



Universität St.Gallen

Customer Privacy Orientation:

Conceptualization, Scale Development, and Consequences





Mauro Luis Gotsch

Scientific Project Manager
University of Applied Sciences of the Grisons
Commercialstrasse 19, 7000 Chur, Switzerland
Email: mauroluis.gotsch@fhgr.ch

Dennis Herhausen

Associate Professor of Marketing
Vrije Universiteit Amsterdam
De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands
Email: dennis.herhausen@vu.nl

Marcus Schögel

Associate Professor of Marketing Management
University of St. Gallen
Dufourstrasse 40a, 9000 St. Gallen, Switzerland
Email: marcus.schoegel@unisg.ch



Abstract

As new personal data processing capabilities are made available to more firms, demonstrating privacy friendly marketing strategies becomes an essential part of a firm's value proposition. Yet, so far, no research has systematically conceptualized and operationalized the different organizational facets that span a firm's customer privacy orientation (CPO). We address the resulting conceptual ambiguity by (re-)conceptualizing CPO, defining it as the extent to which an organization engages in strategic, structural, and operative privacy orientation while developing, delivering, and maintaining products and/or services that ensure favorable privacy perceptions by customers, which is determined by four component dimensions (strategic CPO, structural CPO, operative CPO, and customer perceptions of CPO). This conceptualization emerges from a two-stage multimethod conceptualizing process leveraging the existing literature and qualitative data from 39 in-depth expert interviews. We then use several studies with a total of 813 managerial participants to develop and validate a parsimonious four-factor, 12-item CPO scale that shows internal consistency, reliability, and validity. Our findings provide scholars a unifying understanding and measurement instrument of CPO and equip managers with a self-assessment tool to analyze and develop their privacy orientation.

Keywords: Customer privacy orientation, privacy strategy, information privacy, marketing strategy, scale development



Inhaltsverzeichnis

Customer Privacy Orientation	6
Customer Background	8
Overview of the Research Process	10
Step 1: Literature Review	12
Step 2: Expert Interviews	13
Sampling procedure	13
Interview structure	13
Analytical approach	14
Step 3: Reconceptualization and Dimensionality	14
Strategic privacy orientation	14
Structural privacy orientation	15
Operative privacy orientation	16
Customer perceptions of privacy orientation	17
Step 4: Item Generation	18
Step 5: Item Validity	21
Step 6: Scale Refinement	21
Step 7: Scale Purification	24
Step 8: Nomological Validity	26
Discussion	30
Theoretical implications	30
Partical implications	31
Limitations and directions for further research	31
References	33
Appendix	38



Highlights

- This article conceptualizes customer privacy orientation (CPO) in the context of corporate processing of customer data.
- It develops and validates a parsimonious four-factor, 12-item scale for measuring CPO.
- It suggests how to evaluate and develop a customer privacy-oriented position in a larger ecosystem.
- It examines two potential antecedents of CPO as well as the construct's impact on marketing and financial performance.

Customer Privacy Orientation

Half a year after the release of ChatGPT 3.5, the generative artificial intelligence (AI) by OpenAI, McKinsey's annual global survey reported that already 60% of organizations have adopted the technology in some capacity in their daily business. Although 40% of respondents saw the use of generative AI as a potential threat to the privacy of their employees and customers, only 20% of organizations in the sample are working to mitigate those risks (Chui et al., 2023). Such a disconnect is not a new phenomenon – as many social and policy risks often only concretely emerge once technologies like ChatGPT are introduced into marketing practice (Stahl & Eke, 2024). However, the potential erosion of customer's data privacy has been a point of contention for each data-driven technology of the past 20 years (K. D. Martin & Murphy, 2017). Hence, while organization's demand for more data is growing at a stable rate, most companies "continue to fall short in attention and commitment to data ethics policies and practices" (Davenport & Bean, 2023). In parallel, "the dramatic loss of privacy has become a major concern for consumers" (Hoffman et al., 2022) and the demand for more customer privacy protection has been rising worldwide (Cisco, 2022).

Capturing more customer data in new marketing technologies is therefore likely to further increase customers' data vulnerability and perceptions of harm, due to the ever-increasing complexity of how their data is being processed (K. D. Martin et al., 2017). Since customer trust is a prerequisite to create sustainable value from digital technologies like generative AI (Shin et al., 2022), marketing strategies need to be able to both address privacy regulations and customers' need for data privacy (Uysal et al., 2022). Yet, so far, marketing research on organizational privacy has focused "too much on individual silos", rather than holistic responses to increase customer privacy (K. D. Martin & Murphy, 2017, p. 153). Hence, by developing a better understanding on how a customer privacy oriented marketing strategy is developed, companies can move beyond a stance of "mere compliance" and create a competitive advantage founded in consumer trust (Quach et al., 2022, p. 22).

Despite its relevance, the conceptualization and operationalization of customer privacy orientation (CPO) has received limited attention in marketing literature. Research so far predominantly focusses on the consequences of violating customers' privacy (K. D. Martin et al., 2017) or the impact of data privacy regulation on organizations (Steinhoff & Martin, 2022), without considering the potential strategic, structural and operational benefits of a customer privacy-oriented firm. There is a need to "find a balance between the advantages of data sharing and the necessity to safeguard the privacy and security of individuals and businesses" (Pappas et al., 2023, p. 950). The few related existing instruments either consider customer privacy as a small part of a larger construct like "Corporate Digital Responsibility" (Lobschat et al., 2021) or focus solely on the strategic importance of the topic (K. D. Martin et al., 2020).

However, recommendations on how firms can holistically "deliver consistent, transparent privacy protection to their customers while achieving other important organizational objectives" are still lacking (Greenaway et al., 2015, p. 601). Despite of the high practical relevance of the topic, both academia and practitioners lack an accepted definition, conceptualization, and adequate measure of a firm's CPO. As a result, there are so far no systematic investigations on the effects of CPO applicable across industries. This study aims to contribute to addressing both these research gaps, by delineating a holistic conceptualization of CPO which integrates the previously isolated strategic, structural, operative, and perceptual perspectives. We then operationalize CPO as a self-assessment scale showing internal consistency,



reliability, as well as construct and nomological validity. Moreover, we identify three antecedents to CPO and provides first evidence for its positive effect on marketing and firm performance. The results of these efforts provide important contributions to the literature on data privacy. To conceptualize CPO, we combine literature-based insights from the privacy literature with interview-based insights from privacy experts. Specifically, we identify CPO as a multidimensional construct that manifests itself in four dimensions: (1) strategic CPO, (2) structural CPO, (3) operative CPO, and (4) customer perceptions of CPO. We build on these findings and develop an empirically sound measurement scale for CPO by drawing on survey data from multiple studies. The resulting scale is concise, industry-spanning, and easy to administer, and will hopefully serve as a standard for future research and managerial adoption. Practitioners can use the scales to establish, evaluate, and detect potential deficits in their firms' privacy orientation towards customers. We further examine selected antecedents of CPO and identify corporate social responsibility (CSR) (Turker, 2009) and compliance culture and leadership (Amankwa et al., 2018) as relevant antecedents to CPO. Finally, we add to research on the benefits of CPO beyond the avoidance of reputational damage (K. D. Martin et al., 2017) and identify its positive effects on marketing and economic performance.

Customer Background

Previous research on CPO has defined it as “the extent to which a firm delivers consistent, transparent privacy protection to its customers while achieving other important organizational objectives” (Greenaway et al., 2015, p. 580). This definition implies an inherent tension between a firm’s demand for customer data and their customers’ demand for privacy – an observation which has been repeated in other studies (Gerlach et al., 2019; Pelteret & Ophoff, 2016; Quach et al., 2022). Therefore, CPO is often discussed with other constructs that face similar trade-offs between short-term profit and a culture that fosters the well-being of multiple stakeholder groups. For example, CPO has implicitly or explicitly been considered as part of CSR (Allen & Peloza, 2015; Pollach, 2011) or corporate digital responsibility (Lobschat et al., 2021; Wirtz et al., 2023).

Moreover, previous research acknowledges the multi-dimensional nature of CPO and related constructs. Greenaway et al. (2015) define privacy orientation as improving the control of customers over collected data, the procedural justice in the collection of said data (i.e., the degree to which its use being perceived as ‘fair’) and the legal obligations of the company. Analogous to the three-level model of Greenaway & Chan (2015) and the categorization of the role of privacy in marketing by Martin & Murphy (2017), “privacy orientation” must address consumer antecedents, structural forces, and societal demands. Martin (2018a) has consistently portrayed CPO “as a form of strategy” used to build a basis of competitive advantage - particularly when the negative impact of privacy violations on trust is realized by a competitor. As such, CPO is dictated top-down to the operative level but can only be effective from a firm’s perspective if it reduces consumers’ perceived vulnerability (Martin et al., 2017).

Table 1 provides an overview of previous articles related to CPO. While research on this important topic is progressing, we note that the extend literature is fragmented in focusing only on the company or customer (with the notable exemption of K. D. Martin et al., 2020), and that the articles inherent diverse perspectives on CPO. We aim to address the resulting conceptual ambiguity by reconceptualizing and developing a sound measurement instrument for CPO. We next give an overview over our research process.

Table 1: Overview of previous research related to CPO

Article	Method	Focus	Strategy Perspective	Structural Perspective	Operational Perspective	Perceptual Perspective	Core findings
Baruh & Cemalcilar (2014)	Quantitative, Survey	Customer				Yes	Personal privacy orientation consists of the belief of privacy as a right, other-contingent privacy, concern about own informational privacy and concern about privacy of others.
Greenaway, et al. (2015)	Conceptual	Company	Yes		Yes		The extent to which a firm delivers consistent, transparent privacy protection to its customers while achieving other important organizational objectives is dependent on the ethical obligations, the information management strategy and the legal risk assessment of a given firm.
Martin et al. (2017)	Experiment, Event Study	Customer			Yes	Yes	Transparency and control in firms' management practices related to data privacy can suppress the negative effects of customer data vulnerability.
Martin & Murphy (2017)	Conceptual	Customer	Yes		Yes	Yes	To evaluate the level of privacy offered by any organization, a holistic view blending consumer, organizational, ethical, and legal concerns is necessary.
Martin (2018)	Experiment, Survey	Customer				Yes	Trust assuages privacy concerns by taking away the risk of information misuse. Privacy violations may be particularly difficult to recover from without the benefit of a firm's perceived ability or integrity.
Amankwa et al. (2018)	Quantitative, Survey	Company		Yes			Supportive organizational culture and end-user involvement significantly improve employees' attitudes towards compliance with information security policies.
Martin et al. (2020)	Interviews, Surveys	Company , Customer	Yes			Yes	Big data as a driver of customer relationship performance, the impacts of regulation, and privacy protection as a proactive retail strategy suggest a convergence of the interests between costumers, retailers and regulators is possible.
Lobschat et al. (2021)	Conceptual	Company	Yes	Yes			Corporate digital responsibility consists of a set of shared values and norms guiding an organization's operations with respect to four main processes: technology and data capture, operation and decision making, inspection and impact assessment, and refinement of technology and data.
Quach et al. (2022)	Qualitative	Company	Yes			Yes	Digital technologies empower firms' data monetization or data sharing strategies, while also creating privacy tensions within the customer base.
Steinhoff & Martin (2022)	Conceptual	Company			Yes	Yes	Human-based, technology-based and hybrid frontline services are all impacted by changing data privacy regulatory frameworks but face different challenges. Hence, research should work to address all three types differently to optimize each for of the six dimensions of global privacy regulations (fairness, data limits, transparency, control, consent, and recourse).
This paper	Interviews, Surveys	Company , Customer	Yes	Yes	Yes	Yes	CPO is the degree to which an organization engages in strategic, structural, and operative privacy orientation while developing, delivering, and maintaining products and/or services to ensure favorable privacy perceptions by customers. CPO is anteceded by CSR, compliance supportive organizational culture and leadership. CPO has a positive effect on marketing and firm performance.



Overview of the Research Process

Our research follows the recommendations for reconceptualizing concepts (Mackenzie et al., 2011, p. 297) and scale development (Homburg et al., 2015, p. 45; Lytras et al., 2021) by using an eight-step research process, as summarized in Table 2. First, we conducted a literature review of 138 privacy research articles across the consumer, psychological, and economic domains. This review revealed four theoretical perspectives on CPO. Second, we qualitatively analyzed data stemming from 36 in-depth interviews and five privacy laws and guidelines. Our findings confirm the four perspectives. Third, based on the literature review and expert interviews, we reconceptualize CPO and its four underlying dimensions. Fourth, we developed multiple potential items for the four dimensions based on the existing literature on privacy. Five unaffiliated researchers judged the initial items' clarity, content validity, and face validity. Fifth, 41 data privacy professionals from the International Association of Privacy Professionals and the Swiss Association for Organizational Data Privacy further evaluated the initial items. Sixth, we administered the remaining items in a survey to 353 managers from the Swiss Marketing Association. Seventh, we used data collected from 387 managers from the European Union, the United Kingdom, and Switzerland for scale purification. Eighth, we use the same data to test for nomological validity. We find first evidence of CSR and compliance culture and leadership as antecedents to CPO and that CPO has a positive relationship with marketing and financial performance. We close with a discussion of the theoretical and practical implications as well as the limitations and directions for further research.

Table 2: Overview of the Research Process

Process Step	Details	Outcome
Step 1: Literature Review	Review of privacy research across the consumer, psychological, and economic domains. A total of 137 articles discuss relevant perspectives on CPO.	Four key perspectives on CPO in the literature.
Step 2: Expert Interviews	Qualitative analysis of 36 in-depth interviews and five privacy laws and guidelines	Managerial views mirror the four key perspectives on CPO
Step 3: Reconceptualization and Dimensionality	Definition of CPO as “the extent to which an organization engages in strategic, structural, and operative privacy orientation while developing, delivering, and maintaining products and/or services to ensure favorable privacy perceptions by customers”	Four CPO dimensions
Step 4: Item Generation	Multiple potential items based on the existing literature on privacy. Five unaffiliated researchers judged the items’ clarity, content validity, and face validity.	65 initial items to measure CPO
Step 5: Item Validity	Evaluation by 41 data privacy professionals from the International Association of Privacy Professionals and the Swiss Association for Organizational Data Privacy.	51 items to measure CPO
Step 6: Scale Refinement	Survey of 353 managers from the Swiss Marketing Association. Exploratory and confirmatory factor analysis	32 items scale for CPO
Step 7: Scale Purification	Survey of 387 managers from the European Union, the United Kingdom, and Switzerland. Exploratory and confirmatory factor analysis	12 items for CPO
Step 8: Nomological Validity	Establishment of nomological validity	CSR and a Compliance culture and leadership are positively related to CPO. In turn, CPO is positively related to marketing performance and financial performance.

Step 1: Literature Review

We started our literature review on CPO by drawing on the influential work of Martin and Murphy (2017), who summarized privacy research across the consumer, psychological, and economic domains. Using forward and backward sampling of this work, we identified a total of 138 articles that discuss four key perspectives on CPO.

First, some studies approach the topic of customer privacy from a *strategic perspective*. Specifically, the customer data strategy guiding data processing (Greenaway et al., 2015), privacy collaborations with other industry actors (K. D. Martin et al., 2017; Wortmann et al., 2022), positioning within a larger data ecosystem (K. D. Martin & Murphy, 2017) and trust building within one's customer base (Lobschat et al., 2021; Quach et al., 2022) are all addressed by a strategic perspective on CPO. To emphasize the strategic perspective, Martin and Murphy (2017) introduced the term "privacy as strategy" into marketing literature and postulated to successfully that firms need to differentiate themselves from other using superior customer privacy practices.

Second, other studies approach the topic of customer privacy from a *structural perspective*. These structural aspects of CPO refer mostly to how privacy risks are managed within a company and how such measures are translated into a "privacy enforcement architecture" (Ashley et al., 2002, p. 47). References to company structure include discussing the role of the chief privacy officer or their team should play in the overall organizational structure (Bamberger & Mulligan, 2010; Solove, 2013) or when talking about inter-departmental data transmission (Hermalin & Katz, 2006). Other recommend a more customer-centric organizational structure helping to align privacy processes with the needs of customers (Child et al., 2012; K. D. Martin et al., 2020). At the same time, the data privacy architecture, i.e., the rules, contexts and infrastructure which determine the "meaningful control, ownership, and other claims to data" (Hummel et al., 2021, p. 12) within an organization, is closely influenced by its organizational and incentive structure (Bu et al., 2020). Another clearly defined structural force is the overall privacy risk management, which plays a central role to ensure sustainable CPO (Amankwa et al., 2018).

Third, additional studies approach the topic of customer privacy from an operative perspective. As operative customer privacy is concerned with product or service-related features (Dienlin & Metzger, 2016; Dinev et al., 2012; Steinhoff & Martin, 2022), or the effective communication of said features (Boerman et al., 2018; Hann et al., 2007; Huang & Bashir, 2020), it is probably the most researched perspective. Other tactics, such as providing compensation for sharing data (H. Chen et al., 2017) or nudging costumers within user interfaces to incentivize the use of privacy controls (Acquisti et al., 2017; Kitkowska et al., 2020) have also been suggested as potential approaches on an operative level. The idea of ensuring transparency and control in the design of products and services has also been repeated often and across different studies (Beke et al., 2018; Bélanger & Crossler, 2011; K. D. Martin & Murphy, 2017). However, operative customer privacy is just the most visible part of a bigger strategy that only works in collaboration with one's customer base.

Finally, some studies approach the topic of customer privacy from a customer perspective. Customers knowingly sharing data with a firm reflects their trust in the firm's privacy principles and signals "a willingness to assume the risks of disclosure" (Culnan & Bies, 2003, p. 327). On the one hand, this trust creates a switching cost for the customer to exchange a firm's services with a competing one. On the other hand, this competitive advantage can only be maintained if the firm's privacy policy as perceived



by the customer is consistent with the firm's practices (Balapour et al., 2020). As such, consumer perceptions of CPO influence a firm's privacy practices in two major ways. First: consumers' intention to adopt new features or products which could affect their privacy is dependent on their existing trust and privacy concerns relating to the firm (Miltgen et al., 2016). Over time, this may even erode attempts to correct existing privacy practices through new operative measures, as they are more likely to be ignored by customers. Alternatively, customers may fall into a state of privacy fatigue, which in the long term leads to a general dissatisfaction with a firm's offerings (Choi et al., 2018) or the intentional falsification of data (S. (Joseph) Chen et al., 2023). Second: Low perceptions of CPO also negatively impact the emotional violation felt, should a breach of the customer's privacy occur. This in turn may lead to more drastic customer behaviors, from negative word of mouth to switching behavior (K. D. Martin et al., 2017).

Having uncovered four perspectives on CPO in the literature review, we next complement these insights with the managerial perspective on CPO.

Step 2: Expert Interviews

Sampling procedure

Following the literature review, we conducted 39 in-depth expert interviews to obtain a holistic understanding of CPO. To ensure the relevance of the sample, we only include privacy experts from B2C companies or companies with direct access to customer data. Specifically, we interviewed 21 data privacy officers, 11 CEO/CMOs of smaller firms with data protection responsibilities, 5 data privacy consultants, and 2 data privacy auditors from various industries. These include retailing (12 experts), IT/Telecommunication (9 experts), banking and fintech (7 experts), data strategy and consultancy (7 experts), mobility and automotive (3 experts), and medical start-ups (2 experts). By recruiting a sample of diverse industries, we ensured transferability across a wide range of companies.

Interview structure

Each expert was interviewed based on a previously provided interview guide. Interviews started with questions pertaining to respondent's responsibilities within the company. Afterwards the interview focused on open-ended questions with the aim to define CPO (e.g., which characteristics do you associate with CPO? What distinguishes an organization with high privacy orientation from one with low privacy orientation?) and followed up with directed questions (e.g., how does your management support the privacy measures of your team?). Respondents were encouraged throughout to provide examples and additional details to avoid potential misinterpretation (Glaser and Strauss 1967). Finally, respondents had the opportunity to talk about additional points they considered important. Great care was given to phrase all questions in a non-directive manner and to avoid guiding the conversation according to the previously established theoretical basis.



Analytical approach

The expert interviews lasted 40.5 minutes on average (minimum 20 minutes, maximum 58 minutes). The interviews were recorded to ensure a verbatim transcription. Additionally, we followed the recommendations of several interviewees and reviewed the data privacy and security criteria catalogues of the GDPR, the ISO-IEC 27000, GAIA-X, digital trust label, and the NIST Privacy Framework. The interviews and documents were analyzed using directed content analysis (Hsieh and Shannon 2005) based on the four theoretical dimensions established in the literature review. These dimensions served as the main categorization matrix which was expanded through the inductive approach of coding all documents (Assarroudi et al., 2018). As a result, the four main perspectives from the literature review were slightly adjusted. First signs of theoretical saturation (i.e., lowered numbers of unique themes per run and high repetition rate of existing data structure points) were noted at interview 28. At this point, efforts were made to include additional experts from industries with already heightened data privacy regulations such as finance and health care. This effort yielded additional insights, with the number of unique themes dropping again at interview 34. After five additional interviews and the inclusion of insights from the recommended criteria catalogues any further data collection was stopped. As a result, we differentiate four dimensions of CPO as described next.

Step 3: Reconceptualization and Dimensionality

Based on our literature review and expert interviews, we define CPO as *the extent to which an organization engages in strategic, structural, and operative privacy orientation while developing, delivering, and maintaining products and/or services to ensure favorable privacy perceptions by customers*. We further define strategic CPO as the extent to which an organization integrates consistent, transparent privacy protection to its customers in strategic marketing decisions, structural CPO as the extent to which an organization establishes rules, norms, or structures to guide privacy preserving behavior, operative CPO as the extent to which customer privacy concerns are embodied in operative marketing decisions of an organization, and customer perceptions of CPO as the extent to which customers perceive that privacy issues related to their data are treated fairly by an organization. We summarize supporting evidence on these dimensions from the literature review and expert interviews below.

Strategic privacy orientation

Our interviews reveal that CPO needs to be guided top down from a strategic level. This is in accordance with the conclusion of Martin & Murphy that a stance towards CPO “cannot be a short-term approach designed for quick benefits” (2017, p. 152). The need for a long-term commitment towards CPO backed by top-management is essential because it aligns employees behind a shared commitment. We derived four main elements of this dimension from the literature and the interviews. First, strategic privacy orientation requires a data strategy, which clarifies the goals and business function of processing data in the first place. By specifying which data points are to be captured and developed, companies can go beyond the purpose limitation and data minimization required by the GDPR and embrace a data privacy strategy (Martin et al., 2020). Second, to ensure a long-term consistency in CPO, collaboration with other industry participants to create more favorable privacy standards are necessary. This ensures compliance of other actors in the data processing supply chain but might also sets a



benchmark that forces others to live up to these ‘newly established’ industry standards (Lobschat et al., 2021). Third, companies need to position themselves according to the chosen data strategy to align customers’ expectations regarding CPO with the CPO experienced when interacting with said company. Fourth, all these efforts must lead to a trust relationship with customers – be it as part of the company’s brand promise or mission statement. Such proactive stances regarding CPO help to mitigate the negative effects of data monetization and data sharing strategies on privacy tensions (Gotsch & Schögel, 2021; Quach et al., 2022). For many European companies, CPO as a strategic objective was discussed for the first time prior to the ratification of the GDPR. This process of strategic positioning using CPO was described by the data privacy officer of an internet service provider:

The question is: can you position yourself positively? As a service company: Can you tell a potential customer that you are a good provider? That you have considered his (privacy) rights very carefully? (...) This change of mind happened very quickly for us. It was a big wave; it is not something that we could just address by changing our privacy policy. Instead, it had to be understood: The customer is at the center of everything, and it doesn’t start with data privacy. (...) We want a long-lasting and coherent customer experience. From the customer’s point of view: they want the feeling that they are entrusting their data to a company that knows how to handle them responsibly. You don’t demote it (the brand promise) to a footnote. The contract relegates the privacy policy to the footnote. The point is to position yourself to the customer authentically. You tell the customer: We use your data and yes, we have economic interests. We’re not trying to hide anything.

Hence, taking a clear strategic position on CPO enables companies to guide internal processes and to clarify its importance to the customer as well as other stakeholders.

Structural privacy orientation

Especially the in-depth interviews with data privacy officers of larger firms showed that enforcing CPO requires inter-departmental collaboration as well as rules and processes to shape a larger privacy culture. While most interviewed experts agreed that CPO is dictated top-down as a strategic direction, they also emphasized the need for this structural dimension to avoid employee apathy and ensure accountability towards a company’s stated CPO goals. As a data privacy officer and trainer explained:

Good process management systems have the biggest influence on privacy orientation. Who does what? How? Or put another way, it is all about response management or data governance. Employees need to know what they need to do, what their exact role is. What processes are in place? Before a data breach can occur, during a data breach or even after a data loss. (...). If the company knows that, that’s worth a lot. If they write a privacy strategy, no matter how nice it is; a strategy of 20 pages, 40 pages, as long as they leave it on the table then that doesn’t help at all. That means very little, zero, it is just paper. It lacks functionality. You need fitting processes. (...) Once the entire team understands that, then we can call that a privacy culture or privacy mindset.

Such shared values, norms and artefacts are enshrined in both formal (e.g., audits, learning platforms, etc.) and informal (e.g., understanding of one’s role, privacy literacy, etc.) structures which influence

employees' behavior regarding CPO (Lobschat et al., 2021). More concretely, the structural forces anchoring CPO within a company's culture include its data processing policies and procedures, as well as a data privacy architecture which determines access to customer data (Ashley et al., 2002). Additionally, the existence of a dedicated privacy or data governance team and corresponding privacy champions in other functions helps to ensure that privacy concerns are prioritized and addressed in a consistent manner across different departments. This sentiment has been echoed in prior studies, where a supportive organizational culture was found to positively affect employees' data security compliance intentions (Amankwa et al., 2018). Finally, respondents stressed that proactive privacy risk management requires that internal privacy norms and regulations are regularly put to the test, both via internal audits (e.g., for individual projects) as well as external ones (e.g., for the entire company). The reporting from such audits in turn serve demonstrate CPO to a company's stakeholders (Bloemendal, 2022).

Operative privacy orientation

Addressing CPO concerns on a tactical or operative level is another crucial step in a larger privacy strategy. This echoes the need for "more holistic perspectives" (Martin et al., 2017) regarding customer privacy, as many companies still focus only data privacy on a touchpoint level (Lupiáñez-Villanueva et al., 2022). Both the respondents and previous studies agree that ignoring privacy concerns or legal requirements up to the point of data extraction "would amount to fixing a leaky faucet in a sinking ship" (Shastri et al., 2019, p. 1). Naturally, operative decisions are nonetheless the most visible part of CPO behavior to the customer and are therefore necessary to address their privacy needs. This refers mostly to decisions taken at data processing service frontline interfaces; whether they are human-based (e.g., personnel), hybrid (e.g., call-centers) or completely technology based (e.g., online applications). Their purpose is to interpret and enforce the privacy norms relating directly to customers: data limitation, transparency, control, consent, and easy recourse (Steinhoff & Martin, 2022). Our respondents stressed the importance of clear communication combined with privacy tools which are intuitive to use for the customer. Often, this requires considering privacy needs on an individual touchpoint's level instead of in general. As the head of the data governance team of an IT-service provider put it:

It is always worthwhile to refer to people who know the products very well. I think that sometimes we underestimate the complexity of the service that we provide. You have to know the preferences and the behavior of the customers when using these services. In my experience, if you refer only to other marketing departments or external agencies, you often get a generalist and human centered design for your privacy controls.... It's nice, but it's of no use in a specific case. It is not precise enough. What does the service look like in concrete terms for the customer? As an example: How does a customer who obtains a voice assistant act? I was significantly involved in such a project. I was responsible for potential data privacy issues arising (from this touchpoint). We discussed things like: What happens when a person receives this voice assistant via mail order? (...) The result: the device that you get today has a physical switch on it and it's toggled off. Only if you physically set it to on, then the voice assistant can be used. Only then is the microphone active, which is then placed in the customer's living room.

Echoing this quote, effective operative customer privacy requires one the hand the clear communication of privacy controls to customers, while considering their motivations and capabilities of doing so



effectively (Bartsch & Dienlin, 2016; Martin, 2018). The GDPR calls this principle “privacy by design”, but our respondents stressed the need to go beyond a purely compliance-oriented application of the principle. Instead, companies with high CPO should address the customers’ privacy needs as soon as they arise in the customer journey.

Customer perceptions of privacy orientation

Finally, all respondents recognized the role of the customer as a central driver and influence on successful CPO. Central to this dimension is the customer’s perception of fairness or procedural justice in the exchange of data for benefits. As Steinhoff & Martin (2022, p. 4) describe it: “Fairness goes beyond the regulatory stipulation that any uses of customer data must be legally compliant; it implies an element of ethical practice, exceeding basic legal frames, that determines whether the organization *should* obtain customer data for the purposes conveyed”. As with operative customer privacy, customer perceptions regarding fairness are highly context-sensitive and dependent on the company’s previous behavior. Low perceptions of CPO hinder a company’s efforts in this regard in two ways: first in a generally lowered trust in the company as a whole, which may lead customers to seek other services altogether (Miltgen et al., 2016). Second: recovery of trust is hindered by customers’ low importance given to any possible improvements to CPO (K. Martin, 2018a). More concretely: users of a service with a business model of reselling data are less likely to use the privacy settings offered to them and are more likely to protect themselves through other means like misrepresenting their own data (Jiang et al., 2013). As such, for a company to achieve high perceptions of customer privacy they not only need to fulfill their CPO promises internally, but they also need to design their efforts to address their customers’ privacy needs. As the data privacy officer of a financial service company put it:

I think that (privacy orientation) is a give and take. I think you need a customer contact strategy that actually derives the interaction intensity from the customer’s behavior or stated preferences. I’ll make an example: If I see that you registered immediately at our online shop, looked-up financing options for several cars, download our app and so on. Then these are clear signals of someone who is open, who reveals information and is obviously not very sensitive. Of course, on the other hand: there may be one who grants no opt in (referring to the cookie banner), who wants to be addressed perhaps at most in writing but only for matters not relating to our marketing interests. This person we’d send a maximum of two messages per year and the other maybe eight. I think this should be our customer contact strategy: attractive, fair, and self-learning.

This dimension therefore serves as the guiding metric for the other CPO dimensions. Consequently, it suggests that companies with a high CPO seek to increase the effectiveness and transparency of customer interactions involving the exchange of customer data. As Miltgen et al. (2016, p. 4664) concluded: “Improving both risk perception and trust (regarding data privacy) is indispensable to increase consumers’ behavioral intentions”.

Taken together, the literature review and expert interviews suggest a holistic conceptualization of CPO that consists of four dimensions. Thus, we continue to develop a corresponding measurement instrument for CPO.



Step 4: Item Generation

We developed multiple potential items that could capture the four dimensions of strategic CPO, structural CPO, operative CPO, and customer perceptions of CPO, starting with an initial list of items based on the existing literature on privacy. Since the goal of item generation is “to produce a set of items that fully captures all of the essential aspects of the domain of the focal construct, while minimizing the extent to which the items tap concepts outside the domain of the focal constructs” (Mackenzie et al., 2011, p. 304), several items per dimension were formulated by one researcher and reviewed by the other researchers in the author team. These initial items were then presented to five unaffiliated researchers for pre-testing the items’ clarity, content validity, and face validity. All concerns and notes were taken into account. During this process, 12 items were reworded to be more concise, and two items were deleted because they were deemed misleading. The resulting 65 items are displayed in Table 3 and were then used in an item validity test with data privacy experts.

Table 3: Overview of the Item Development

Initial Items	A	B	C
<i>Strategic CPO</i>			
1. top management explicitly names data privacy as an important part of our company's strategy.	X	X	X
2. top management emphasizes that the protection of costumers' data privacy is the responsibility of each employee.	X	X	X
3. the protection of the data privacy of customers is named within our mission statement.	X	X	X
4. each employee understands the objectives for gathering and processing our customers' data	X	X	
5. top management has introduced strategies on how to improve the data privacy of our customers	X	X	
6. we use a specific set of data protection standards for selecting our business partners	X	X	
7. our company's role in the data processing ecosystem is clearly communicated	X	X	
8. we engage in dialogue with our stakeholders about the data privacy aspect of our business model	X	X	
9. data privacy is a core value of our brand(s)	X	X	
10. our high data privacy standards are publicly communicated	X	X	
11. we do more for the data privacy of our customers than our industry peers	X		
12. we participate in data security business networks	X		
13. we participate in data privacy business networks			
14. we invest in research and development programs to create data privacy preserving products and services			
15. among other target markets, we also target data privacy-conscious consumers			
16. we regularly poll our customers to assess their trust in our data processing			
17. we value customer retention over customer acquisition			
<i>Structural CPO</i>			
18. all accesses to our customer data are logged and recorded.	X	X	X
19. we regularly conduct internal privacy risk assessments with a clearly defined scope.	X	X	X
20. our company has a system in place that ensures that improper or frequent accesses to customer data are immediately noticed.	X	X	X
21. we have created a separate department specializing in data privacy issues	X	X	
22. our data privacy officer operates fully independently from other departments	X	X	
23. our access permissions and authorizations to customer data are clearly defined	X	X	
24. we have clear guidelines on how to react to a detected personal data breach	X	X	
25. we conduct an external privacy audit at least once every year	X	X	
26. we demand a privacy audit report before sending customer data to an external business partner	X	X	
27. our data privacy officer is proactively involving themselves in new projects	X	X	
28. we organize presentations for our employees to inform them about our data privacy regulations	X	X	
29. we have access to an online archive or training platform, where our employees can learn about our privacy regulations	X	X	
30. our data privacy officer has the full support from top management	X		
31. direct access to customer data is limited to a select few authorized individuals	X		
32. there are clear rules on how customer data is shared with our business partners	X		
33. there are clear rules on how customer data is shared with the company's business partners	X		
34. our data privacy officer or his team are able to oversee most of our data processing activities	X		
35. we train at least one member of each department to be able to act as a data privacy consultant or expert	X		
36. we train each employee on how our data privacy policy affects their daily work	X		
37. we regularly train each employee about the current privacy regulations within their markets	X		

Initial Items	A	B	C
38. improper handling of customer data is sanctioned	X		
39. our employees have enough time to keep customer data within the system up to date	X		
40. our employees believe in the data privacy values of our organization	X		
41. we measure various key performance indicators (KPIs) relating to data privacy (e.g. number of data privacy complaints, results of data privacy audits, etc.)	X		
42. knowledge about data privacy by candidates are a bonus in our recruitment process			
43. our data privacy officer leads a diverse and cross-functional team			
44. our departments are organized in a customer-centric as opposed to a product-centric manner			
Operative CPO			
45. our customers can test our products and services without sharing a lot of personal data.	X	X	X
46. we do not collect customer data unless the customer receives a clear benefit in return.	X	X	X
47. we make efforts to use as little personal data for our products and services as possible.	X	X	X
48. we only collect enough data from customers to fulfil their order(s)	X	X	
49. we work with pseudonymized data whenever possible	X		
50. the precise purpose for the processing of customer data is known to all employees interacting with said data	X		
51. most of our company's stored customer data is up to date	X		
52. our customers can view all their personal data stored within our company within a short timeframe			
53. our customers can view all their personal data stored within our company without assistance of our employees			
54. our customers can edit or delete all their personal data stored within our company without assistance of our employees			
Customer Perceptions of CPO			
55. our customers understand, what data we collect from them.	X	X	X
56. our customers understand, why we collect data from them.	X	X	X
57. our data processing activities are transparent to our customers.	X	X	X
58. our employees know who to contact if they have questions regarding our data privacy regulations or data processing	X	X	
59. our customers know who to contact if they have questions regarding our data privacy regulations or data processing	X	X	
60. our customers can talk to an employee in a timely fashion if they have a question regarding our data privacy regulations or data processing	X	X	
61. our privacy policy is easily understandable for anyone reading it	X		
62. our customers can view all their personal data stored within the company within a short timeframe	X		
63. our customers receive a direct benefit from sharing their data with us			
64. our customers receive compensation for sharing their data with us			
65. our customers are incentivized to use the privacy settings of our products or services			

Note: All items start with "At my company..." A = Item Validity Step, B = Scale Refinement Step, C = Scale Purification Step



Step 5: Item Validity

In cooperation with the International Association of Privacy Professionals and the Swiss association for organizational data privacy, the 65 items were evaluated by 41 data protection officers from the European Union and Switzerland. The survey presented them with definitions for the dimensions as well as their corresponding items. They were tasked with rating each item's representativeness and importance for its corresponding dimension on a 5-point evaluation scale (from 1 = not relevant to the dimension to 5 = central to the dimension, Mean = 3.10, SD = 0.99). Additionally, each participant was asked to comment on the items' face validity and content validity via a corresponding comment field. All items which scored below a mean of 3.5 on representativeness were deleted or if corresponding comments were made, adjusted. The remaining 51 items were all rated to be highly representative of their respective dimension by the majority of the respondents and none were rated to be unrepresentative.

These 51 items were presented to a group of four marketing researchers who were tasked with assigning the items to the four CPO dimensions and asked to evaluate their clarity and conciseness. The set of 51 items was then translated into German, presented to three bi-lingual marketing researchers for a clarity evaluation of the German items, and then retained for the next step in the scale development process.

Step 6: Scale Refinement

We used 7-point Likert scale (1= strongly disagree to 7= strongly agree) to measure the 51 items. A convenience sample of 16 employees with management experience was recruited to test the two versions of the questionnaire (i.e., English and German). This pretest revealed no difficulties in understanding any of the items. Thus, the survey was distributed to 1,584 managers from the official mailing list of the Swiss Marketing Association with both English and German options to accommodate the language skills of participants. Using several reminders, we obtained 346 fully completed surveys from participants that passed all attention checks (a 22% response rate). These respondents all have managerial responsibility, an average professional experience in their current position of 6.76 years, and work in B2C industries (31%), B2B industries (24%), or industries that have a both a B2C and B2B focus (45%).

Their assessment of the 51 items were used in an exploratory factor analysis with direct oblimin rotation to reduce the number of viable items while allowing correlation between the items and test the underlying dimensions of the CPO construct. The resulting four factors were consistent with our expectations, and the four factors explained 57% of variance — see Table 4. Additionally, to avoid issues of cross loadings, 19 items with factor loadings lower than 0.60, and corrected item-to-total correlations of 0.50 and above were removed. The remaining 32 items showed satisfactory Cronbach's Alpha for all dimension (strategic CPO = .93, structural CPO = .93, operative CPO = .73, customer perceptions of CPO = .88). The intercorrelations of the resulting factors were as follows: The strategic dimension demonstrated significant negative correlations with the structural ($r = -.61$), operative ($r = -.41$), and the customer perceptions of privacy orientation ($r = -.13$). The structural dimension had positive correlations with the operative dimension ($r = .18$) and the customer perceptions of privacy orientation ($r = .42$). The operative dimension exhibited a positive correlation with customer perceptions of privacy



orientation ($r = .28$). The final set of 32 items was used in the next study, with the aim of obtaining a more parsimonious scale and to test for nomological validity.

Table 4: EFA in the Scale Refinement Step

51 Items	Strategic CPO	Structural CPO	Operative CPO	Customer Perceptions of CPO
Strat1	-.795	.492	.100	.324
Strat2	-.792	.402	.050	.350
Strat3	-.674	.489	.249	.279
Strat4	-.693	.348	.110	.488
Strat5	-.810	.654	.149	.400
Strat6	-.646	.636	.200	.209
Strat7	-.769	.646	.139	.296
Strat8	-.791	.600	.246	.470
Strat9	-.754	.627	.206	.378
Strat10	-.783	.535	.246	.374
Strat11	-.735	.602	.260	.376
Strat12	-.669	.533	.479	.359
Struc1	-.499	.707	-.064	.135
Struc2	-.613	.690	.037	.504
Struc3	-.402	.669	.070	.227
Struc4	-.663	.628	.014	.557
Struc5	-.411	.463	.348	.527
Struc6	-.656	.566	.047	.616
Struc7	-.657	.520	-.029	.632
Struc8	-.681	.716	.089	.454
Struc9	-.498	.714	.130	.438
Struc10	-.689	.817	.240	.471
Struc11	-.533	.763	.264	.300
Struc12	-.449	.734	.248	.498
Struc13	-.506	.802	.225	.411
Struc14	-.302	.570	.130	.410
Struc15	-.371	.449	.189	.607
Struc16	-.614	.549	.218	.680
Struc17	-.565	.740	.229	.422
Struc18	-.421	.673	.138	.528
Struc19	-.452	.780	.237	.435
Struc20	-.584	.729	.130	.322
Struc21	-.396	.637	.360	.345
Struc22	-.658	.743	.050	.484
Struc23	-.676	.775	.076	.465
Struc24	-.574	.731	.026	.338
CPe1	-.505	.487	.081	.694
CPe2	-.461	.464	.131	.697
CPe3	-.462	.434	.229	.748
CPe4	-.369	.435	.307	.693
CPe5	-.252	.251	.315	.793
CPe6	-.188	.215	.320	.786
CPe7	-.407	.331	.416	.828
Ope1	-.216	.231	.658	.263
Ope2	-.263	.190	.612	.413
Ope3	-.239	.274	.717	.409
Ope4	-.351	.575	.473	.255
Ope5	-.177	.183	.600	.550
Ope6	-.488	.458	.318	.714
Ope7	-.406	.458	.256	.680
Ope8	-.226	.337	.265	.560

Step 7: Scale Purification

We conducted a second quantitative study to confirm the newly developed scale's dimensionality, reliability, and nomological validity. Therefore, we included not only the 32 items in the questionnaire but also additional items, introduced and discussed in Step 8.

A sample of managers from publicly traded customer-facing companies from the European Union, the United Kingdom, and Switzerland was recruited via prolific. All participants were filtered according to the above stated inclusion criteria (i.e., at least one year of managerial experience in their current position) and paid for participation. Publicly traded firms of larger size were chosen to ensure that they fall under the GDPR mandate of employing a data privacy officer – either directly or by the market location principle (GDPR Art. 13). This was done to ensure that all questions relating to data privacy of officers would point to the legally required and uniform set of duties. The recruiting process yielded 418 participants. These were filtered to exclude any participants who failed attention checks. 387 answers were chosen as a basis for the final study. These respondents all have managerial responsibility, an average professional experience in their current position of 6.23 years, and work in B2C industries (43%) or industries that have both a B2C and B2B focus (57%). Prominent industries in the sample include Retail and FMCG (15%), Healthcare and Medical (12%), and Banking and Financial Services (12%).

An exploratory factor analysis of the 32 items confirmed CPO's dimensionality, indicating the same four-factor structure, and explaining 66% of total variance — see Table 5. To simplify the use of the CPO construct for future research and to be more appealing for marketing practice, we aimed to develop a more parsimonious scale (Homburg and Tischer 2023). Therefore, we selected the three items with the highest loadings of each of the four CPO dimensions, keeping a concise scale of 12 items.

Cronbach's Alpha was satisfactory for all dimensions of the reduced scale (strategic CPO = .84, structural CPO = .89, operative CPO = .92, customer perceptions of CPO = .78). The resulting measurement model with 12 items provided a good fit to the data ($\chi^2 = 138.1$; $df = 48$; $p < 0.001$; CFI = 0.968; TLI = 0.956; RMSEA = .070; PCMIN/DEF = 2.87; SRMR = 0.038). The inter-item correlations of each dimension exceeded a value of 0.50, suggesting convergent validity. Average variance extracted for each dimension exceeded the recommended level of 0.50. Finally, discriminant validity was tested with 0.85 cut-off in a comparison of AVE and shared variance between the construct and found to be satisfactory.

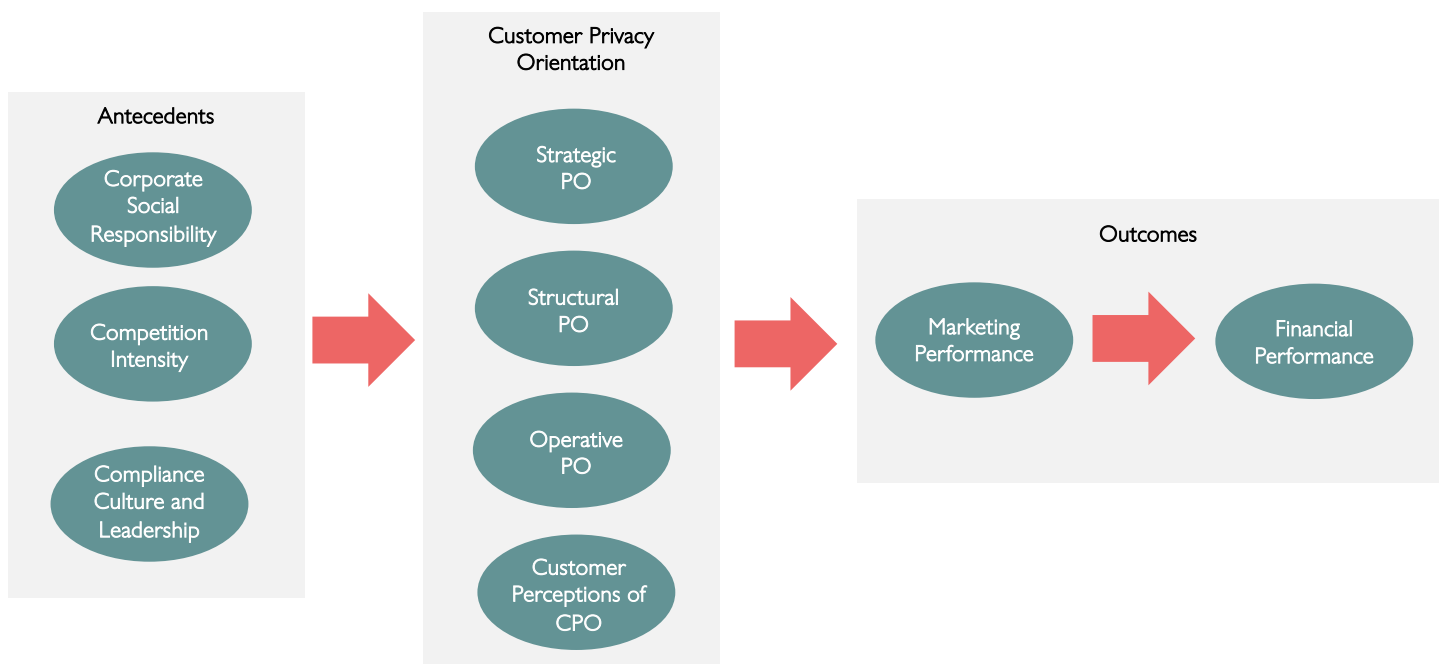
Table 5: EFA in the Scale Purification Step

32 Items	Strategic CPO	Structural CPO	Operative CPO	Customer Perceptions of CPO
Strat1	.833	.527	.166	-.371
Strat2	.828	.565	.114	-.443
Strat3	.822	.389	.278	-.329
Strat4	.724	.557	.185	-.619
Strat5	.796	.709	.280	-.462
Strat6	.645	.663	.263	-.371
Strat7	.763	.712	.227	-.534
Strat8	.657	.711	.287	-.460
Strat9	.815	.681	.266	-.517
Strat10	.781	.668	.257	-.532
Struc1	.435	.784	.233	-.491
Struc2	.593	.850	.270	-.477
Struc3	.492	.816	.293	-.497
Struc4	.471	.704	.216	-.299
Struc5	.380	.709	.238	-.352
Struc6	.625	.770	.241	-.623
Struc7	.547	.818	.119	-.547
Struc8	.440	.747	.383	-.327
Struc9	.556	.741	.379	-.420
Struc10	.578	.768	.361	-.543
Struc11	.534	.732	.211	-.362
Struc12	.491	.739	.196	-.329
CPe1	.428	.427	.386	-.866
CPe2	.400	.379	.367	-.882
CPe3	.534	.512	.439	-.847
CPe4	.517	.670	.244	-.723
CPe5	.471	.663	.270	-.776
CPe6	.486	.622	.272	-.758
Ope1	.152	.264	.800	-.175
Ope2	.205	.236	.771	-.319
Ope3	.268	.339	.846	-.335
Ope4	.297	.297	.708	-.466

Step 8: Nomological Validity

We used the data collection reported above to test for nomological validity. The nomological network of CPO is presented in Figure 1. The antecedents and consequences were chosen in accordance with the predominant constructs and relationships relevant to privacy in marketing as defined by Martin & Murphy (2017, p. 140). Specifically, seeing how CSR promotes proactive engagement in several stakeholder interests and has also been discussed as an important foundation in constructs such as corporate digital responsibility (Lobschat et al., 2021; Wirtz et al., 2023), we deem it as an important antecedent of CPO. In addition, compliance culture and leadership based on Amankwa et al. (2018) is seen as a baseline requirement for CPO. Furthermore, competition intensity has been suggested in past research to play “an important role” in shaping how well firms can compete with a privacy-oriented positioning (Casadesus-Masanell & Hervás-Drane, 2015, p. 242). Our interviews as well as previous studies (K. D. Martin et al., 2017) also suggest that an increased CPO could lead to higher levels of marketing performance by more closely aligning customers’ privacy expectations with the data processing of a given firm (Quach et al., 2022). Such a mutually beneficial relationship would ideally drive a firm’s financial performance (K. D. Martin et al., 2020, p. 477). All scales in the nomological network of CPO and their properties can be found in the Appendix

Figure 1: Nomological Network of Customer Privacy Orientation





The EFA of all measured items mapped them on the 9 theoretical constructs and explained 68% of variance. Cronbach's Alpha was satisfactory for each construct and the CFA of all nine constructs provided a good fit for the data ($\chi^2 = 1762.53$; $df = 783$; $p < 0.001$; CFI = 0.921; TLI = 0.913; RMSEA = .057 ; PCMIN/DEF = 2.25; SRMR = 0.045). This study relied on structural equation modelling to investigate the relationship between the three antecedents, four CPO dimensions and two consequences. First, a model with CPO as a second order construct was estimated using the lavaan SEM package for JASP and demonstrated good fit to the data ($\chi^2 = 1852.76$; $df = 806$; $p < 0.001$; CFI = 0.915; TLI = 0.909; RMSEA = .058 ; PCMIN/DEF = 2.30; SRMR = 0.060). Second, to test the effects of the antecedents on the individual CPO dimensions as well as the effects of the individual CPO dimensions on the outcomes, a model with the individual CPO dimensions was estimated. The resulting model also showed an overall good fit to the data ($\chi^2 = 1890.82$; $df = 795$; $p < 0.001$; CFI = 0.911; TLI = 0.904; RMSEA = .060 ; PCMIN/DEF = 2.38; SRMR = 0.062). We present the results for both models in Table 6

Table 6: Results of Structural Equation Modeling

Path	β (standardized)	S.E.	p
<i>Model 1: Second Order Construct for CPO</i>			
CSR → CPO	0.274	0.036	<.001
Compliance Culture and Leadership → CPO	0.639	0.055	<.001
Competition Intensity → CPO	-0.003	0.027	0.936
CPO → Marketing Performance	0.552	0.062	<.001
CPO → Financial Performance	-0.078	0.070	0.186
Marketing → Financial Performance	0.720	0.093	<.001
<i>Model 2: Dimensions of CPO</i>			
CSR → Strategic PO	0.119	0.052	<.050
CSR → Structural PO	0.211	0.051	<.001
CSR → Oper. PO	0.403	0.058	<.001
CSR → Customer Perceptions of CPO	0.202	0.053	<.001
Compliance Culture and Leadership → Strategic PO	0.600	0.071	<.001
Compliance Culture and Leadership → Structural PO	0.578	0.070	<.001
Compliance Culture and Leadership → Operative PO	0.129	0.066	<.050
Compliance Culture and Leadership → Customer Perceptions of CPO	0.483	0.068	<.001
Competition Intensity → Strategic. PO	-0.081	0.043	0.087
Competition Intensity → Structural PO	0.003	0.041	0.935
Competition Intensity → Operative PO	0.116	0.044	<.050
Competition Intensity → Customer Perceptions of CPO	-0.078	0.043	0.097
Strategic PO → Marketing Performance	0.095	0.043	0.142
Structural PO → Marketing Performance	0.214	0.042	<.001
Operative PO → Marketing Performance	0.162	0.044	<.010
Customer Perceptions of CPO → Marketing Performance	0.199	0.040	<.010



Across both models, CSR was positively related to CPO ($\beta = .302, p < 0.001$) and its strategic ($\beta = .119, p < 0.05$), structural ($\beta = .211, p < 0.001$), operative ($\beta = .448, p < 0.001$), and perceptual dimensions ($\beta = .202, p < 0.001$). Compliance culture and leadership was positively related to the second order CPO construct ($\beta = .639, p < 0.001$) as well as its strategic ($\beta = .600, p < 0.001$), structural ($\beta = .578, p < 0.001$), operative ($\beta = .129, p < 0.05$) and perceptual dimensions ($\beta = .483, p < 0.001$). Surprisingly, competition intensity was neither significantly related to on CPO ($\beta = -.003, p = 0.936$) nor to its strategic ($\beta = -.081, p = 0.087$), structural ($\beta = -.003, p = 0.935$) or perceptual dimensions ($\beta = -.078, p = 0.097$). There was a only a significant positive effect on the operative privacy orientation ($\beta = .116, p < 0.05$). Thus, based on our findings, it would be worth to revisit competition intensity as a potential antecedent of CPO.

The results also provide first indication that an increased CPO is related to higher levels of marketing and in turn financial performance. CPO was found to have a significant positive effect on marketing performance ($\beta = .552, p < 0.001$) but not directly on financial performance ($\beta = -.078, p = 0.116$). However, the effect is mediated through marketing performance ($\beta = .720, p < 0.001$).¹ Looking at the individual CPO dimensions, the positive relationship with marketing performance is driven by the structural ($\beta = .214, p < 0.01$), operative ($\beta = .162, p < 0.01$) and perception driven dimensions ($\beta = .192, p < 0.01$). The effect of the strategic dimension on marketing performance is non-significant ($\beta = .095, p = 0.142$), which suggests that it is not the strategy that led to desirable outcomes but rather its implementation. In total, the nomological network sheds first light on the patterns and relations which drive and are driven by CPO.

¹ It must be acknowledged that marketing and financial performance are measured subjectively. Thus, while they provide a positive link in the context of nomological validity they may be limited in terms of objective consequences.

Discussion

We developed a holistic conceptualization of CPO which integrates the previously isolated strategic, structural, operative, and perceptual perspectives. We then operationalize CPO as a self-assessment scale showing internal consistency, reliability, and validity. Moreover, we identify three antecedents to CPO and provide first evidence for its positive effect on marketing and firm performance. The results of these efforts provide important theoretical and practical implications on the applications of privacy orientation on the organizational level.

Theoretical implications

Our reconceptualization and operationalization contribute to the literature stream on data ecosystems, privacy in small and medium-sized enterprises, and data driven innovation. First, our conceptualization and measurement instrument for CPO provides important insight to data ecosystems (Wirtz et al., 2023). Data-driven value creation is often not achieved within a single firm, but rather in a larger data ecosystem of collaborators (Quach et al., 2022). From a customer perspective, informed consent to share data becomes unlikely, due to the hard to predict ramifications of privacy violations in an ecosystem context. From a company perspective, the question of how to position oneself within such a data eco-system becomes central – both to select reliable collaborators and to signal reliability to other industry actors (Lobschat et al., 2021). Thus, a common conceptualization and measurement instrument for CPO allows to compare actors within such an ecosystem or assess risk levels as well as their source.

Second, there is a lack of personnel and expertise to ensure a strategically aligned and secure data processing in small and medium-sized enterprises (Heidt et al., 2019; Li et al., 2022). At the same time, it is expected that even SMEs, with access to AI-driven tools and analysis instruments, will collect and process larger amounts of data in the foreseeable future (Bianchini & Michalkova, 2019). If such data processing is launched without a prior definition of strategic objectives, there is a risk of an "erosion of privacy" for their customers (Palmatier & Martin, 2019, p. 87). To address this problem, many European SMEs rely on manual GDPR compliance test, which are both costly and do not address the lack of a strategic direction. As such "building a shared understanding of privacy's non-functional requirements" is crucial to analyzing a given SME's data strategy and suggest privacy improvements (Li et al., 2022).

Third, data driven innovations increase privacy concerns in consumers – especially if new types of data are demanded by it (Bleier et al., 2020). With an increasing concern amongst consumers about how their data is used by marketers (Kim et al., 2019) trust in a firm's privacy measures become the central drivers of information disclosure behavior (Hayes et al., 2021a; Shin et al., 2022). However, while metrics such as the consumer-brand-relationship might predict the willingness to disclose novel data, it does not resolve the tension between privacy needs and data demands. As such, to avoid consumer backlash from potential privacy violations, a firm must exhibit a strong privacy orientation as well (Balapour et al., 2020; Wu et al., 2012).

Practical implications

Mirroring the theoretical contributions, we also provide important practical implications. First, with the ratification of the GDPR, a compliance baseline was established which can and has been used to evaluate both individual firms as well as data ecosystems. Unfortunately, these evaluations are usually done post-hoc and do not account for a host of risk factors related to data privacy (Lupiáñez-Vilanova et al., 2022). Yet, due to the rapid digitalization of most industries, the need to assess the privacy orientation of such ecosystems only grows (Lobschat et al., 2021; Wirtz et al., 2023). Hence, our measure of CPO may be used to characterize and compare the privacy strategy of actors within the same data ecosystem. At the same time, managers may use the four CPO dimensions to position themselves more effectively within a given data ecosystem.

Second, to balance the data needs of a competitive business with privacy laws requires both a common conceptualization of privacy orientation as well as a means of measuring it reliably over time (Li et al., 2022). CPO and its corresponding scale allow to assess the current direction of an SME's privacy strategy across its four dimensions. In doing so, specific weaknesses can be identified and corrected. At the same time, the scale can be used to track the progress of change initiatives and compare them with other companies in the same industry. This is especially relevant for emerging technologies like the Metaverse, whose widespread adoption could be stopped due to consumers' missing trust or privacy concerns (Dwivedi et al., 2022).

Third, customer concerns have been measured using privacy calculus scales (Hayes et al., 2021b; Shin et al., 2022) which do not take a firm's ability to address privacy concerns sustainably into account. CPO both considers the customers' perspective while also assessing a firm's overall capability to satisfy privacy needs in the long term. As such, future studies might use CPO as a basis to assess the success and acceptance of a data driven innovation in a given industry context.

Limitations and directions for further research

The results of this study are to be understood within the following limitations. First, while the reconceptualization of CPO is based on an extensive systematic literature review and interviews and surveys with a balanced mix of industry professionals, it is not tailored to any specific industry or market. Adapting the CPO scale to industries with specific privacy needs (e.g., health care, insurances, banking) may yield additional insights for the future of data processing in these fields. Second, the CPO construct was designed with the European market in mind. As such, it reflects a European understanding of management processes and privacy as a human right – analogue to the GDPR. However, considering how context-sensitive all other privacy research has shown itself to be (K. D. Martin & Murphy, 2017), the proposed framework might be expanded by taking different management styles, cultures, markets, or legal guidelines into consideration. Third, we focused our sample on managerial professionals from customer facing, large enterprises in Europe. This was done to ensure the practicability and relevance to other profit-driven businesses. However, we acknowledge that other professionals (e.g., legal experts or policy makers) might have advocated for even stricter measures to improve CPO. Consequently, we suggest future studies focus on evaluating CPO from the perspective of different stakeholders to draw comparative results and to further expand our understanding of CPO. Fourth, throughout this paper, research efforts were focused on the privacy of customer data, meaning private individuals, not other companies. As such, all results mostly relate to organizations in a business to consumer (B2C) market. However, we suspect that the benefits of privacy orientation might also



increase the digital trust in organizations looking to participate in a larger data ecosystem (Wortmann et al., 2022). Future studies might therefore use the CPO construct to explore its benefits and downsides in a business-to-business context. Finally, the results of our nomological validity analysis suggest several paths for future research. Our initial model looked at three antecedents and two consequences. All the measurements relied on the accurate self-assessment of the participants and might therefore be skewed by their perception. Hence, no secondary performance data on the companies of the sample was employed. By using a longitudinal study design or using market data in combination with the CPO scale, additional insights into its effects are sure to be gained.

References

- Acquisti, A., Komanduri, S., Analytics, C., Leon, P. G., De Mexico, B., Schaub, F., Wang, Y., Wilson, S., Cranor, ; L F, Sadeh, N., Wang, ; Y, Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Sadeh, N., Sleeper, M., Wang, Y., Adjerid, I., ... Sleeper, M. (2017). 44 Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, 50(3), 1–41. <https://doi.org/10.1145/3054926>
- Allen, A. M., & Peloza, J. (2015). Someone to watch over me: The integration of privacy and corporate social responsibility. *Business Horizons*, 58(6), 635–642. <https://doi.org/10.1016/j.bushor.2015.06.007>
- Amankwa, E., Looock, M., & Kritzing, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, 420–436. <https://doi.org/10.1108/ICS-09-2017-0063>
- Ashley, P., Powers, C., Schunter, M., & Terms, G. (2002). From Privacy Promises to Privacy Management A New Approach for Enforcing Privacy Throughout an Enterprise. *New Security Paradigms Workshop*, 43–50.
- Assarroudi, A., Heshmati Nabavi, F., Armat, M. R., Ebadi, A., & Vaismoradi, M. (2018). Directed qualitative content analysis: the description and elaboration of its underpinning methods and data analysis process. *Journal of Research in Nursing*, 23(1), 42–55. <https://doi.org/10.1177/1744987117741667>
- Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, 52. <https://doi.org/10.1016/j.ijinfomgt.2019.102063>
- Bamberger, K. A., & Mulligan, D. K. (2010). New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States. *Law and Policy*, 1–32. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701087
- Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147–154. <https://doi.org/10.1016/j.chb.2015.11.022>
- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. *Foundations and Trends in Marketing*, 11(1), 1–71. <https://doi.org/10.1561/17000000057>
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. In *MIS Quarterly: Management Information Systems* (Vol. 35, Issue 4, pp. 1017–1041). University of Minnesota. <https://doi.org/10.2307/41409971>
- Bianchini, M., & Michalkova, V. (2019). Data Analytics in SMEs: Trends and Policies. *OECD SME and Entrepreneurship Papers*, 15, 1–45. <https://doi.org/10.1787/1de6c6a7-en>
- Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466–480. <https://doi.org/10.1016/j.IJRESMAR.2020.03.006>
- Bloemendal, M. ten. (2022). On the advent of environmental, social and governance reporting and its intersection with privacy. *Journal of Data Protection & Privacy*, 5(1), 39–49.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, 00(0), 1–25. <https://doi.org/10.1177/0093650218800915>

- Bu, F., Wang, N., Jiang, B., & Liang, H. (2020). "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management*, 53, 102124. <https://doi.org/10.1016/j.ijinfomgt.2020.102124>
- Casadesus-Masanell, R., & Hervas-Drane, A. (2015). Competing with privacy. *Management Science*, 61(1), 229–246. <https://doi.org/10.1287/mnsc.2014.2023>
- Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291–302. <https://doi.org/10.1016/j.chb.2017.01.003>
- Chen, S. (Joseph), Tran, K. T., Xia, Z. (Raymond), Waseem, D., Zhang, J. A., & Potdar, B. (2023). The double-edged effects of data privacy practices on customer responses. *International Journal of Information Management*, 69. <https://doi.org/10.1016/j.ijinfomgt.2022.102600>
- Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, 28(5), 1859–1872. <https://doi.org/10.1016/j.chb.2012.05.004>
- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51. <https://doi.org/10.1016/j.chb.2017.12.001>
- Chui, M., Yee, L., Hall, B., Singla, A., & Sukharevsky, A. (2023). *The state of AI in 2023: Generative AI's breakout year August 1, 2023 | Survey*. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year>
- Cisco. (2022). *Data Transparency's Essential Role in Building Customer Trust - Cisco Consumer Privacy Survey*.
- Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), 323–342. <https://doi.org/10.1111/1540-4560.00067>
- Davenport, T. H., & Bean, R. (2023). *Data and analytics leadership annual executive survey - delivering business value from data and analytics investments*.
- Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, 21(5), 368–383. <https://doi.org/10.1111/jcc4.12163>
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2012). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22, 295–316. <https://doi.org/10.1057/ejis.2012.23>
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., ... Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>
- Fraj, E., Martínez, E., & Matute, J. (2011). Green marketing strategy and the firm's performance: the moderating role of environmental culture. *Journal of Strategic Marketing*, 19(4), 339–355. <https://doi.org/10.1080/0965254X.2011.581382>

- Gerlach, J. P., Eling, N., Wessels, N., & Buxmann, P. (2019). Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Information Systems Journal*, 29(2), 548–575. <https://doi.org/10.1111/isj.12222>
- Glaser, B., & Strauss, A. (1967). *The discover of grounded theory: Strategies for qualitative research*. Aldine de Gruyter.
- Gotsch, M. L., & Schögel, M. (2021). Addressing the privacy paradox on the organizational level: review and future directions. *Management Review Quarterly* 2021, 1–34. <https://doi.org/10.1007/S11301-021-00239-4>
- Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. *Information Systems Journal*, 25(6), 579–606. <https://doi.org/10.1111/isj.12080>
- Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. L. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems*, 24(2), 13–42. <https://doi.org/10.2753/MIS0742-1222240202>
- Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021a). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, 55, 16–30. https://doi.org/10.1016/J.INTMAR.2021.01.001/ASSET/IM-AGES/LARGE/10.1016_J.INTMAR.2021.01.001-FIG6.JPEG
- Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021b). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, 55, 16–30. <https://doi.org/10.1016/J.INTMAR.2021.01.001>
- Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, 21(6), 1285–1305. <https://doi.org/10.1007/S10796-019-09959-1>
- Hermalin, B. E., & Katz, M. L. (2006). Privacy, property rights and efficiency: The economics of privacy as secrecy. *Quant Market Econ*, 4, 209–239. <https://doi.org/10.1007/s11129-005-9004-7>
- Hoffman, D. L., Moreau, C. P., Stremersch, S., & Wedel, M. (2022). The Rise of New Technologies in Marketing: A Framework and Outlook. *Journal of Marketing*, 86(1), 1–6. <https://doi.org/10.1177/00222429211061636>
- Homburg, C., Artz, M., Wieseke, J., Homburg is Professor of Business Administration, C., Wieseke is Professor of Business Administration, J., Glaser, M., Hahn, A., Haumann, T., Klar-mann, M., Totzek, D., & van Triest, S. (2012). Marketing Performance Measurement Systems: Does Comprehensiveness Really Improve Performance?: *Journal of Marketing*, 76(3), 56–77. <https://doi.org/10.1509/JM.09.0487>
- Homburg, C., Schwemmler, M., & Kuehnl, C. (2015). New product design: Concept, measurement, and consequences. *Journal of Marketing*, 79(3), 41–56. <https://doi.org/10.1509/jm.14.0199>
- Huang, H. Y., & Bashir, M. (2020). “Seeking Privacy Makes Me Feel Bad?”: An Exploratory Study Examining Emotional Impact on Use of Privacy-Enhancing Features. *Advances in Intelligent Systems and Computing*, 1129 AISC, 600–617. https://doi.org/10.1007/978-3-030-39445-5_44
- Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review: *Big Data & Society*, 8(1), 1–17. <https://doi.org/10.1177/2053951720982012>
- Jiang, Z., Suang Heng, C., & F Choi, B. C. (2013). Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, 24(3), 579–595. <https://doi.org/10.1287/isre.1120.0441>

- Kim, T., Barasz, K., & John, L. K. (2019). Why am i seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, 45(5), 906–932. <https://doi.org/10.1093/jcr/ucy039>
- Kitkowska, A., Wästlund, E., Martucci, L. A., Warner, M., & Shulman, Y. (2020). Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. *Sixteenth Symposium on Usable Privacy and Security*, 437–456.
- Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, 146. <https://doi.org/10.1016/j.infsof.2022.106868>
- Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, 122, 875–888. <https://doi.org/10.1016/j.jbusres.2019.10.006>
- Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., Rodríguez De Las, T., & Ballell, H. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*.
- Lytras, M. D., Visvizi, A., Chopdar, P. K., Sarirete, A., & Alhalabi, W. (2021). Information Management in Smart Cities: Turning end users' views into multi-item scale development, validation, and policy-making recommendations. *International Journal of Information Management*, 56. <https://doi.org/10.1016/j.ijinfomgt.2020.102146>
- Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. *MIS Quarterly*, 35(2), 293–334. <https://doi.org/https://doi.org/10.2307/23044045>
- Martin, K. (2018a). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, 82, 103–116. <https://doi.org/10.1016/J.JBUSRES.2017.08.034>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, 81(1), 36–58. <https://doi.org/10.1509/jm.15.0497>
- Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., Wang, Y., & Weaven, S. K. (2020). Data Privacy in Retail. *Journal of Retailing*, 96(4), 474–489. <https://doi.org/10.1016/j.jretai.2020.08.003>
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/10.1007/s11747-016-0495-4>
- Miltgen, C. L., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research*, 69(10), 4659–4666. <https://doi.org/10.1016/j.jbusres.2016.04.015>
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Pappas, I. O., Mikalef, P., Dwivedi, Y. K., Jaccheri, L., & Krogstie, J. (2023). Responsible Digital Transformation for a Sustainable Society. In *Information Systems Frontiers* (Vol. 25, Issue 3, pp. 945–953). Springer. <https://doi.org/10.1007/s10796-023-10406-5>
- Pelteret, M., & Ophoff, J. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. *Informing Science: The International Journal of an Emerging Transdiscipline*, 19. <http://www.informingscience.org/Publications/3573>
- Pollach, I. (2011). Online privacy as a corporate social responsibility: an empirical study. *Business Ethics: A European Review*, 20(1), 88–102. <https://doi.org/10.1111/J.1467-8608.2010.01611.X>



- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, 1–25. <https://doi.org/10.1007/S11747-022-00845-Y/TABLES/4>
- Shastri, S., Wasserman, M., & Chidambaram, V. (2019). The Seven Sins of Personal-Data Processing Systems under GDPR. *11th USENIX Workshop on Hot Topics in Cloud Computing*, 1–7.
- Shin, D., Kee, K. F., & Shin, E. Y. (2022). Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms? *International Journal of Information Management*, 65. <https://doi.org/10.1016/j.ijinfomgt.2022.102494>
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- Stahl, B. C., & Eke, D. (2024). The ethics of ChatGPT – Exploring the ethical issues of an emerging technology. *International Journal of Information Management*, 74. <https://doi.org/10.1016/j.ijinfo-mgt.2023.102700>
- Steinhoff, L., & Martin, K. D. (2022). Putting Data Privacy Regulation into Action: The Differential Capabilities of Service Frontline Interfaces. *Journal of Service Research*, 0(0). <https://doi.org/10.1177/10946705221141925>
- Turker, D. (2009). Measuring Corporate Social Responsibility: A Scale Development Study. *Journal of Business Ethics*, 85, 411–427. <https://doi.org/10.1007/s10551-008-9780-6>
- Uysal, E., Alavi, S., & Bezençon, V. (2022). Trojan horse or useful helper? A relationship perspective on artificial intelligence assistants with humanlike features. *Journal of the Academy of Marketing Science*, 50(6), 1153–1175. <https://doi.org/10.1007/s11747-022-00856-9>
- Wirtz, J., Kunz, W., Hartley, N., Tarbit, J., & Kunz, W. H. (2023). Corporate Digital Responsibility in Service Firms and Their Ecosystems. *Journal of Service Research*, 1–47. https://www.researchgate.net/publication/363487796_Corporate_Digital_Responsibility_in_Service_Firms_and_Their_Ecosystems/
- Wortmann, F., Schäfer, F., Bronner, W., Slama, D., Peylo, C., & Natalia Oropeza. (2022). *Establishing Digital Trust - Towards a Strategic Roadmap for Industrial Companies*. <https://digitaltrustforum.org/index.html>
- Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889–897. <https://doi.org/10.1016/j.chb.2011.12.008>



Appendix: Additional Measurement Scales and their Properties

Scales and Items ("At my company...")	Mean	SD
<i>Strategic privacy orientation (alpha =0.837)</i>		
• top management explicitly names data privacy as an important part of our company's strategy.	5.35	1.64
• top management emphasizes that the protection of costumers' data privacy is the responsibility of each employee.	5.66	1.54
• the protection of the data privacy of customers is named within our mission statement.	4.79	1.83
<i>Structural privacy orientation (alpha =0.889)</i>		
• all accesses to our customer data are logged and recorded.	5.20	1.81
• we regularly conduct internal privacy risk assessments with a clearly defined scope.	4.83	1.84
• our company has a system in place that ensures that improper or frequent accesses to customer data are immediately noticed.	4.89	1.77
<i>Customer perceptions of privacy orientation (alpha =0.920)</i>		
• our customers understand, what data we collect from them.	5.11	1.61
• our customers understand, why we collect data from them.	5.21	1.53
• our data processing activities are transparent to our customers.	5.09	1.63
<i>Operative privacy orientation (alpha =0.781)</i>		
• we only collect enough data from customers to fulfil their order(s).	5.25	1.61
• our customers can test our products and services without sharing a lot of personal data.	4.25	1.93
• we make efforts to use as little personal data for our products and services as possible.	4.59	1.74
<i>Corporate social responsibility (Turker, 2009, alpha = 0.942)</i>		
• we participate in activities which aim to protect and improve the quality of the natural environment.	4.75	1.79
• we make investment to create a better life for future generations.	4.76	1.74
• we implement special programs to minimize our negative impact on the natural environment.	4.74	1.79
• we target sustainable growth which considers future generations.	4.76	1.79
• we support non-governmental organizations working in problematic areas.	4.37	1.87
• we contribute to campaigns and projects that promote the well-being of the society.	4.88	1.68
• we encourage our employees to participate in voluntary activities.	4.77	1.91
• we emphasize the importance of our social responsibilities to the society.	4.97	1.70
<i>Competition intensity (Homburg et al., 2012, alpha = 0.922)</i>		
• Competition in our industry is cutthroat.	4.70	1.80
• There are many competitive rivalries in our industry.	5.11	1.77
• Our competitors are relatively strong.	5.12	1.64
• Intensive competitor-related activities are a hallmark in our industry.	4.78	1.70
<i>Compliance culture and leadership (Amankwa et al., 2018, alpha = 0.926)</i>		
• A mechanism for monitoring information security policies exists.	5.37	1.49
• I believe it is necessary for our company to have an officer or team monitoring compliance with information security policies	5.64	1.48
• Following security policy is a key part of my everyday duties and responsibilities.	5.25	1.71
• Our security managers often emphasize the importance of compliance with security policies.	5.52	1.52
• Information security policy is given high priority by our security managers.	5.53	1.51



- Our top management (including security managers) have always demonstrated compliance with information security policies. 5.40 1.53
- Security awareness and training programs that emphasize the importance of compliance with security policies exist in our company. 5.54 1.57

Marketing performance (Fraj et al., 2011, alpha = 0.867)

Please rate each item from a 1=with respect to our competitors, our position is much worse to 7=with respect to our competitors, our position is much better

- Corporate reputation 5.18 1.32
- Alignment between company's offer and market expectations 5.14 1.23
- Successful launching of new products onto the markets 4.97 1.39
- Corporate and brand image 5.25 1.37
- Customer loyalty 5.36 1.29
- Customer satisfaction 5.38 1.24

Financial performance (Fraj et al., 2011, alpha = 0.905)

Please rate each item from a 1=with respect to our competitors, our position is much worse to 7=with respect to our competitors, our position is much better

- Profitability 5.03 1.43
 - Sales growth 4.98 1.38
 - Economic results 4.98 1.35
 - Profit before tax 4.95 1.44
 - Market share 4.92 1.42
-