

O'Cass, A., & Carlson, J. (2012). An e-retailing assessment of perceived website-service innovativeness: Implications for website quality evaluations, trust, loyalty and word of mouth. *Australasian Marketing Journal*, *20*(1), 28–36. https://doi.org/10.1016/j.ausmj.2011.10.012

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262. https://doi.org/10.1016/S0167-4870(02)00172-1

Ozyilmaz, A., Erdogan, B., & Karaeminogullari, A. (2018). Trust in organization as a moderator of the relationship between self-efficacy and workplace outcomes: A social cognitive theory-based examination. *Journal of Occupational and Organizational Psychology*, *91*(1), 181–204. https://doi.org/10.1111/joop.12189

Pandey, J. K. (2023). Public trust and collaborative e-governance performance: a study on government institutions and services. *Transforming Government: People, Process and Policy*, *17*(4), 510–531. https://doi.org/10.1108/TG-08-2023-0113/FULL/PDF

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Penaloza, L. (2006). Association for consumer research. *Advances in Consumer Research*, *33*, 212–218.

Perdereaux-Weekes, A. W. (2021). *To Investigate the Impact of Data Privacy Regulation on Disclosure Decisions: Examining Consumers' Willingness to Share or Withhold Personal Identifiable Information in the Wake of GDPR, CCPA, and LGDP*. St. Thomas University.

Popova, N., Kataiev, A., Skrynkovskyy, R., & Nevertii, A. (2019). Development of trust marketing in the digital society. *Economic Annals-XXI*, *176*(3–4), 13–25. https://doi.org/10.21003/ea.V176-02

Raimondo, M. (2000). The Measurement of Trust in Marketing Studies: a Review of Models and Methodologies. *16th IMP-Conference, Bath, UK*, 1–43.

Robinson, C. (2016). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582. https://doi.org/10.1016/J.TELE.2016.09.006

Robinson, C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 214–233. https://doi.org/10.1080/10919392.2018.1482601

Rohunen, A., Markkula, J., Heikkilä, M., & Oivo, M. (2020). Explaining Diversity and Conflicts in Privacy Behavior Models. *Journal of Computer Information Systems*, *60*(4), 378–393. https://doi.org/10.1080/08874417.2018.1496804

Rowley, J. (2004). Just another channel? Marketing communications in e-business. *Marketing Intelligence & Planning*, *22*(1), 24–41. https://doi.org/10.1108/02634500410516896/FULL/PDF

Schunk, D. H., & DiBenedetto, M. K. (2020). Motivation and social cognitive theory. *Contemporary Educational Psychology*, *60*(December 2019), 101832. https://doi.org/10.1016/j.cedpsych.2019.101832

Song, C., & Lee, J. (2016). Citizens' Use of Social Media in Government, Perceived Transparency, and Trust in Government. *Public Performance & Management Review*, *39*(2), 430–453. https://doi.org/10.1080/15309576.2015.1108798

Swain, S., Jebarajakirthy, C., Maseeh, H. I., Saha, R., Gupta, N., & Grover, R. (2023). Permission marketing: a systematic review of 22 Years of research. *Marketing Intelligence & Planning*. https://doi.org/10.1108/MIP-05-2022-0187

Tesseras, L. (2019). Has GDPR improved brand experience? Most consumers aren't convinced. *2019*. https://www.marketingweek.com/consumers-gdpr-brand-experience/

Tezinde, T., Smith, B., & Murphy, J. (2002). Getting permission: Exploring factors affecting permission marketing. *Journal of Interactive Marketing*, *16*(4), 28–36. https://doi.org/10.1002/DIR.10041

Theocharidis, A. I., Argyropoulou, M., Karavasilis, G., Vrana, V., & Kehris, E. (2020). An approach towards investigating factors affecting intention to book a hotel room through social media. *Sustainability (Switzerland)*, *12*(21), 1–20. https://doi.org/10.3390/SU12218973

Treiblmaier, H., & Chong, S. (2011). Trust and perceived risk of personal information as antecedents of online information disclosure: Results from three countries. *Journal of Global Information Management*, *19*(4), 76–94. https://doi.org/10.4018/JGIM.2011100104

Trein, P., & Varone, F. (2024). Citizens' agreement to share personal data for public policies: trust and issue importance. *Journal of European Public Policy*, *31*(9), 2483–2508. https://doi.org/10.1080/13501763.2023.2205434/ASSET/0AD7AD4D-16BD-436C-97F9-E61414377808/ASSETS/GRAPHIC/RJPP_A_2205434_F0003_OB.JPG

Tsang, M. M., Ho, S. C., & Liang, T. P. (2004). Consumer Attitudes Toward Mobile Advertising: An Empirical Study. *International Journal of Electronic Commerce*, *8*(3), 65–78. https://doi.org/10.1080/10864415.2004.11044301

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, *136*, 76–85. https://doi.org/10.1016/J.JBUSRES.2021.07.031

Venkatesh, V., Thong, J. Y. L., & Xin, X. (2012a). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly: Management Information Systems*, *36*(1), 157–178.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174. https://doi.org/10.1016/J.JSIS.2013.01.003

Walrave, M., & Heirman, W. (2013). Adolescents, Online Marketing and Privacy: Predicting Adolescents' Willingness to Disclose Personal Information for Marketing Purposes. *Children & Society*, *27*(6), 434–447. https://doi.org/10.1111/J.1099-0860.2011.00423.X

Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), 63–70. https://doi.org/10.1145/272287.272299

Wang, N., Zhao, Y., Zhou, R., & Li, Y. (2022). Factors influencing users' online information disclosure intention and the moderating effect of cultural background and platform type. *Journal of Information Management*, *75*(6), 1178–1208. https://doi.org/10.1108/AJIM-04-2022-0218

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542. https://doi.org/10.1016/J.IJINFOMGT.2016.03.003

Watson, C., McCarthy, J., & Rowley, J. (2013). Consumer attitudes towards mobile marketing in the smart phone era. *International Journal of Information Management*, *33*(5), 840–849. https://doi.org/10.1016/J.IJINFOMGT.2013.06.004

Xu, H., Dinev, T., Jeff Smith, H., & Hart, P. J. (2008). *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View.*

Yakut, E. (2019). A Social Cognitive Theory Perspective on Marketing Studies: A Literature Review. *Yaşar Üniversitesi E-Dergisi*, *14*(October), 18–43.

Zhang, X., Kumar, V., & Cosguner, K. (2017). Dynamically managing a profitable email marketing program. *Journal of Marketing Research*, *54*(6), 851–866. https://doi.org/10.1509/JMR.16.0210

Zhao, J., Huang, J., & Su, S. (2019). The effects of trust on consumers' continuous purchase intentions in C2C social commerce: A trust transfer perspective. *Journal of Retailing and Consumer Services*, *50*(October 2018), 42–49.

Zimaitis, I., Urbonavičius, S., Degutis, M., & Kaduškevičiūtė, V. (2022a). Influence of trust and conspiracy beliefs on the disclosure of personal data online. *Journal of Business Economics and Management.*, *23*(3), 551–568. https://doi.org/10.3846/JBEM.2022.16119

Zsigmondová, A., Zsigmond, T., & Machová, R. (2021). Theoretical Background to the Role of Trust in Marketing. *SHS Web of Conferences*, *115*, 03019. https://doi.org/10.1051/shsconf/202111503019

ANNEX 1 – MASTER THESIS SUMMARY IN ENGLISH

THE IMPACT OF TRUST ON CONSUMER'S WILLINGNESS TO DISCLOSE PERSONAL DATA TO BRANDS IN PERMISSION-BASED MARKETING

DANIELIUS ALIAŠEVIČIUS

Master thesis

Marketing and Integrated Communication

Vilnius University, Faculty of Economics and Business Administration

Supervisor – assoc. prof. dr. Mindaugas Degutis

Vilnius, 2026

SUMMARY

73 pages, 11 figures, 13 tables, 83 references.

The aim of this master's thesis is to examine how trust-related factors influence consumers' willingness to disclose personal data in the context of permission-based marketing. The study focuses on trust in brand, trust in government, trust in technologies, privacy concerns, perceived control over personal data, perceived benefits of personalization, and differences in disclosure behavior across types of personal data with varying sensitivity levels.

The thesis consists of three main parts: a literature analysis, an empirical research section, and conclusions with recommendations. The literature review is grounded in Privacy Calculus Theory, Commitment–Trust Theory, Trust Transfer Theory, and technology-related trust frameworks, emphasizing the role of trust, perceived risks and benefits, and the heterogeneity of personal data in disclosure decisions.

Empirical research was conducted using a quantitative survey of Lithuanian consumers familiar with an urban mobility service provider "Bolt". Data were analyzed using IBM SPSS Statistics. The results indicate that perceived control over personal data is the strongest predictor of privacy concerns ($\beta = -0.670$), while trust in brand also significantly reduces privacy concerns ($\beta=-0.129$). In contrast, trust in government and trust in technologies do not exhibit direct effects in the model. Furthermore, perceived benefits of personalization emerge as the most important driver of consumers' willingness to disclose personal data ($\beta = 0.391$).

Analysis across data types reveals a clear sensitivity-based hierarchy. Consumers are most willing to disclose low-sensitivity data, such as contact information ($M = 4.36$), and least willing to share highly sensitive data, such as medical ($M = 1.94$) and financial data ($M = 1.82$). Cluster analysis identifies three distinct consumer segments with systematically different privacy-related profiles, confirming that disclosure behavior varies significantly across consumer groups.

In the conclusions and recommendations, the study highlights the importance of perceived benefits and perceived control in permission-based marketing and emphasizes the need for sensitivity-based and segment-specific data collection strategies. The results provide practical guidance for designing transparent and trust-enhancing data practices and contribute to the academic understanding of personal data disclosure behavior.

ANNEX 2 – MASTER THESIS SUMMARY IN LITHUANIAN

PASITIKĖJIMO ĮTAKA VARTOTOJŲ NORUI PERDUOTI ASMENS DUOMENIS PREKIŲ ŽENKLAMS LEIDIMAIS GRĮSTOJE RINKODAROJE

DANIELIUS ALIAŠEVIČIUS

Magistro baigiamasis darbas

Rinkodara ir integruota komunikacija

Vilniauus universiteto Ekonomikos ir verslo administravimo fakultetas

Darbo vadovas – assoc. prof. dr. Mindaugas Degutis

Vilnius, 2026

SANTRAUKA

73 puslapiai, 11 paveikslėlių, 13 lentelių, 83 literatūros šaltiniai.

Šio magistro baigiamojo darbo tikslas – ištirti, kaip su pasitikėjimu susiję veiksniai veikia vartotojų norui atskleisti asmens duomenis prekių ženklams leidimais grįstoje rinkodaros kontekste. Tyrime analizuojamas pasitikėjimas prekės ženklu, pasitikėjimas valdžios institucijomis, pasitikėjimas technologijomis, privatumo susirūpinimas, suvokiama asmens duomenų kontrolė, suvokiama suasmeninimo nauda bei asmens duomenų atskleidimo skirtumai priklausomai nuo duomenų jautrumo lygio.

Darbą sudaro trys pagrindinės dalys: mokslinės literatūros analizė, empirinio tyrimo metodologija ir rezultatų analizė bei išvados su pasiūlymais. Literatūros apžvalga grindžiama Privatumo skaičiavimo teorija (Privacy Calculus Theory), Įsipareigojimo–pasitikėjimo teorija (Commitment–Trust Theory), Pasitikėjimo perdavimo teorija (Trust Transfer Theory) bei su technologijomis susijusiais pasitikėjimo modeliais. Analizuojant literatūrą pabrėžiamas pasitikėjimo, suvokiamos rizikos ir naudos vaidmenys bei asmens duomenų nevienalytiškumas sprendžiant dėl jų atskleidimo.

Empirinis tyrimas atliktas taikant kiekybinį metodą – apklausti Lietuvos vartotojai, susipažinę su miesto mobilumo paslaugų teikėju „Bolt“. Duomenys analizuoti naudojant IBM SPSS Statistics programą. Tyrimo rezultatai parodė, kad suvokiama asmens duomenų kontrolė yra stipriausias privatumo susirūpinimo veiksnys ($\beta = -0.670$), o pasitikėjimas prekės ženklu taip pat reikšmingai mažina privatumo susirūpinimą ($\beta = -0.129$). Tuo tarpu pasitikėjimas valdžios institucijomis ir pasitikėjimas technologijomis tiesioginio poveikio tiriamame modelyje neparodė. Be to, nustatyta, kad suvokiama suasmeninimo nauda yra svarbiausias vartotojų norui atskleisti asmens duomenis veiksnys ($\beta = 0.391$).

Skirtingų asmens duomenų tipų analizė atskleidė aiškią jautrumu pagrįstą hierarchiją. Vartotojai labiausiai linkę atskleisti mažo jautrumo duomenis, tokius kaip kontaktinė informacija ($M = 4.36$), ir mažiausiai – didelio jautrumo duomenis, pavyzdžiui, mediciniuius ($M = 1.94$) ir finansinius duomenis ($M = 1.82$). Klasterinė analizė leido identifikuoti tris skirtingus vartotojų segmentus, pasižyminčius skirtingais privatumo, pasitikėjimo ir kontrolės profiliais, patvirtinant, kad asmens duomenų atskleidimo elgsena reikšmingai skiriasi tarp vartotojų grupių.

Išvadose ir pasiūlymuose pabrėžiama suvokiamos naudos ir suvokiamos asmens duomenų kontrolės svarba leidimu grįstoje rinkodaroje bei akcentuojamas poreikis taikyti duomenų jautrumu ir vartotojų segmentais pagrįstas duomenų rinkimo strategijas. Tyrimo rezultatai suteikia praktinių įžvalgų kuriant skaidrias, pasitikėjimą stiprinančias asmens duomenų tvarkymo praktikas ir prisideda prie mokslinio supratimo apie vartotojų asmens duomenų atskleidimo elgseną.

ANNEX 3 – SURVEY QUESTIONNAIRE IN ENGLISH

I am Danielius Aliaševičius, a master's student in Marketing and Integrated Communications at Vilnius University. This short survey (6–8 minutes) is part of my master's thesis, which aims to explore how trust influences people's willingness to share their personal data in exchange for personalized services.

Participation is voluntary and anonymous, and all responses will be used for academic purposes only. If you have any questions or comments, please contact me at danielius.aliasevicius@evaf.stud.vu.lt. Thank you for your time and contribution!

Block 1 (screening questions)

1. Are you aware of UAB „Bolt Services" brand/company, or just commonly known as „Bolt", as an urban mobility services provider?
    - Yes, I use/used their services (proceed to Block 2)
    - Yes, but I never used their services (proceed to Block 2)
    - No, I am not aware (End of survey)

Block 2 (main block)

2. How often are you consciously or unconsciously giving permissions to various companies/brands to gather your personal data for personalized goods or services to you?
    - Once or more times per day
    - A few times per week
    - A few times per month
    - Once per month
    - A few times per year
    - Almost never
    - I don't know
3. Rate your level of agreement with the statements regarding trust in technologies:

	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
Technologies and the internet is a safe environment in which to exchange information with others.							
Technologies and the internet is a reliable environment in which to conduct business transactions or personal purchases.							
Technology and internet merchants are dependable.							
Technologies and the internet can be trusted.							

4. Rate your level of agreement with the statements regarding trust in government (regulatory effectiveness):

	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
The existing laws in my country and internationally, (such as General Data Protection Regulation, GDPR) are sufficient to protect consumers' online privacy.							
There are stringent international laws to protect personal information of individuals on the Internet.							
The government is doing enough to ensure that consumers are protected against online privacy violations.							

From now on, while answering questions, think about *UAB "Bolt Services"* or just *Bolt* as an urban mobility service provider.

5. Rate your level of agreement with the statements regarding perceived control over personal data:

	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
I am usually bothered when I do not have control over personal information that I provide to this company/brand.							
I am usually bothered when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by this company/brand.							
I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction with this company/brand.							

6. Rate your level of agreement with the statements regarding privacy concerns:

I am concerned that this company/brand will:	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
… gather too much personal information about me.							
… use my personal data for purposes other than the reason I provided the information for.							
... share my personal information with other parties.							
I am concerned about my privacy at this company.							

7. Rate your level of agreement with the statements regarding trust in brand/company:

	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
I feel safe in my transactions with this company/brand.							
I trust this company/brand to keep my personal information safe.							
Overall this company/brand is trustworthy.							
I feel that any information communicated by this company/brand is secure.							

8. Rate your level of agreement with the statements regarding willingness to disclose personal data:

While purchasing or ordering services at this company/brand, you are often asked to provide to them your personal data. Please, specify, how much are you willing to provide personal data of each type of data:	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
Contact Information (Name, Email address, Phone number, Home adress)							
Demographic Data (Age, Gender, Education level, Location from)							
Online Behavioral Data / Cookies (Browsing History, Purchase History, Website Visits)							
Social Networking Data (Interests, Likes, Social Connections)							
Preferences Data of Receiving Content methods (Content preferences, Frequency of communication preferences, Preferred communication channels)							
Profile and views data (Hobbies, Faith orientation, Political orientation, Relationship status, Favourite brands)							
Medical data (Health conditions, Medical history, Medications)							
Financial data (Income level, Loans information, Transaction history, Investment portfolio details)							

Live Location Data (Geolocation, Location-based Marketing Data)							

9. Rate your level of agreement with the statements regarding perceived benefits of personalized communication:

The personalized communication of this company/brand will:	1 – Strongly disagree	2 – Disagree	3 – Slightly disagree	4 – Neighter agree or disagree	5 – Sligthly agree	6 – Agree	7 – Strongly agree
… be supposedly relevant to my needs.							
… be supposedly meaningful to me.							
... be supposedly useful to me.							
... be supposedly interesting to me.							
... be supposedly provide purchase recommendations that match my needs.							
I think this personalized communication of this company/brand enables me to order products that are tailor-made for me.							
Overall, this personalized communication of this company/brand is tailored to my situation.							
I believe this personalized communication of this company/brand is customized to my needs.							

Block 3 (demographics of the respondents)

10. What is your age?
- 18–24
- 25–34
- 35–44
- 45–54
- 55–64
- 65 and older

11. What is your gender?
- Male
- Female
- Other / I don‘t want to answer

12. Where do you live?*
- In a big city (Vilnius, Kaunas, Klaipeda, Siauliai, Panevezys)
- In a smaller city (between 3 000 and 80 000 residents)
- In a village (fewer than 3 000 residents)

**According to the 1994 Law of the Republic of Lithuania on Territorial Units and Their Boundaries, one of the main characteristics of a city is the number of inhabitants (more than 3,000).*

13. What is your highest level of education completed?
    - Primary education
    - Secondary education
    - Vocational education
    - Bachelor’s degree
    - Master’s degree
    - Doctorate or higher

ANNEX 4 – SURVEY QUESTIONNAIRE IN LITHUANIAN

Esu Danielius Aliaševičius, Vilniaus universiteto Marketingo ir integruotos komunikacijos magistrantas. Ši trumpa apklausa (6–8 min.) yra mano magistro darbo dalis, kurio tikslas - išsiaiškinti, kaip pasitikėjimas veikia žmonių norą dalintis savo duomenimis mainais į suasmenintas paslaugas.

Dalyvavimas yra savanoriškas ir anonimiškas, o atsakymai bus naudojami tik akademiniams tikslams. Klausimų ar pastabų atveju rašykite: danielius.aliasevicius@evaf.stud.vu.lt. Dėkoju už Jūsų laiką ir indėlį!

Blokas 1 (atrankos klausimai)

1. Ar esate girdėję apie UAB „Bolt Services“ prekės ženklą / įmonę, arba tiesiog plačiai žinomą kaip „Bolt“, kaip miesto judumo paslaugų teikėją?

- Taip, naudoju / anksčiau naudojausi jų paslaugas (pereikite prie 2 Bloko)
- Taip, bet niekada nesu naudojęsis jų paslaugomis (pereikite prie 2 Bloko)
- Ne, nesu girdėjęs (apklausa baigta)

Blokas 2 (pagrindinis blokas)

2. Kaip dažnai sąmoningai ar nesąmoningai suteikiate leidimus įvairioms įmonėms / prekių ženklams rinkti jūsų asmens duomenis, kad jie galėtų jums siūlyti suasmenintas prekes ar paslaugas?

- Kartą ar daugiau kartų per dieną
- Kelis kartus per savaitę
- Kelis kartus per mėnesį
- Kartą per mėnesį
- Kelis kartus per metus
- Beveik niekada
- Nežinau

3. Įvertinkite savo pritarimą teiginiams, susijusiems su pasitikėjimu technologijomis:

	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
Technologijos ir internetas yra saugi aplinka, kurioje galima keistis informacija su kitais.							
Technologijos ir internetas yra patikima aplinka, kurioje galima atlikti verslo sandorius ar asmeninius pirkinius.							
Technologijų ir interneto paslaugų teikėjai yra patikimi.							
Technologijomis ir internetu galima pasitikėti.							

4. Įvertinkite savo pritarimą teiginiams, susijusiems su pasitikėjimu valdžia (reguliavimo veiksmingumas):

	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
Šalies ir tarptautiniai įstatymai (pvz., Bendrasis duomenų apsaugos reglamentas, BDAR, angl.k. – GDPR) yra pakankami apsaugoti vartotojų privatumą internete.							
Yra griežti tarptautiniai įstatymai, skirti apsaugoti asmens duomenis internete.							
Valdžia (Vyriausybė) daro pakankamai, kad užtikrintų vartotojų apsaugą nuo privatumo pažeidimų internete.							

Nuo šiol atsakydami į klausimus galvokite tik apie miesto judumo paslaugų teikėją UAB „Bolt Services“ („Bolt“).

5. Įvertinkite savo pritarimą teiginiams apie asmens duomenų kontrolę:

	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
Dažniausiai jaučiu nerimą, kai neturiu kontrolės dėl asmeninės informacijos, kurią pateikiu šiai įmonei/prekės ženklui.							
Dažniausiai jaučiu nerimą, kai neturiu kontrolės ar autonomijos sprendžiant, kaip ši įmonė/prekės ženklas renka, naudoja ir dalijasi mano asmenine informacija.							
Man kelia susirūpinimą, kai dėl rinkodarinio sandorio su šia įmone/prekės ženklu prarandama arba nevalingai sumažėja mano asmeninės informacijos kontrolė.							

6. Įvertinkite savo pritarimą teiginiams, susijusiais su privatumo susirūpinimu:

Aš nerimauju, kad ši įmonė/prekės ženklas:	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
… surenka per daug mano asmeninės informacijos.							

… naudoja mano asmens duomenis kitais tikslais, nei dėl kurių pateikiau informaciją.							
… dalinasi mano asmens informacija su kitomis šalimis.							
Aš nerimauju dėl savo privatumo šioje įmonėje.							

7. Įvertinkite savo pritarimą teiginiams, susijusiems su pasitikėjimu su šiuo prekės ženklu/įmone:

	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
Jaučiuosi saugus atlikdamas "sandorius" su šia įmone/prekės ženklu.							
Tikiu, kad ši įmonė/prekės ženklas saugiai saugo mano asmeninę informaciją.							
Apskritai ši įmonė/prekės ženklas yra patikima.							
Jaučiu, kad visa informacija, kurią perduoda ši įmonė/prekės ženklas, yra saugi.							

8. Įvertinkite savo pritarimą teiginiams, susijusiems su noru atskleisti asmens duomenis:

Perkant ar užsakant paslaugas šioje įmonėje, dažnai prašoma pateikti savo asmens duomenis. Prašome nurodyti, ar esate noriai pasirengę pateikti kiekvieno tipo asmens duomenis:	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
Kontaktinė informacija (vardas, el. pašto adresas, telefono numeris, namų adresas)							
Demografiniai duomenys (amžius, lytis, išsilavinimo lygis, gyvenamoji vieta)							
Interneto naršymo duomenys / Slapukai (naršymo istorija, pirkimų istorija, apsilankymai svetainėse)							
Socialinių tinklų duomenys (pomėgiai, „patinka" mygtuko paspaudimai, socialiniai ryšiai)							
Turinio gavimo būdų pageidavimų duomenys (turinio pasirinkimai,							

komunikacijos dažnumo pageidavimai, pageidaujami komunikacijos kanalai)							
Profilio ir nuostatų duomenys (hobiai, išpažįstama religija, politinės pažiūros, santykių statusas, mėgstami prekės ženklai)							
Medicininiai duomenys (sveikatos būklė, medicinos istorija, vartojami vaistai)							
Finansiniai duomenys (pajamų lygis, paskolų informacija, sandorių istorija, investicijų portfelio duomenys)							
Gyvoji buvimo vietos informacija (geolokacija (angl. k. – GPS), vietos pagrindu teikiama rinkodaros informacija)							

9. Įvertinkite savo pritarimą teiginiams, susijusiems su suasmenintos komunikacijos naudomis:

Šios įmonės/prekės ženklo suasmeninta komunikacija:	1 – Visiškai nesutinku	2 – Nesutinku	3 – Iš dalies nesutinku	4 – Nei sutinku, nei nesutinku	5 – Iš dalies sutinku	6 – Sutinku	7 – Visiškai sutinku
… bus man pritaikyta ir atitiks mano poreikius.							
… man bus prasminga.							
… man bus naudinga.							
… man bus įdomi.							
… man suteiks pirkimo rekomendacijų, atitinkančių mano poreikius.							
Manau, kad šis įmonės/prekės ženklo suasmenintas bendravimas leidžia man užsisakyti produktus ar paslaugas, pritaikytus būtent man.							
Apskritai, šis įmonės/prekės ženklo suasmenintas bendravimas yra pritaikytas mano situacijai.							
Tikiu, kad šis įmonės/prekės ženklo suasmenintas bendravimas yra pritaikytas mano poreikiams.							

3 blokas (respondentų demografiniai duomenys)

10. Koks yra jūsų amžius?

- 18–24 m.
- 25–34 m.

- 35–44 m.
- 45–54 m.
- 55–64 m.
- 65 m. ir vyresnis

11. Kokia yra jūsų lytis?
- Vyras
- Moteris
- Kita / nenoriu atsakyti

12. Kur jūs gyvenate?*
- Didmiestyje (Vilnius, Kaunas, Klaipėda, Šiauliai, Panevėžys)
- Miestelyje (3 000–80 000 gyventojų)
- Kaimo vietovėje (mažiau nei 3 000 gyventojų)

**Remiantis 1994 m. Lietuvos Respublikos teritorijos administracinių vienetų ir jų ribų įstatymu, vienas pagrindinių miesto požymių yra gyventojų skaičius (daugiau nei 3 000).*

13. Koks yra jūsų aukščiausias baigtas išsilavinimo lygis?
- Pagrindinis išsilavinimas
- Vidurinis išsilavinimas
- Profesinis išsilavinimas
- Bakalauras
- Magistras
- Daktaras arba aukštesnis