

University of St. Gallen
School for Management, Economics,
Law, and Social Sciences

Privacy as Strategy

Conceptualisation and Implementation of Organisational Privacy Orientation

Mauro Luis Gotsch

Gallusstrasse 6

9000 St. Gallen

Tel.: +41 71 224 75 70

E-Mail: mauro.gotsch@unisg.ch

Dissertation

Supervisor: Prof. Dr. Marcus Schögel

Co-Supervisor: Prof. Dr. Reinhard Jung

University of St. Gallen

Winter Semester 2022

“Futuristic as this may sound, the vision of individuals and groups as so many objects to be continuously tracked, wholly known, and shunted this way or that for some purpose of which they are unaware has a history. It was coaxed to life nearly sixty years ago under the warm equatorial sun of the Galapagos Islands, when a giant tortoise stirred from her torpor to swallow a succulent chunk of cactus into which a dedicated scientist had wedged a small machine.

It was a time when scientists reckoned with the obstinacy of free-roaming animals and concluded that surveillance was the necessary price of knowledge. Locking these creatures in a zoo would only eliminate the very behaviour that scientists wanted to study, but how were they to be surveilled? The solutions once concocted by scholars of elk herds, sea turtles, and geese have been refurbished by surveillance capitalists and presented as an inevitable feature of twenty-first-century life on Earth. All that has changed is that now we are the animals.”

- Shoshana Zuboff, The Age of Surveillance Capitalism

Acknowledgements

First of all, I would like to thank Prof. Dr. Marcus Schögel for giving me the inspiration for the topic of my dissertation and providing me with the opportunity to research and work at the intersection of marketing theory and practice. Marcus helped me to see the relevance in my research and how theory is successfully translated into actionable strategies. Thank you Marcus for your support, encouragement and four years of interesting discussions.

Furthermore, I would like to thank Prof. Dr. Reinhard Jung for the feedback and guidance on my research design and his helpful advice on developing my research proposal into a research project worth pursuing.

Apart from my academic advisors, I have a long list of friends, consultants and colleagues which I would like to thank for making my time as a doctoral student such a memorable journey. These are the people who kept track of my progress, motivated me to keep going and shaped this dissertation in a myriad minor and major ways for the better.

Thank you to my brilliant colleagues and the old “French Press Crew”. Martin S. (a.k.a. Martin Schuhmacher), I still miss our banter, your “good” ideas, agar.io, all the platforms, Macklemore and millionaire’s bacon. Martin B. (our equal opportunities officer) – without your calm and kind nature, there never would have been a crew to begin with (and Martin S. would have overslept far more often). Iris (die Strenge von der MRSG), not only did you buy the French press in the first place, your advice and support (both academically and otherwise) helped all of us be our best selves. Severin (our “savage” VUCA expert), your sharp wit and talent for information gathering made working on projects together a joy and ensured we had something to talk about at all times. Felix, I am still happy I profiled you as a fellow nerd the minute you walked into the office – I learned much through our free-form conversations, flowing easily from historical topics to literature to D&D and back again. To all of you: I will never forget the discussions, stories and wild adventures we shared together. I hope they were just a prelude to many more yet to come.

I would like to thank Marcel C., whom I first met because he cycled all the way from Appenzell to Zurich Altstetten to ask if he could join the Engulgasse flat. Thank you for painted walls, flat pizzas, stuffed chickens, design science research, furniture I was too lazy to buy, and boardgame nights with the fate of humanity at stake. You made me feel at home in St. Gallen.

I’m grateful to the “post-pandemic” generation of colleagues at the institute (in chronological order): Friederike R., Alexander T., Susanna R., Pia S., Eve G., Malte B and Thedda D. It was a pleasure seeing you all start on the same journey, and I hope my sarcastic quips and heartfelt advice were of any help to you. I think the institute is in good hands with you all.

Florian G., thank you for your help with the Bootcamp and all other MiMM-related work. I've greatly enjoyed our political discourse (and your political engagement in general) and I am happy that we managed to publish two papers together in the very last weeks of my doctorate.

Thank you to Brigitte, Joachim and Alex for making me feel at home in the Swabian vineyards, for parties with and without Olma Bratwürsten, for helping to lock up a treasure chest, and for all your support during my doctorate.

Of course, a large portion of thanks goes to my family. To my parents, thank you for unconditionally supporting me in my studies; both emotionally and financially. Marco, thank you for teaching me your work ethic and can-do attitude, for any crafting skills I possess, for continuously building our beautiful retreat in the mountains and of course, for the best mulled wine in Grisons. Thank you to Bea for being the family's sage, whom everyone looks to for guidance, for raising us to be curious, for talks about food, music and movies and especially for your good humour. To both of you, without your guidance and the home, you have always kept open to me, I would have never had the confidence to pursue my studies. Nina, thank you for being my role model and the person who made me value knowledge in all its forms since I was a child. If it weren't for your example, I would have never applied for the cantonal school or even my Bachelor. Your effortless intellectual curiosity and interested mind are still the ideals I strive towards (even if I still disagree with most your movie opinions and like to argue with you on long car-rides).

Finally, I would like to thank Iris. With you, facing writing slumps, long seminars, cold flats, warm beers, difficult puzzles, Geheimnummern, coughing ghosts, low R squared, steep mountain roads, German internet, bad puns or even a global pandemic were a breeze. As such, it is no exaggeration when I say: Of all the great things that happened to me during this journey, meeting you is still easily the best.

Thank you all!

Summary

Discussions on the protection of data privacy have been following in the shadow of all major digital innovations of the past twenty years. Consumers' data privacy concerns are growing globally, and several strict data protection regulations have been passed as a response. Consequently, most organisations are confronted with the question of how their data processing activities could be more closely aligned with their customers' privacy needs. Marketing as function plays a central role in answering this question; both as a driver of problematic data processing and as a potential solution to it. While there have been several marketing studies looking at the psychology and economics of privacy, the field is still missing a lens to unify these disparate research streams. Specifically, a conceptualisation of privacy orientation on an organisational level is needed to drive privacy research from a managerial perspective. This dissertation aims at providing such a basis by answering the following questions:

How can companies use their consumer data privacy protection approaches for strategic differentiation?

Which are the relevant dimensions of organisational privacy orientation and how do they contribute to a company's marketing performance?

To this end, the relevant research streams at the intersection of marketing and data privacy of the past twenty years are systematically analysed. Across six articles, a customer centric approach is used to define a conceptual framework of organisational privacy orientation. The first four articles explore privacy orientation as a construct and how it is currently understood in the market. The fifth article provides a thorough theoretical basis for the construct and provides first insights into its dimensionality. The last article reports a series of five studies detailing the definition, development and validation of a self-assessment scale for organisational privacy orientation. Taken together, the findings explain what organisational privacy orientation entails, how it is achieved and what its consequences are. The self-assessment scale can be used to measure the degree of a firm's current privacy orientation and to help formulate actionable strategies to increase it. Taken together, this dissertation's results provide marketing managers with the knowledge to deliver consistent, transparent privacy protection to their customers while still reaping the benefits from processing customer data.

Zusammenfassung

Diskussionen über Datenschutz standen im Schatten aller großen digitalen Innovationen der letzten zwanzig Jahre. Datenschutzbedenken von Konsument:Innen nehmen seit den Tagen des Webs 2.0 weltweit zu und als Reaktion darauf, wurden weltweit strengere Datenschutzgrundverordnungen erlassen. Infolgedessen sehen sich Unternehmen immer öfter mit der Frage konfrontiert, wie sie ihre Datenverarbeitungsaktivitäten besser auf die Datenschutzbedürfnisse ihrer Kundschaft abstimmen können. Das Marketing spielt bei der Beantwortung dieser Frage eine zentrale Rolle; sowohl als Treiber problematischer Datenverarbeitung als auch als eine potenzielle Lösung dafür. Obwohl es mehrere Marketingstudien gibt, welche sich mit der Psychologie und den wirtschaftlichen Aspekten des Datenschutzes befassen, fehlt es noch immer an einem vereinenden Ansatz für diese Forschungsrichtungen. Um die Datenschutzforschung aus einer Managementperspektive voranzutreiben, wird insbesondere eine Konzeptualisierung der Datenschutzorientierung auf Unternehmensebene benötigt. Diese Dissertation zielt darauf ab, eine solche Grundlage zu schaffen, indem sie die folgenden Fragen beantwortet:

Wie können Unternehmen ihre Ansätze zum Schutz von Kundendaten zur strategischen Differenzierung nutzen?

Welches sind die relevanten Dimensionen der organisationalen Datenschutzorientierung und wie tragen diese zur Marketingleistung eines Unternehmens bei?

Zu diesem Zweck werden die relevanten Forschungsströme an der Schnittstelle von Marketing und Datenschutz der letzten zwanzig Jahre systematisch analysiert. In sechs Artikeln wird ein kundenorientierter Ansatz verwendet, um einen konzeptionellen Rahmen für die Datenschutzorientierung von Unternehmen zu definieren. Die ersten vier Artikel befassen sich mit der Datenschutzorientierung als Konstrukt und mit der Frage, wie sie derzeit auf dem Markt verstanden wird. Der fünfte Artikel schafft eine theoretische Grundlage für das Konstrukt «Organisationale Datenschutzorientierung» und gibt erste Einblicke in seine Dimensionalität. Der letzte Artikel berichtet über eine Reihe von fünf Studien, welche die Definition, Entwicklung und Validierung einer Selbstbewertungsskala für die Datenschutzorientierung von Unternehmen beschreiben. Gemeinsam erklären die Ergebnisse, was organisationale Datenschutzorientierung bedeutet, wie sie erreicht wird und welche Konsequenzen für Unternehmen diese hat. Die Selbstbewertungsskala kann verwendet werden, um den Grad der aktuellen Datenschutzorientierung eines Unternehmens zu messen und um Strategien zur Verbesserung der Datenschutzorientierung zu formulieren. Insgesamt zeigen die Ergebnisse dieser Dissertation Marketingmanagern auf, wie sie ihrer Kundschaft einen konsistenten und transparenten Datenschutz bieten können, ohne auf die Vorteile der Verarbeitung von Kundendaten zu verzichten.

Table of Contents

<i>List of Figures</i>	vii
<i>List of Tables</i>	ix
Introduction.....	1
1. Article.....	14
Gotsch, M. (2020). Was hat das Marketing nach 2 Jahren DSGVO gelernt? <i>Swiss Marketing Review</i> , 6, 4-9. Translated from German to English by the author.	
2. Article.....	26
Gotsch, M. (2021). The individual and joint effects of data usage control & transparency on customers' privacy responses. <i>AMA Summer Academic Conference Poster Submission</i> , 1-7.	
3. Article.....	33
Friesenecker, M., Gotsch, M., Schögel, M. (2022). Knowing is Half the Battle – The Effect of SME Marketers' Privacy Literacy on Privacy Orientation. <i>Marketing Review St. Gallen</i> , 2, 36-43.	
4. Article.....	51
Gotsch, M. (2022). Customer Centricity & Datenschutz – Die Geschichte eines Missverständnisses. <i>Marketing Review St. Gallen</i> , 2, 12-19. Translated from German to English by the author.	
5. Article.....	66
Gotsch, M. & Schögel, M. (2021). Addressing the Privacy Paradox on the Organisational Level – Review and Future Directions. <i>Management Review Quarterly</i> , 1-34.	
6. Article.....	105
Gotsch, M. & Schögel, M. (n.d.). Organisational Privacy Orientation – Scale Development and Validation. <i>Journal of Business Research</i> , under review.	
Managerial Implications.....	141
<i>Appendix</i>	x

List of Figures

Please note: The first number indicates the article where the figure appears and the second the order of appearance within the article.

Introduction

Figure 0-1 The tension between consumer privacy and firm utilisation of data sources (Gotsch & Schögel, 2022).....	5
Figure 0-2 Overarching structure of the thesis (own illustration).....	7
Figure 0-3 Papers and publication status in overview (own illustration).....	9

1. Article

Figure 1-1 The seven core GDPR principles (own illustration).....	17
Figure 1-2 Paradigm shift (based on Matz et al., 2020).....	21
Figure 1-3 Strategic advantages through data privacy (based on Palmatier & Martin, 2019) ..	22

2. Article

Figure 2-1 Tukey's Post Hoc Test between groups. Likert-Scale from 1-7 used for all groups. Harmonic mean sample of 55.2 used. All values rounded to the 2nd decimal. Group differences shown in thick lines aren't statistically significant, all others are significant a $p < 0.05$ level. ...	31
Figure 2-2 Mediation model (Hayes Process Macro) with all values rounded to the 3rd decimal	31

3. Article

Figure 3-1 Hypotheses & research design	39
Figure 3-2 OPLIS knowledge levels (n=55).....	41
Figure 3-3 Website privacy orientation items (n=55).....	42
Figure 3-4 Privacy orientation of SME websites (n=55)	43
Figure 3-5 Correlations between model variables / * sign. at the 0.05 level (2-tailed) / ** sign. at the 0.01 level (2-tailed)	43
Figure 3-6 Model with standardised path coefficients / *sign. at the 0.01 level	44
Figure 3-7 Hypothesis and results in overview	45

4. Article

Figure 4-1 Customer-oriented and speculative data flows (adapted from Zuboff, 2019) 59

Figure 4-2 Customer-oriented view of data protection (based on Gotsch & Schögel, 2021) ... 61

5. Article

Figure 5-1 Guide to the four phases of a literature review (based on Okoli, 2015, p. 885) 73

Figure 5-2 Literature selection process..... 75

Figure 5-3 Data structure of the literature review (based on Gioia et al., 2013, p. 21)..... 78

Figure 5-4 Relationship between the aggregate dimensions 79

Figure 5-5 Connections between strategic initiative codes 82

Figure 5-6 Connections between structural improvement codes..... 85

Figure 5-7 Connections between HR management codes 87

Figure 5-8 Connections between service development codes 89

Figure 5-9 Categorisation of theories (adapted from Barth & de Jong, 2017, p. 1043) 90

Figure 5-10 Dynamic model for addressing the privacy paradox as a firm 91

6. Article

Figure 6-1 Study 5, CFA model and results for the OPO scale. Note: all coefficient values are standardised and appear next to the associated path (all values sig. at a $p < 0.001$ level)..... 124

Figure 6-2 Study 5, test of the nomological validity of the scale. Note: all path coefficients are standardised estimates. *** $p < 0.05$ / ** $p < 0.01$ / * $p < 0.001$ 125

List of Tables

Please note: The first number indicates the article where the figure appears and the second the order of appearance within the article.

6. Article

Table 6-1 Constructs related to organisational privacy orientation.	112
Table 6-2 Scale development process.....	116
Table 6-3 Organisational privacy orientation dimensions.....	118
Table 6-4 Study 4 – sample characteristics	121
Table 6-5 Study 5 - sample characteristics.....	122
Table 6-6 Study 5 scale items with descriptive statistics and factor loadings	124
Table 6-7 Study 5 - Discriminant validity tests.....	124
Table 6-8 Study 5, statistics for the paths of the nomological validity test.....	127

Introduction

In the 128th Stanford commencement speech on June 16th 2019, Apple's CEO Tim Cook addressed the tech giants of Silicon Valley and reprimanded them for their lax approach to the topic of privacy:

In a world without digital privacy, even if you have done nothing wrong other than think differently, you begin to censor yourself. Not entirely at first; just a little. Bit by bit. To risk less, to hope less, to imagine less, to dare less, to create less, to try less, to talk less, to think less. The chilling effect of digital surveillance is profound, and it touches everything. (Cook, 2019)

This attack on Apple's neighbours in the Silicon Valley was not unexpected. Just a week earlier, Apple unveiled its new privacy-focused advertising campaign at the Computer Electronics Show. With the slogan "What happens on your iPhone, stays on your iPhone", Apple reportedly did not just want to offer a sales argument, but rather to restate a company mission (Fazzini, 2019). In a news cycle dominated by "fake news", Chinese and Russian espionage and data abuse scandals, Apple's declaration of privacy was well-received. However, the question arose whether this promise would mark the beginning of a larger industry trend or if it was just an advertising slogan. Of the "four most influential companies in the world" (Galloway, 2017), Apple may have produced the fewest data protection scandals, but it still benefits from the loose handling of customer data. For example, Safari, the iPhone's standard browser, is set up to run all search queries through Google. A privilege for which Google is said to have paid over \$9 billion (Cao, 2018). In addition, numerous applications, which have both access to usage data and a questionable reputation in dealing with them (e.g., Facebook, FaceApp, TikTok, etc.), are still distributed via the Appstore (Akpan, 2019; Feldman, 2020; Fowler, 2020).

Relevance & Motivation

All this is not intended to call Apple's efforts to increase their customers' privacy into question, but rather to demonstrate that the issue of informational privacy is of high strategic and technological complexity. In particular, the example of mapping software shows the impotence of data protection policies such as Apple's. In a small experiment, Hill (2019) investigated what happens when the services of Silicon Valley's technology giants are blocked using a self-made VPN. When it came to Google's services, Hill discovered that many of their apps like Uber, Yelp or Lyft stopped working because they depended on the Google Maps API. Similar interactions can be observed with most modern digital platform systems: by design, these applications are linked and require a variety of customer data to function (Oxera, 2018).

Palmatier & Martin (2019, p. 87) point to this problem with their research; they conclude that the increased implementation of "big data technologies" (such as face recognition, voice recognition, geolocation, IoT, etc.) will escalate the vulnerability of consumers regarding data protection and privacy.

The countertrend to the escalation scenario proposed by Palmatier & Martin (2019, p. 87) manifests in the ratification of stricter data protection policies. In May 2018 the new General Data Protection Regulation (GDPR) of the European Union (EU) was ratified. Its seven basic principles are intended to address many of today's and tomorrow's privacy problems in a sustainable manner (EDöB, 2018, p. 2). Corresponding voices in the USA, which would support a nation-wide law reform, have been growing louder for years (Auxier et al., 2019; Cisco, 2019; Clemons et al., 2014; Lee Rainie & Duggan, 2015; Salesforce, 2019). In January 2020, the California Consumer Privacy Act (CCPA), intended to protect the privacy of its almost 40 million inhabitants, became effective. A strong political statement for the home state of the Silicon Valley (Worcester, 2019). Only a year later, the People's Republic of China introduced the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), heralding a "thorough reorganisation of the way through data is collected, stored, and managed" within all adjacent Asian countries (Creemers, 2022, p. 1).

This creates a tension between the increasingly data-driven (marketing) applications and privacy legislation. Yet, from a marketing point of view, the main question should be focused around where the customer stands on this issue. In the EU, there has been a slight trend in the average acceptance of the need to use personal data for certain services in recent years. Yet, the same report also shows customers do not like making such decisions in the first place (Ridley-Siebert, 2015). This is not a new finding - Acquisti (2004, p. 21) demonstrated in the early days of the Web 2.0 that customers, regardless of their level of knowledge, are both expressing concerns about privacy and still use data-intensive services (e.g., Social Media).

Research on this so-called "Privacy Paradox" (Barnes, 2006) has been published throughout the past decade – most of it declaring it either "a relic of the past" (Dienlin & Trepte, 2015, p. 295) or a "myth" (Solove, 2021, p. 51). Yet, the still ongoing debate on the paradox highlights the difficulty in trying to map customers' privacy behaviour in a general model. A systematic literature review by Barth & de Jong (2017) looked at 32 decision models trying to explain the "Privacy Paradox" and concluded that the depiction of rational decision-making behaviour is only practicable to a limited extent, seeing that several moderating variables influence customer behaviour. For this reason, the recommendation was made to tailor data-intensive services closer towards the customers' needs: "Creating privacy awareness in combination with tools that support users in their privacy decisions should help users to avoid paradoxical behaviour" (Barth & de Jong, 2017, p. 1051).

To date, little research has been conducted on what data privacy strategies on an organisational level should look like. Approaches such as more transparent communication (T. Kim et

al., 2019), incentive systems (Fuller, 2019) or increased control over shared data (Feng & Xie, 2019) have so far had mixed effects on customers. Most consumers are primarily concerned with the overall purpose of commercial data processing (Beke et al., 2018, p. 7). Therefore, single improvements to data processing without any strategic oversight cannot alleviate their privacy concerns. Martin & Murphy (2017) also support this conclusion in their literature review on privacy's role in marketing:

"Although a coherent subset of theoretic approaches has provided a robust understanding through deep insights, in some respects this focus has limited our view of privacy too much to individual silos such as consumers, organisations, ethics and law. (...) Future research directions should embody a holistic approach, blending the many consumer, organisational, ethical, and legal concerns that feature in contemporary data privacy questions. Since stakeholders are affected in multiple and potentially unforeseen ways, additional work in this important domain remains critical and needed" (p. 153).

In other words, there is a need in both research and marketing practice to understand data protection as a sustainable organisational strategy.

The Four Dimensions of the Research Question

In accordance with the recommendations of Martin & Murphy (2017, p. 153), Choi, Park & Jung (2018, p. 50), Acquisti, et al. (2017, p. 32) and Beke, Eggers & Verhoef (2018, p. 47) the overall research questions of this thesis are designed to both explore the intersection between marketing & privacy from an organisational-strategic point of view while still taking the customers' needs into account. Thus, the overarching research questions are formulated as:

RQ1 "How can companies use their consumer data privacy¹ protection approaches for strategic differentiation²?"

RQ2 "Which are the relevant dimensions of organisational privacy orientation³ and how do they contribute to a company's marketing performance⁴?"

The detailed meaning of the four aspects of data privacy, strategic differentiation, privacy orientation and their link to marketing performance are discussed in the following. The theoretical basis and the placement within research streams of these constructs is discussed within the studies featured in this dissertation.

Defining Privacy

Privacy has historically been a "notoriously hard to capture" concept (Koops et al., 2017, p. 487), as it has legal, psychological, philosophical and varying colloquial meanings (Parker,

1974, p. 276). As such, several distinctions between types of privacy can be drawn, e.g., between “privacy of communication” and “privacy of data and image” (Finn et al., 2013, p. 5). The term “information privacy” or “data privacy” is also often invoked in any context where “personal information is communicated to others” (Son & Kim, 2008, p. 503). While this term comes the closest to the topic of this dissertation, it still shows considerable overlap to other definitions. Hence, especially when discussing customer data, the need for an overarching definition of data privacy arises.

Martin & Murphy (2017, p. 136) propose a definition based on the work of Nissenbaum (2010), which encapsulates most aspects relevant to privacy from a marketer’s point of view: Privacy is the “claim to appropriate flows of personal information within distinctive social contexts”. The flow of information from the customer’s point of view can be deemed as appropriate, if they have control over how much they can be “sensed” (using any sense) by others (i.e., in this case, a company) (Parker, 1974, p. 273; Petronio, 2010, p. 179). What information or data constitutes “personal data” is defined in legal practice as any information relating to a “directly or indirectly identified or identifiable person” (GDPR, Art. 2-5 & Art. 26). As such, within this dissertation, the term “data privacy” is used interchangeably with “informational privacy”. Finally, because customers’ estimation when their personal privacy is being violated depends on the distinctive social context of this exchange (Parker, 1974, p. 279; Westin, 2003), it is included in this definition.

Current research strongly suggests, that while several measures to improve consumers’ data privacy are known to us, their effectiveness are highly dependent on external conditions (Dinev et al., 2012; James et al., 2015; Morlok, 2016; Plangger & Montecchi, 2020; Waters & Ackerman, 2011) as well as the “context and personality” of consumers (Bansal et al., 2016, p. 13). This is not surprising, considering the “interdisciplinary nature of privacy research” which needs to consider the individual, organisational and societal context of each research question (Ginosar & Ariel, 2017, p. 955).

In the broader literature, these different levels and their effects are generally viewed through the lens of the “Privacy Calculus” (Laufer & Wolfe, 1977; Martin & Murphy, 2017; Plangger & Montecchi, 2020, p. 32). The calculus tracks how a given variable affects the perceived benefits of data disclosure versus the perceived risk of said disclosure (Dinev et al., 2012; Dinev & Hart, 2006; Jiang et al., 2013; Pomfret et al., 2020; Xu et al., 2011). Yet, even when implementing privacy measures on a strategic level, their efficacy and effectiveness on the “Privacy Calculus” will be mediated by factors outside the company’s control (Martin & Murphy, 2017, p. 151). This is especially true when utilizing more complex behavioural privacy models, such as the “Antecedents–Privacy Concerns–Outcomes (APCO)” model, which also considers pre-existing biases or concerns (Dinev et al., 2015, p. 644). Therefore, this dissertation analyses data privacy exclusively from an organisational perspective, considering “that it is impossible to develop a one-size-fits-all conceptualisation of general privacy” (Smith et al., 2011).

Strategic Differentiation

Public discourse about privacy policy is most often framed dichotomously: either companies are forced to regulate by the state, which potentially harms the beneficial effects of information sharing (Bowie & Jamal, 2006), or they are left to self-regulate, which potentially creates large costs for consumers down the road (e.g., through data breaches) (Acquisti et al., 2016, p. 479; Martin et al., 2017a, p. 39; Solove, 2013, p. 1880).

Currently, the EU falls largely on the side of regulating firms' data processing (see e.g., DLA Piper, 2020). However, this still leaves most firms with a large possibility space to further protect or exploit their customers' privacy (Pomfret et al., 2020, p. 540) (see fig. 1).

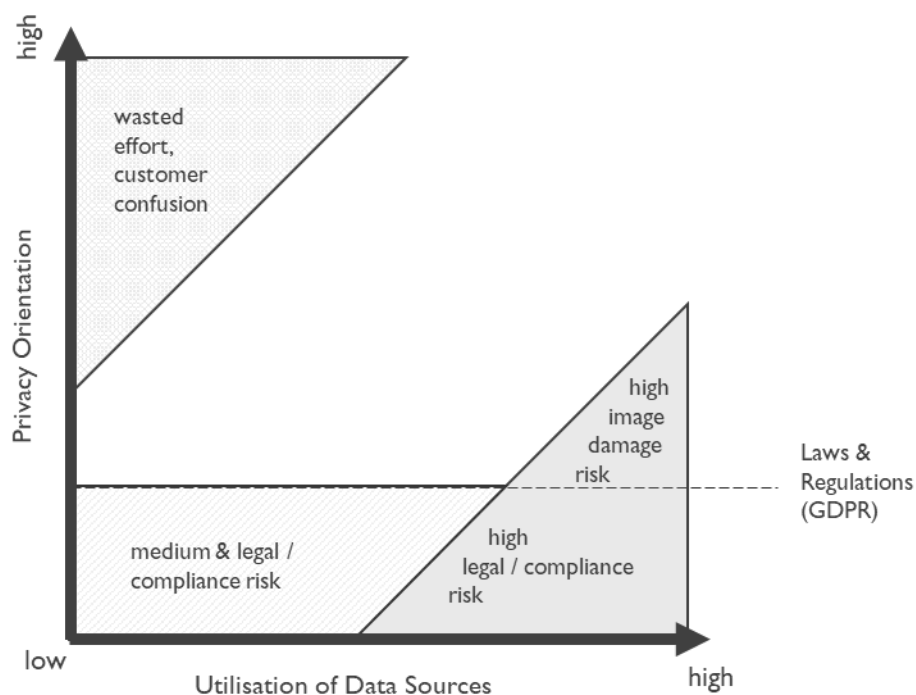


Figure 0-1 The tension between consumer privacy and firm utilisation of data sources (Gotsch & Schögel, 2022)

Because the benefits of processing customer data are apparent to most companies, the question arises, why they should consider voluntary self-regulations or even defining alternate revenue streams not based on the algorithmic targeting of consumers. Companies like to use a utilitarian framework when talking about privacy issues; postulating that it is a market exchange like any other. Like exchanging currency for goods, customers trade their data for targeted promotions or personalisation.

However, this reasoning is flawed, as it ignores that the former example is driven mainly by the customers' needs, while the latter "provides significantly more utility to marketers and advertisers (...) fostering an unbalanced exchanged relationship that may be seen as one-sided" (Rapp et al., 2009, p. 54). Even with equal benefits, the exchange would still favour companies. Due to the increasing complexity involved in understanding companies' privacy

policies, giving informed consent is difficult for most consumers (Milne et al., 2006). It has also been suggested that especially digital platform companies are purposefully exploiting this informational imbalance through their design to extract consent from consumers (Nouwens et al., 2020; Sanchez-Rola et al., 2019; Waldman, 2020). This does not negate the fact that companies can extract benefits from customer data which are useful to customers. However, it also hints at the existence of a strategic benefit derived from empowering customers to more effectively leveraging their personal data (Martin et al., 2017a).

Hence, for customer privacy to be considered by firms as more than just a compliance issue, a strategic focus on it must first produce such a competitive advantage. Meaning, it should give companies the capability to perform in one or many ways that competitors would find difficult to reproduce now and in the future (Kotler, 2000). However, to test which strategies contribute to privacy orientation and to track their effects, a conceptualisation of privacy orientation from an organisational perspective is needed.

Privacy Orientation

Greenaway, et al. (2015, p. 580) defined company privacy orientation as “The extent to which a firm delivers consistent, transparent privacy protection to its customers while achieving other important organisational objectives.” In their conceptualisation, they established privacy orientation as a three-dimensional construct which is distinguished by control over data streams, perceived procedural justice and legal obligations. As such, privacy orientation is understood as a means to navigate the tension between customers’ privacy demands and the data processing needs of a firm (Greenaway et al., 2015, p. 581).

However, by understanding privacy orientation largely in terms of legal risk mitigation, any potential upsides of treating privacy orientation as a strategic objective in its own right might be overlooked. Privacy is a high universal customer need (Lombardi & Ciceri, 2016), which is currently being underserved by data processing firms (see e.g., Cisco, 2019; Orange, 2019; Salesforce, 2019). This suggests a first-mover advantage for firms able to sustainably position themselves as privacy oriented (Martin & Murphy, 2017).

Similar to how the benefits of green marketing orientation are driven by a long-term investment in green products and an environmentally aware company culture (Fraj et al., 2011; Tariq et al., 2019), it is expected that organisational privacy orientation is driven by more than just a compliance strategy. Also analogous to green marketing efforts, it is expected that a consistent privacy orientation can be perceived by customers as a unique positioning when compared with companies merely partaking in privacy greenwashing (Szabo & Webster, 2021). Hence, a common conceptualisation of organisational privacy orientation would allow researchers to distinguish more effectively between a strategic commitment to privacy and deceptive privacy branding.

Privacy and Marketing Performance

The demand for marketing performance measurements grows in tandem with the ongoing digitalisation of company processes, (Katsikeas et al., 2016). Marketing performance itself is a challenging construct to operationalise. Previous studies have divided the various measurements for marketing performance into two rough categories: financial or non-financial (Rahman et al., 2017; Rust et al., 2004; Stewart, 2009). It is expected that successful marketing performance first drives operational performance (e.g., customer behaviour, product market performance, etc.) which, in turn, translates in organisational performance (e.g., accounting performance, financial market performance) in the long-term (Katsikeas et al., 2016).

Since the benefits of data processing affect both operational performance and organisational performance, it is expected that organisational privacy orientation might influence both. Past studies have illustrated that neglecting privacy has a negative impact on organisational performance (e.g., through negative spill over effects after data breaches) (Martin et al., 2017b). Unfortunately, most studies so far have only investigated very specific performance measurement outcomes, such as customer trust & satisfaction (Dehghanpouri et al., 2020; Eastlick et al., 2006; Featherman et al., 2010; Wu et al., 2012), when it comes to the effects of privacy measures. Additionally, all these studies used different tactical measures of privacy orientation and therefore lack comparability. Hence, this dissertation's goal is to create a unified understanding of organizational privacy orientation, which allows for a meaningful comparison between studies exploring the intersection between data privacy and marketing.

Thesis Outline

Considering that the intersection between marketing and privacy is still missing a cohesive overarching framework and treating customer privacy "as a focal domain for proactive marketing strategy is relatively new" (Palmatier & Martin, 2019, p. 180), the stated research questions are best answered in three consecutive steps (see fig. 2).



Figure 0-2 Overarching structure of the thesis (own illustration)

The goal of this thesis is to understand organisational privacy orientation and what effects this construct has or could have on marketing performance. Hence, the first step, and the subject

of the first three papers, is creating a better understanding of how privacy orientation is currently addressed in the market. Specifically, estimating the impact of the GDPR on European companies (Paper 1), testing how the transparency and control demanded by the GDPR affect customer perception (Paper 2) and what role marketing as a function plays in both (Paper 3).

The second step involved establishing a theoretical basis on which organisational privacy orientation as a construct could be built upon. The lens of “customer centricity” was used to unify the different perspectives on privacy into a cohesive set of actionable measures (Paper 4). In combination with previous literature on organisational privacy initiatives, a better understanding on the possible contexts and circumstances, in which privacy measures could successfully be employed, was developed.

Finally, the findings from all four papers were combined into a robust and valid conceptualisation of the privacy orientation construct (Paper 5 and 6). The construct and its corresponding self-assessment scale can be used to catalogue the strategic measures available to companies when orienting themselves towards privacy as well as observing the effects of said measures. Such an overview is not just necessary to explore the possibility space from a marketer’s point of view, but also to make privacy orientation measurable for experimental testing.

Apart from being able to aid in the assessment of privacy measures across different industries (e.g., through comparing effect sizes) the scale is also able to identify different dimensions along which companies can adjust their existing policies to gain competitive advantages through organisational privacy orientation.

Papers at a Glance

The first three papers explore specific facets of the intersection between marketing and data privacy. Paper 1 was written as a retrospective on the impact of the GDPR on commercial data processing and how marketers have and could have reacted to it. Paper 2 and Paper 3 quantitatively explore the impact of three major factors contributing to higher organisational privacy from a marketing point of view: customer control over data streams, transparent data processing and employee privacy literacy. Paper 4 creates the foundation for the concept of organisational privacy orientation and posits the customer centric thinking as its major component. Finally, Papers 5 and 6 conceptualise organisational privacy orientation, describe how it is built within organisations, how it can be measured and what impacts it has on a company.

	Explorative			Descriptive	Prescriptive	
Authors and Title	P1 Gotsch, 2020: What have marketers learned after two years of GDPR?	P2 Gotsch, 2021: The individual and joint effects of data usage control & transparency on customers' privacy responses	P3 Friesenecker, Gotsch & Schögel, 2022: Knowing is half the Battle - The Effect of Marketers' Privacy Literacy on SMEs' Privacy Orientation	P4 Gotsch, 2022: Customer Centricity & Data Privacy: A story of misunderstanding	P5 Gotsch & Schögel, 2021: Addressing the Privacy Paradox on the Organisational Level - Review and Future Directions	P6 Gotsch & Schögel, 2023: Organisational Privacy Orientation - Scale Development and Validation
Research Question	What strategies have companies used to reconcile their data processing activities with the GDPR?	How do data usage control and transparency in a corporate context affect situational trust and privacy behavior before and after a data breach?	How do data usage control and transparency in a corporate context affect situational trust and privacy behavior before and after a data breach?	How can customer centric data privacy be conceptualized? Is customer centricity beneficial to organizational privacy orientation?	How can companies address the privacy paradox to improve their customers' information privacy?	How can organizational privacy orientation be conceptualized?
Research Method	Conceptual, desk research	2x2 experimental survey, analysis of variance, mediation	Quantitative data collection, mediation modelling	Conceptual, desk research	Systematic literature review	Scale development across 5 studies
Publication Status	Swiss Marketing Review, 2020 (6). 4-9.	2021 AMA Summer Academic Conference, Poster Submission	Marketing Review St. Gallen, 2022 (2). 36-43.	Marketing Review St. Gallen, 2022 (2). 12-19.	Management Review Quarterly, 2021. 1-34.	Journal of Business Research, under review
Results	Literature overview, conceptual development and definition of research gap.	Demonstrating the limitations of tactical organizational privacy measures.	Identifying the marketing function as a vital influence on privacy orientation	Identifying the marketing function as a vital influence on privacy orientation	Framework establishing the dimensionality and processes behind privacy orientation	Measurement development for the organizational privacy orientation construct

Figure 0-3 Papers and publication status in overview (own illustration)

References

- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Pre-Proceedings to EC'04, May 17-20, New York*, 1–9.
- 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. (2017). 44 Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online ACM Reference Format. *ACM Computing Surveys*, 50(3), 1–41. <https://doi.org/10.1145/3054926>
- Acquisti, A., Taylor, C., Wagman, L., Boheme, R., Bonatti, A., Calo, R., Cooper, J., Goldfarb, A., Grossklags, J., Hoofnagle, C., Hui, K.-L., Jentzsch, N., Kim, J.-H., Malin, B., Nissenbaum, H., Odlyzko, A., Picker, R., Png, I., Preibusch, S., ... Acquisti, F. (2016). The Economics of Privacy †. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Akpan, N. (2019, July 24). *Is FaceApp a security risk? 3 privacy concerns you should take seriously* | PBS NewsHour. PBS News Hour. <https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously>
- Auxier, B. Y. B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and Privacy: Concerned, Confused, and Feeling a Lack of Control Over Their Personal Information. *Pew Research Center*, November, 1–63.
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management*, 53(1), 1–21. <https://doi.org/10.1016/j.im.2015.08.001>
- Barnes, S. B. (2006). A privacy paradox: Social Networking in the United States. *First Monday*, 11(9). <https://doi.org/https://doi.org/10.5210/fm.v11i9.1394>
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. In *Foundations and Trends in Marketing* (Vol. 11, Issue 1). <https://doi.org/10.1561/17000000057>
- Bowie, N. E., & Jamal, K. (2006). Privacy Rights on the Internet: Self-Regulation or Government Regulation? *Business Ethics Quarterly*, 16(3), 323–342. <https://doi.org/10.5840/beq200616340>
- Cao, P. (2018). Google reportedly paying Apple \$9 billion to remain default search engine in Safari on iOS - 9to5Mac. 9to5Mac. <https://9to5mac.com/2018/09/28/google-paying-apple-9-billion-default-search-engine/>
- 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>
- Cisco. (2019). *Consumer Privacy Survey - The growing imperative of getting data privacy right*. <https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf>
- Clemons, E. K., Wilson, J., & Jin, F. (2014). Investigations into Consumers Preferences Concerning Privacy: An Initial Step Towards the Development of Modern and Consistent Privacy Protections Around the Globe. In IEEE (Ed.), *47th Hawaii International Conference on System Science* (pp. 4083–4092). <https://doi.org/10.1109/HICSS.2014.504>
- Cook, T. (2019). *2019 Commencement address by Apple CEO Tim Cook* | Stanford News. Stanford News. <https://news.stanford.edu/2019/06/16/remarks-tim-cook-2019-stanford-commencement/>
- Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, 8(1), 1–12. <https://doi.org/10.1093/CYBSEC/TYAC011>
- Dehghanpouri, H., Soltani, Z., & Rostamzadeh, R. (2020). The impact of trust, privacy and quality of service on the success of E-CRM: the mediating role of customer satisfaction. *Journal of Business & Industrial Marketing*, 1–17. <https://doi.org/10.1108/JBIM-07-2019-0325>

- Dienlin, T., & Trepte, S. (2015). Putting the Social (Psychology) into Social Media: Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors. *European Journal of Social Psychology*, 45(3), 285–297. <https://doi.org/10.1002/ejsp.2038>
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Dinev, T., McConnell, A. R., Smith, H. J., & Jeff, H. (2015). Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4), 639–655. <https://doi.org/10.1287/isre.2015.0600>
- 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>
- DLA Piper. (2020). *DLA Piper GDPR Data Breach Survey: January 2020* (Issue January).
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. <https://doi.org/10.1016/j.jbusres.2006.02.006>
- EDöB. (2018). *Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz*. November, 1–11.
- Fazzini, K. (2019). *Apple’s big bet on privacy has risks*. CNBC. <https://www.cnbc.com/2019/01/10/apple-privacy-big-bet-risks.html>
- Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24(3), 219–229. <https://doi.org/10.1108/08876041011040622>
- Feldman, B. (2020, April). Why The Zoom App Isn’t Safe & Has a Lot of Security Problems. *New York Magazine*.
- Feng, Y., & Xie, Q. (2019). Privacy Concerns, Perceived Intrusiveness, and Privacy Controls: An Analysis of Virtual Try-On Apps. *Journal of Interactive Advertising*, 19(1), 43–57. <https://doi.org/10.1080/15252019.2018.1521317>
- Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. *European Data Protection: Coming of Age, January*, 3–32. https://doi.org/10.1007/978-94-007-5170-5_1
- Fowler, G. A. (2020, July 13). Should you delete TikTok? Here’s everything you need to weigh the real privacy risks - The Washington Post. *The Washington Post*.
- 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>
- Fuller, C. S. (2019). Is the market for digital privacy a failure? *Public Choice*, 180(3–4), 353–381. <https://doi.org/10.1007/s11127-019-00642-2>
- Galloway, S. (2017). *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google*. Random House Large Print.
- Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, 54(7), 948–957. <https://doi.org/10.1016/j.im.2017.02.004>
- Gotsch, M. L., & Schögel, M. (2022). Privacy as Strategy - Ein Framework für das kundenzentrierte Datenmanagement. *GfM Forschungsreihe*, 2(1), 1–15. <https://www.alexandria.unisg.ch/265983/>
- 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>
- Hill, K. (2019). *Life Without the Tech Giants*. Gizmodo. <https://gizmodo.com/life-without-the-tech-giants-1830258056>
- James, T. L., Nottingham, Q., Collignon, S. E., Warkentin, • Merrill, & Ziegelmayer, J. L. (2015). The interpersonal privacy identity (IPI): development of a privacy as control model. *Information Technology and Management*, 17, 341–360. <https://doi.org/10.1007/s10799-015-0246-0>
- 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>
- Katsikeas, C. S., Morgan, N. A., Leonidou, L. C., & Hult, G. T. M. (2016). Assessing performance outcomes in marketing. *Journal of Marketing*, 80(2), 1–20. https://doi.org/10.1509/JM.15.0287/ASSET/IM-AGES/LARGE/10.1509_JM.15.0287-FIG1.JPEG

- 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>
- Koops, B. J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. In *University of Pennsylvania Journal of International Law* (Vol. 38, Issue 2).
- Kotler, P. (2000). *Marketing Management Analysis* (5th ed.). Prentice Hall.
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a Social Issue and Behavioural Concept. *Journal of Social Issues*, 33(3), 22–41.
- Lee Rainie, B., & Duggan, M. (2015). Privacy and Information Sharing. In *Pew Research Center* (Vol. 14).
- Lombardi, D. B., & Ciceri, M. R. (2016). More than defense in daily experience of privacy: The functions of privacy in digital and physical environments. *Europe's Journal of Psychology*, 12(1), 115–136. <https://doi.org/10.5964/ejop.v12i1.948>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017a). 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., Borah, A., & Palmatier, R. W. (2017b). 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., & 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>
- Milne, G. R., Culnan, M. J., & Greene, H. (2006). A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy*, 25(2), 238–249.
- Morlok, T. (2016). Sharing is (not) caring - The role of external privacy in users' information disclosure behaviors on social network sites. *PACIS*, 75–92. <http://aisel.aisnet.org/pacis2016/75>
- Nissenbaum, H. (2010). Privacy in Context Technology, Policy, and the Integrity of Social Life. In *Privacy in Context*. Stanford University Press.
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Association for Computing Machinery (Ed.), *CHI* (pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376321>
- Orange. (2019). *L'Observatoire des usage du digital*.
- Oxera. (2018). *Market power in digital platforms*.
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Parker, R. B. (1974). A Definition of Privacy. *Rutgers Law Review*, 27(2), 275–297. <https://heinonline.org/HOL/Page?handle=hein.journals/rutlr27&id=283&div=23&collection=journals>
- Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, 2(3), 175–196. <https://doi.org/10.1111/j.1756-2589.2010.00052.x>
- Plangger, K., & Montecchi, M. (2020). Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, 50, 32–44. <https://doi.org/10.1016/j.intmar.2019.10.004>
- Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: socio-demographic and attitudinal influences on privacy and disclosure choices. *Journal of Marketing Management*, 36(5–6), 519–549. <https://doi.org/10.1080/0267257X.2020.1715465>
- Rahman, M., Rodríguez-Serrano, M. Á., & Lambkin, M. (2017). Corporate Social Responsibility And Marketing Performance. *Journal of Advertising Research*, 57(4), 368–378. <https://doi.org/10.2501/JAR-2017-047>
- Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). Advertising and Consumer Privacy: Old Practices and New Challenges. *Journal of Advertising*, 38(4), 51–61. <https://doi.org/10.2753/JOA0091-3367380404>
- Ridley-Siebert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice*, 17, 30–35. <https://doi.org/10.1057/dddmp.2015.40>
- Rust, R. T., Ambler, T., Carpenter, G. S., Kumar, V., & Srivastava, R. K. (2004). Measuring marketing productivity: Current knowledge and future directions. *Journal of Marketing*, 68(4), 76–89. https://doi.org/10.1509/JMKG.68.4.76.42721/ASSET/IMAGES/LARGE/10.1509_JMKG.68.4.76.42721-FIG1.JPEG
- Salesforce. (2019). *State of the connected customer*.

- Sanchez-Rola, I., Dell'amico, M., Kotzias, P., Eurecom, D. B., Bilge, L., Vervier, P.-A., Santos, I., & Balzarotti, D. (2019). Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. *AsiaCCS*, 12, 340–351. <https://doi.org/10.1145/3321705.3329806>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989–1015.
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, 89(1), 1–51.
- Son, B. J.-Y., & Kim, S. S. (2008). Internet User's Information Privacy-Protective Responses: A Taxonomy and Nomological Model. *MIS Quarterly*, 32(3), 503–529.
- Stewart, D. W. (2009). Marketing accountability: Linking marketing actions to financial results. *Journal of Business Research*, 62(6), 636–643. <https://doi.org/10.1016/J.JBUSRES.2008.02.005>
- Szabo, S., & Webster, J. (2021). Perceived Greenwashing: The Effects of Green Marketing on Environmental and Product Perceptions. *Journal of Business Ethics*, 171(4), 719–739. <https://doi.org/10.1007/S10551-020-04461-0/FIGURES/3>
- Tariq, A., Badir, Y., & Chonglertham, S. (2019). Green innovation and performance: moderation analyses from Thailand. *European Journal of Innovation Management*, 22(3), 446–467. <https://doi.org/10.1108/EJIM-07-2018-0148/FULL/PDF>
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the “privacy paradox.” *Current Opinion in Psychology*, 31(2), 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- Waters, S., & Ackerman, J. (2011). Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure. *Journal of Computer-Mediated Communication*, 17(1), 101–115. <https://doi.org/10.1111/j.1083-6101.2011.01559.x>
- Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431–453. <https://doi.org/10.1111/1540-4560.00072>
- Worcester, C. (2019). *The Impact of GDPR and CCPA on Digital Marketers*. AMA. <https://www.ama.org/2019/05/30/the-impact-of-gdpr-and-ccpa-on-digital-marketers/>
- 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>
- Xu, H., Luo, X. (Robert), Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52. <https://doi.org/10.1016/j.dss.2010.11.017>

I. Article

Gotsch, M. (2020). Was hat das Marketing nach 2 Jahren DSGVO gelernt? *Swiss Marketing Review*, 6, 4-9.

Translated from German to English by the author.

What have marketers learned after two years of GDPR?

Mauro Luis Gotsch, MA HSG

mauro.gotsch@unisg.ch / ORCID: 0000-0002-5319-2347

Institute of Marketing, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

Abstract

In May 2018, the European Union's General Data Protection Regulation (GDPR) was ratified. At the time, it was the most demanding and comprehensive data protection regulation for a market of this size. Companies around the world have since tried to adapt their internal policies to meet European customers' needs for more control over personal data streams. But how have marketers reacted to this change and what have companies learned about customer centrality in data privacy over the last few years?

Keywords: *privacy marketing, DSGVO, strategic marketing management, customer centrality*

Introduction

Since the European Parliament adopted the new “General Data Protection Regulation on the protection of individuals regarding the processing of personal data” (GDPR) in April 2016, management magazines have speculated what the end of the Wild West of data collection would mean for marketers (Murphy & Field, 2018). GDPR, which is based on the concept of data privacy as a fundamental human right, was predicted to “dramatically affect the way data is collected” worldwide (Downes, 2018). On the one hand, because its protection should extend to all citizens in the European Union (EU), no matter where their data is processed. On the other hand, the seven GDPR core principles presented in Figure 1 should make it impossible to collect data automatically without explicit customer consent.



Figure 1-1 The seven core GDPR principles (own illustration)

Despite the potentially costly consequences for unprepared companies, many industry experts referred to the GDPR as “good news for marketers” (Gilbert, 2017). For example, Goddard (2017, p. 705) stated that the newfound transparency in data processing would put companies on an equal footing with their customer base and thus foster sustainable trust. Seo et al. (2018) further speculated that gained insights from optimised data processing would lead to more secure data management overall.

Since then, over 160,000 data breaches have been reported to the EU Data Protection Supervisor. Moreover, surveys have repeatedly shown that consumers do not feel any safer about their data privacy than they did before the ratification of the GDPR (see e.g., Insight Intelligence, 2020; Orange, 2019; SUSE, 2019). Of course, part of this uneasiness among customers can be explained by the media hype surrounding the legal changes and, more recently, the public discourse on tracking technology that emerged during the COVID-19 pandemic. However, given the exponential rise in customer data collection (Reinsel et al., 2018), it seems more likely that customers will continue to be concerned about data protection for the foreseeable future.

This trend has long been apparent: in several pre-pandemic consumer surveys, 72% of participants said they would “stop shopping with a company because of privacy concerns” (Cisco, 2019, p. 4; Salesforce, 2019, p. 21).

As one of the biggest beneficiaries of data processing, marketers increasingly have had to ask themselves the following: How can we meet our customers’ growing concern for data privacy? What does a sustainable data processing strategy look like? And what have we learned about data privacy in recent years since the introduction of the GDPR?

How GDPR sheds light on a longstanding marketing problem

Long before GDPR, data privacy legislators and researchers alike called for the private sector to pay more attention to the privacy needs of their customers. Wang and colleagues (1998) warned of the erosion of customer privacy through “internet marketing” (p. 70) almost 25 years ago. The authors argued that marketers in particular were in a good position to collect and implement customers’ legal and operational privacy requirements across the organisation. With the proliferation of the first social networks, these recommendations were given added emphasis. For example, Sarathy et al. (2003) noted that “firms will need to pay continuous attention to privacy issues if consumer goodwill and successful marketing are to be achieved” (p. 124).

These recommendations were then—as they are now—based on two trends: the increasing need among consumers globally (see e.g., Clemons et al., 2014) for sustainable data privacy (Goldfarb & Tucker, 2012), and the escalated vulnerability of consumers’ privacy to digital (marketing) technologies (Palmatier & Martin, 2019).

Prior research showed that consumers often feel their online privacy is being violated, but at the same time they do not know how to effectively fend off such privacy violations (Lombardi & Ciceri, 2016). This is not a new finding. Acquisti (2004, p. 21) has already shown in the early days of the Web 2.0 that customers—regardless of their level of knowledge—express privacy concerns while still using data-intensive services (e.g., social media). Since then, the study of this so-called “Privacy Paradox” (Barnes, 2006) has developed into its own branch of research, but with inconsistent results. A literature review by Barth and de Jong (2017) examined 32 decision models from studies on the Privacy Paradox and concluded that the definition of a general decision-making process has only limited viability, as too many variables influence consumer behaviour.

One of the most frequently cited explanations for consumers’ “paradoxical” behaviour is the one-sided power relationship of sharing personal data (Martin & Murphy, 2017). Companies often falsely claim that this is a market exchange like any other: Customers exchange data for personalised services. However, this assumes the exchange has been initiated by consumers

and is based on an equitable balance of power. Yet, since data points are worth almost nothing individually, customers lack the bargaining chips to establish a fair trade. The value of personal data comes from its aggregation and subsequent processing. The power imbalance is further reinforced by the fact that a seller of such data can ignore potential costs resulting from the sale. However, any person whose data is being sold may face hidden costs (e.g., by sensitive data being published) (Varian, 1996). As a result, customers often engage in data exchanges that “[provide] significantly more utility to marketers and advertisers” and foster such an “unbalanced exchange relationship that may be seen as one-sided” (Rapp et al., 2009, p. 58).

But even with equally distributed benefits, consumers are at a disadvantage: the legal terms of data sharing agreements are usually too opaque. Both privacy policies and collection methods are increasingly complex to understand (Milne et al., 2006; Milne & Boza, 1999; Slepchuk & Milne, 2020). Additionally, many digital platforms intentionally exploit this information imbalance through their design to gain consumer consent more easily (Nouwens et al., 2020).

Nevertheless, customers may still be willing to pay for services with personal data. In the EU, even before the implementation of GDPR, there was a small yet significant trend towards acceptance of sharing personal data in exchange for tangible consumer benefits. However, the same study also showed that customers did not like to make such decisions, as it was perceived that companies alone determine the terms of said exchange (Ridley-Siebert, 2015).

The direct impact of GDPR

The GDPR’s implications quickly became apparent to companies worldwide: If they indeed wanted to continue doing business with EU citizens, they would quickly need to understand and adhere to EU data processing law. Accordingly, the immediate impact for companies was mainly monetary through legal fees and process restructuring. Online companies with free-mium models that relied on reselling customer data had to rethink their business model. Offline companies that rarely focused on maintaining their databases suddenly found themselves forced to take drastic steps. For example, the pub restaurant chain Wetherspoons determined it to be more efficient to delete its entire customer email database than to separate data obtained under consent from legacy data recorded pre-GDPR (Manthorpe, 2017). For Fortune 500 companies, it was estimated that on average of 16 million USD has been spent on company-wide GDPR compliance projects (Smith, 2018). Teixeira and colleagues (2020) determined that the most common issue of such compliance projects was harmonising data processing across multiple sales and communication channels. Many companies reported a lack of access to technical and EU-specific legal knowledge. Shastri and colleagues (2019) argued this was due to GDPR being fundamentally incompatible with previous data architectures. Accordingly, adaptations would have to be implemented from the ground up and company-

wide. Anything else “would amount to fixing a leaky faucet in a sinking ship” (Shastri et al., 2019, p. 1).

These difficulties were also reflected in privacy statements around the globe. One survey (Linden et al., 2020, p. 62) of 6,278 companies within and outside of the EU found that while virtually all companies surveyed had changed their privacy statements, the benefits for consumers were scant. On average, the authors found improvements in transparency and specificity of the declarations could be observed (especially within the EU), but many declarations failed to achieve the full disclosure and transparency required by the GDPR.

At the same time, the notification requirement of the GDPR demonstrated that updating data privacy practices was necessary for many companies. Before the pandemic, the daily average number of data leaks reported in the EU was 278, an increase of 12.6% when compared to the previous year (DLA Piper, 2020, p. 4). Despite this, the EU’s Data Protection Commissioner remained reluctant to prosecute breaches to the extent that the law intended. The 50 million EUR fine imposed on Alphabet (previously known as Google) in 2019 accounted for 89.X% of total fines in the first year of the GDPR, a far cry from the maximum possible fine of 3.7 billion EUR (i.e., 4.0% of Alphabet’s global revenue) (Herrle & Hirsh, 2019).

However, this could change in the foreseeable future: As soon as models for automatic and objective verification of GDPR compliance find wider use, there will be more instances that can reliably detect data protection breaches (Torre et al., 2019). As legislators become more familiar with these rules, stricter sanctions for breaches are to be expected (Vinocur, 2019).

What does this mean for the future of marketing?

Despite the impact of the GDPR to-date, the situation for consumers may not improve in the long-term. Palmatier and Martin (2019, p. 84) suggested the increased use of Big Data (e.g., facial recognition, voice recognition, Internet of Things) will further escalate consumers’ privacy vulnerability—whether data processing is consent-based or not. These recent advances in technology show high potential for use in marketing but rely on a foundation of consumer trust. Accordingly, by building the necessary infrastructure for privacy-oriented strategies (e.g., anonymisation processes, data-minimising analytics, effective privacy training), companies could gain a crucial strategic advantage in their market (Li et al., 2019; Seo et al., 2018).

Nevertheless, the attested potential of data privacy as a strategic option in its own right has rarely been transferred into practice. This is the case despite initial findings pointing to the significant benefits of a privacy-oriented marketing strategy. A stronger focus on customers’ digital privacy has previously been associated with higher trust and customer satisfaction (Dehghanpouri et al., 2020; Eastlick et al., 2006; Featherman et al., 2010; Wu et al., 2012), greater

willingness to share data (Dinev & Hart, 2006; Hui et al., 2007; Morlok, 2016), data leak mitigation (Malhotra & Malhotra, 2011), and corporate economic performance (Martin et al., 2017).

If companies wish to secure these strategic advantages, a shift in company culture is a prerequisite. As many GDPR restructuring projects have shown, it is not enough to focus solely on minimum compliance with the law. Marketers should learn not to view data protection through a legal lens, as this view “cannot achieve the goals demanded of it” (Solove, 2013, p. 1903). Instead, marketers should build on the foundation that GDPR has laid and actively help customers “navigate an otherwise very uneven playing field” (Acquisti & Varian, 2005, p. 503). This requires a shift from asking, “Who collects what data?” to asking, “How is that data used?” (Matz et al., 2020, p. 116).

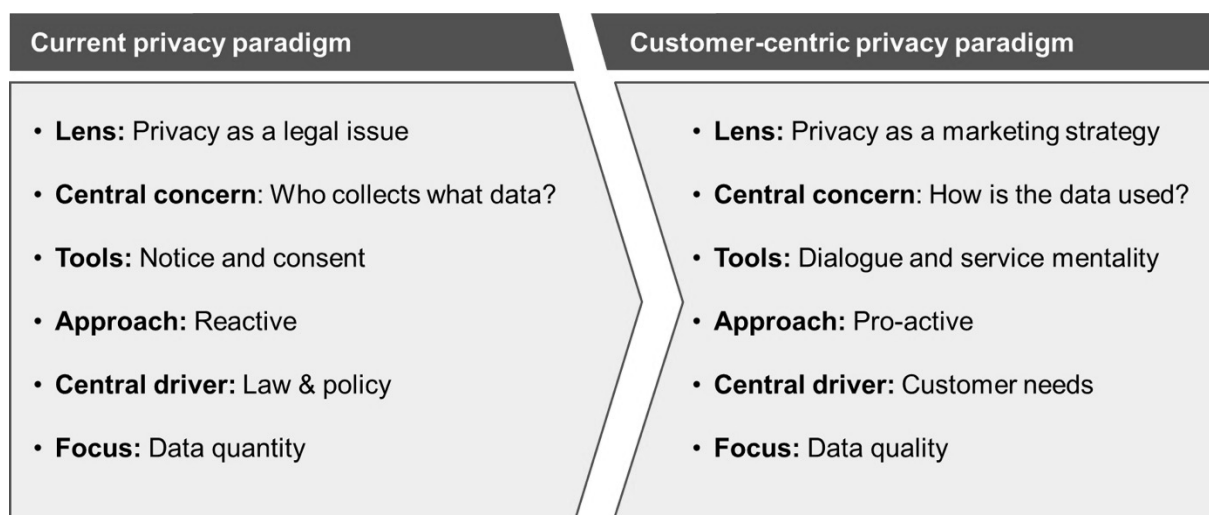


Figure 1-2 Paradigm shift (based on Matz et al., 2020)

At first, the changes under GDPR were mainly communicated to customers through numerous informational emails, laying out how company privacy policies would be adjusted. Since then, marketers have not noticeably improved at selling the value of their data processing practices to customers. The herein discussed Privacy Paradox will persist as long as customers feel that companies are not accommodating their stance on data privacy.

The GDPR remains an opportunity for marketers to create sustainable privacy awareness within their own companies. Today, marketers have the tools at their disposal to support customers in the customer journey with adequate data privacy decisions. Old ideas, such as consent-based dialogue marketing (Gerdes & Hesse, 2013), not buying and selling data, or empowering the customer (e.g., through increased transparency, more control, or easier opt-out) can help customers “overcome their paradoxical behaviour” (Barth et al., 2019, p. 65).

There are many philosophical, legal, technological, and ethical reasons for promoting data privacy. But from a marketing perspective, the goal is to “first satisfy the customer” (Gunther, 2009, p. 19) and to engage them in an equitable dialogue on data privacy. Not because it is required by the GDPR, but because it is an essential part of the customer experience for many companies.

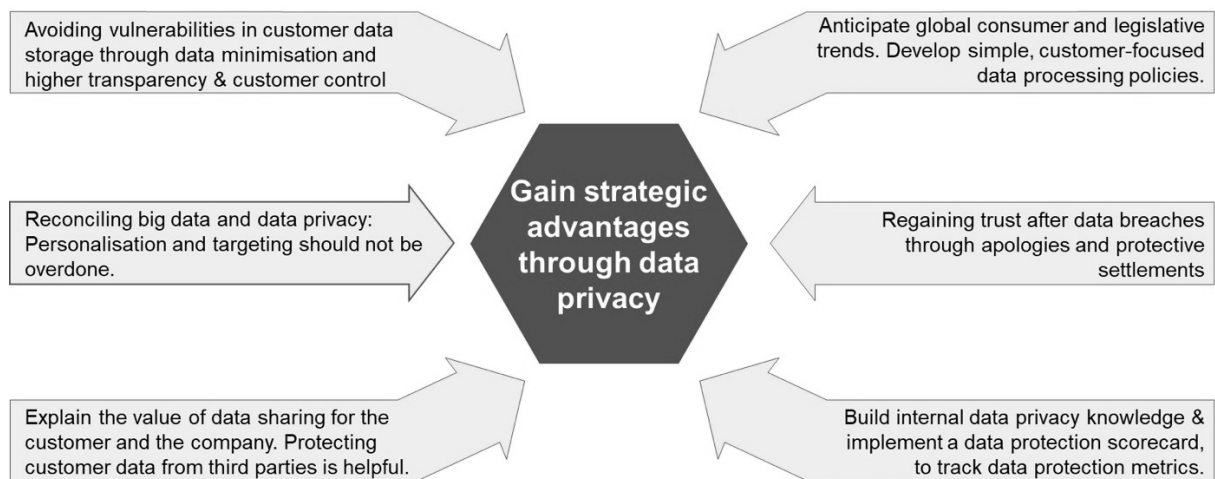


Figure 1-3 Strategic advantages through data privacy (based on Palmatier & Martin, 2019)

References

- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Pre-Proceedings to EC'04, May 17-20, New York*, 1–9.
- Acquisti, A., & Varian, H. R. (2005). Conditioning Prices on Purchase History. *Marketing Science*, 24(3), 367–381. <https://doi.org/10.1287/mksc.1040.0103>
- Barnes, S. B. (2006). A privacy paradox: Social Networking in the United States. *First Monday*, 11(9). <https://doi.org/https://doi.org/10.5210/fm.v11i9.1394>
- Barth, S., & de Jong, M. D. T. (2017). The Privacy Paradox - Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior - A Systematic Literature Review. *Telematics and Informatics*, 34, 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55–69. <https://doi.org/10.1016/j.tele.2019.03.003>
- Cisco. (2019). *Consumer Privacy Survey - The growing imperative of getting data privacy right*. <https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf>
- Clemons, E. K., Wilson, J., & Jin, F. (2014). Investigations into Consumers Preferences Concerning Privacy: An Initial Step Towards the Development of Modern and Consistent Privacy Protections Around the Globe. In IEEE (Ed.), *47th Hawaii International Conference on System Science* (pp. 4083–4092). <https://doi.org/10.1109/HICSS.2014.504>
- Dehghanpouri, H., Soltani, Z., & Rostamzadeh, R. (2020). The impact of trust, privacy and quality of service on the success of E-CRM: the mediating role of customer satisfaction. *Journal of Business & Industrial Marketing*, 1–17. <https://doi.org/10.1108/JBIM-07-2019-0325>
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- DLA Piper. (2020). *DLA Piper GDPR Data Breach Survey: January 2020* (Issue January). <https://www.dlapiper.com/en/netherlands/insights/publications/2019/01/gdpr-data-breach-survey/%0Ahttps://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>
- Downes, L. (2018). GDPR and the End of the Internet's Grand Bargain. *Harvard Business Review*. <https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain>
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. <https://doi.org/10.1016/j.jbusres.2006.02.006>
- Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24(3), 219–229. <https://doi.org/10.1108/08876041011040622>
- Gerdes, J., & Hesse, J. (2013). *Dialogmarketing im Dialog*. Gabler. <https://doi.org/10.1007/978-3-658-02000-2>
- Gilbert, D. (2017, September 4). Why GDPR is great news for marketers and will create a more efficient data economy – Econsultancy. *Econsultancy*. <https://econsultancy.com/why-gdpr-is-great-news-for-marketers-and-will-create-a-more-efficient-data-economy/>
- Goddard, M. (2017). Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–706. <https://doi.org/10.2501/IJMR-2017-050>
- Goldfarb, A., & Tucker, C. (2012). Shifts in Privacy Concerns. *The American Economic Review: Papers & Proceedings*, 102(3), 349–353. <https://doi.org/10.1257/aer>
- Gunther, R. E. (2009). Peter Drucker-the grandfather of marketing: an interview with Dr. Philip Kotler. *Journal of the Academy of Marketing Science*, 37, 17–19. <https://doi.org/10.1007/s11747-008-0105-1>
- Herrle, J., & Hirsh, J. (2019). The Peril and Potential of the GDPR. *Center for International Governance Innovation*, 1–4. https://www.cigionline.org/articles/peril-and-potential-gdpr?gclid=CjwKCAjwusrtrBRBmEi-wAGBPgE3kVYBBY06B_MCO2nR74oylikeYrQXaq79C6feEQZWhd4NmUwDbrnxoCaJYQAvD_BwETHE

- Hui, K., Teo, H. H., & Lee, S.-Y. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31(1), 19–33.
- Insight Intelligence. (2020). *Delade Meningar - Svenska folkets attityder till digital integritet 2020*.
- Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1), 1–6. <https://doi.org/10.1080/1097198X.2019.1569186>
- Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, 1, 47–64. <https://doi.org/10.2478/popets-2020-0004>
- Lombardi, D. B., & Ciceri, M. R. (2016). More than defense in daily experience of privacy: The functions of privacy in digital and physical environments. *Europe's Journal of Psychology*, 12(1), 115–136. <https://doi.org/10.5964/ejop.v12i1.948>
- Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 14(1), 44–59. <https://doi.org/10.1177/1094670510383409>
- Manthorpe, R. (2017). Wetherspoons just deleted its entire customer email database – on purpose | WIRED UK. *Wired*. <https://www.wired.co.uk/article/wetherspoons-email-database-gdpr>
- 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., & 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>
- Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current Opinion in Psychology*, 31(2), 116–121. <https://doi.org/10.1016/j.copsyc.2019.08.010>
- Milne, G. R., & Boza, M. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 13(1), 5–24. [https://doi.org/10.1002/\(SICI\)1520-6653\(199924\)13:1<5::AID-DIR2>3.0.CO;2-9](https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9)
- Milne, G. R., Culnan, M. J., & Greene, H. (2006). A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy*, 25(2), 238–249.
- Morlok, T. (2016). Sharing is (not) caring - The role of external privacy in users' information disclosure behaviors on social network sites. *PACIS*, 75–92. <http://aisel.aisnet.org/pacis2016/75>
- Murphy, M., & Field, M. (2018, May 19). GDPR: After the Wild West rush for data, a law for the digital age. *The Telegraph*. <https://www.telegraph.co.uk/technology/2018/05/19/gdpr-wild-west-rush-data-law-digital-age/>
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Association for Computing Machinery (Ed.), *CHI* (pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376321>
- Orange. (2019). *L'Observatoire des usage du digital*.
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). Advertising and Consumer Privacy: Old Practices and New Challenges. *Journal of Advertising*, 38(4), 51–61. <https://doi.org/10.2753/JOA0091-3367380404>
- Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World - From Edge to Core*.
- Ridley-Siebert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice*, 17, 30–35. <https://doi.org/10.1057/dddmp.2015.40>
- Salesforce. (2019). *State of the connected customer*.
- Sarathy, R., & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics* 2003 46:2, 46(2), 111–126. <https://doi.org/10.1023/A:1025001627419>
- Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An Analysis of Economic Impact on IoT Industry under GDPR. *Mobile Information Systems*, 1–6. <https://doi.org/10.1155/2018/6792028>
- 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.
- Slepchuk, A. N., & Milne, G. R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, 31, 89–93. <https://doi.org/10.1016/j.copsyc.2019.08.007>

- Smith, O. (2018). The GDPR Racket: Who's Making Money From This \$9bn Business Shakedown. *Forbes Magazine*. <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#1e282f334a22>
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- SUSE. (2019, June 4). 84 Prozent der Teilnehmer in Deutschland halten EU-DSGVO nicht für eine Verbesserung - SUSE Communities. SUSE Newsroom. <https://www.suse.com/c/de/news/suse-umfrage-84-prozent-der-teilnehmer-in-deutschland-halten-eu-dsgvo-nicht-fuer-eine-verbesserung/>
- Teixeira, G. A., da Silva, M. M., & Pereira, R. (2020). The Critical Success Factors of GDPR Implementation : a Systematic Literature Review. *Digital Policy, Regulation and Governance*, 21(4), 402–418. <https://doi.org/https://dx.doi.org/10.1108/DPRG-01-2019-0007>
- Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using Models to Enable Compliance Checking against the GDPR: An Experience Report. *Proceedings - 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems, MODELS 2019*, 1–11. <https://doi.org/10.1109/MODELS.2019.00-20>
- Varian, H. R. (1996). Economic Aspects of Personal Privacy. In W. H. Lehr & L. M. Pupillo (Eds.), *Cyber Policy and Economics in an Internet Age* (1st ed., Vol. 43, pp. 127–137). Springer. https://doi.org/https://doi.org/10.1007/978-1-4757-3575-8_9
- Vinocur, N. (2019, December 27). 'We have a huge problem': European tech regulator despairs over lack of enforcement - POLITICO. *Politico News*. <https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605>
- 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>
- 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>

2. Article

Gotsch, M. (2021). The individual and joint effects of data usage control & transparency on customers' privacy responses. *AMA Summer Academic Conference Poster Submission*, 1-7.

The individual and joint effects of data usage control & transparency on customers' privacy responses

Mauro Luis Gotsch, MA HSG

mauro.gotsch@unisg.ch / ORCID: 0000-0002-5319-2347

Institute of Marketing, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

Abstract

New (marketing) technologies drive an exponential increase in globally collected data (Reinsel et al., 2018, p. 3), a trend which is expected to further “escalate” customers vulnerability (Palmatier & Martin, 2019, p. 87) in the coming years (see fig. 5). If unchecked, it is feared the trend may permanently erode consumers’ ability “to take make meaningful action” (Fast & Jago, 2020, p. 44) to protect their privacy. Together with the increasing number of yearly data breaches across industries (DLA Piper, 2020, p. 4), the question on how to prevent and recover from corporate privacy failures grows in importance.

Previous literature has proposed firms should increase their customers’ data usage control and transparency to both reduce customers’ risk exposure and allow them to make more informed choices (Acquisti et al., 2013; Beke et al., 2018; Martin et al., 2017). While control and transparency have been shown to mediate negative customer reactions after a privacy failure (Martin et al., 2017), it is not clear what their individual effect is on the initial evaluation of a company as well as their individual importance for recovery after a corporate privacy failure.

This paper expands on existing privacy literature by juxtaposing the effects of data usage control and transparency individually, demonstrating that data usage transparency even without increased control has a more central role in trust recovery than previously reported.

The results have several implications for corporate data collection processes, first and foremost on the efficiency and effectiveness of engaging customers in a transparent privacy dialogue.

Keywords: *Privacy Marketing, Customer Behaviour, Data Leak, Trust Generation*

Acknowledgements

Thanks to Stefan Tour for helping me with the data collection and for the interesting discussions about the research design featured within this study.

Key Contributions in Overview

Research Questions

Palmatier & Martin (2019, p. 102) cite data usage transparency and control as the central instruments at a company's disposal to "empower" their customers and reduce their vulnerability to privacy failures. Although their effectiveness as mediators between privacy failures and customer behavior has been demonstrated (Ayaburi & Treku, 2020; Bansal & Zahedi, 2015; Martin et al., 2017), it is still unclear on how they directly affect customer behavior. Hence, this paper aims at answering two questions:

- RQ1: How do data usage control and transparency in a corporate context affect situational trust and privacy behavior before and after a data breach?
- RQ2: Is the joint effect of data usage control and transparency significantly higher than their individual effectiveness?

Method

In a 2x2 experimental survey with 221 participants it was tested whether differing levels of data usage control and transparency would change participants' perceived trust and protective behavior before and after a data breach scenario was introduced to them. The independent variables of data usage control and transparency were operationalised using four fictional privacy policies, with the levels for each of the variables (high & low) being manipulated according to the criteria for evaluating privacy policies detailed by Martin et al. (2017) and Dinev, et al. (2012). Based on the privacy policy, trust before breach (adapted from Chen & Jai, 2019) and perceived control and transparency (adapted from Dinev et al., 2012, p. 313; Martin et al., 2017, p. 54) was measured across all groups. All participants were then presented with a fictional data breach scenario, which was adapted from three real data breach cases (eBay Inc., 2014; Equifax, 2017; Target Corporation, 2013). Finally, their trust and switching intention to competing firms were measured using the proposed scale by Martin, et al (2017, p. 54).

Results

It was found that both trust before and after the breach were significantly higher by the group with high transparency and control (group 1, n=56). At the same time, switching intention was significantly lower in group 1 when compared to the group with both low transparency and

control (group 4, n=57). Additionally, the experiment showed that the group with low transparency, but high control (group 2, n=55) was less trusting and more likely to engage in protective behavior after the breach in comparison with the group which offered high transparency and low control (group 3, n=53). Hence, while customers clearly profit from the joint effect of transparency and control, they evaluate them individually and differently. This hints at the higher importance of a transparent privacy dialogue between customers and firms being a central driver of behavioral outcomes.

Finally, since the levels of trust before breach were significantly different between all the groups, we tested whether it was a mediator between the IVs and behavioral outcomes. Using the PROCESS Macro by Hayes (2017), we found the effect of the IVs on trust after the breach and behavioral outcomes to be significantly mediated by the trust before the breach (see fig. 2).

Conclusion

The results affirm the hypothesised positive effect of data usage transparency and control on customers privacy evaluation and behavior. Additionally, through the direct manipulation of the IVs, it was shown that high transparency is more effective at fostering trust in customers when compared to high control alone. Hence, for companies to build trust regarding their data collection processes, engaging the customer in a transparent privacy dialogue can be seen both as a prerequisite to build trust and to protect the company from the negative fallout of a potential privacy failure.

In a next step, we'd like to repeat the study as a field experiment, to see if the effectiveness of transparency and control is as context sensitive as privacy concerns in general are (Bansal et al., 2016).

Images

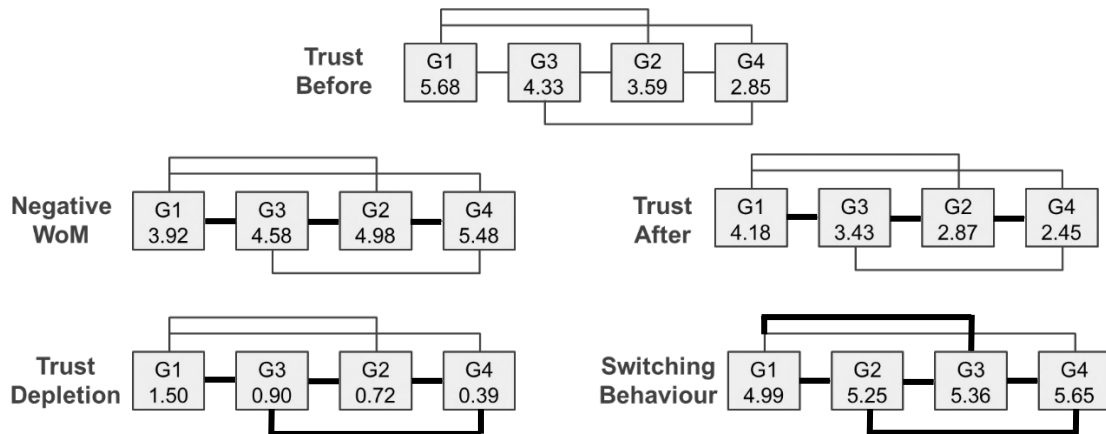


Figure 2-1 Tukey's Post Hoc Test between groups. Likert-Scale from 1-7 used for all groups. Harmonic mean sample of 55.2 used. All values rounded to the 2nd decimal. Group differences shown in thick lines aren't statistically significant, all others are significant at a $p < 0.05$ level.

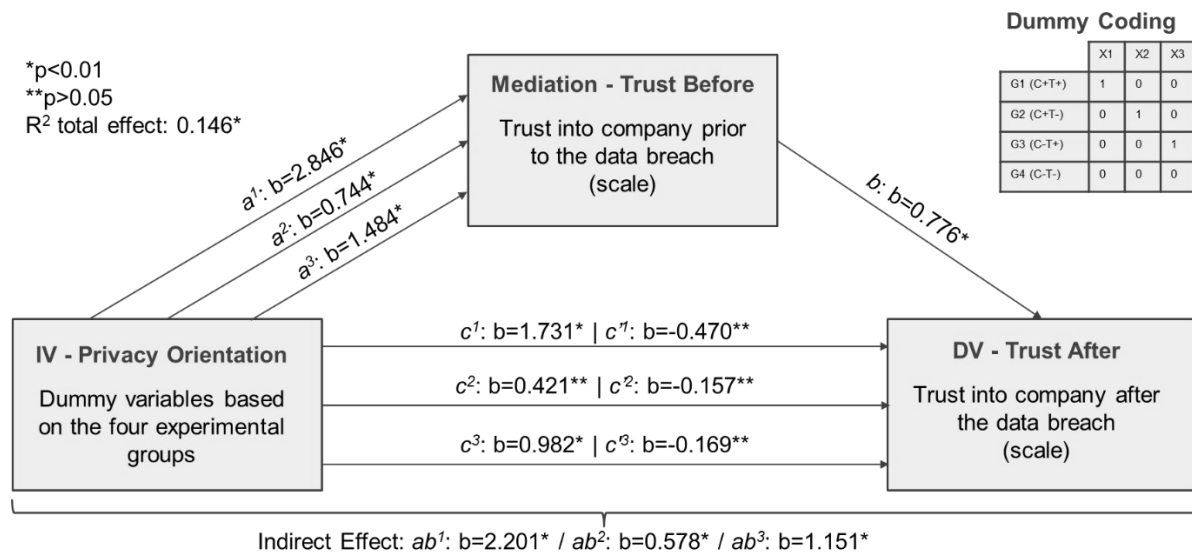


Figure 2-2 Mediation model (Hayes Process Macro) with all values rounded to the 3rd decimal

References

- Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15 seconds: The limits of privacy transparency and control. *IEEE Security and Privacy*, 11(4), 72–74. <https://doi.org/10.1109/MSP.2013.86>
- Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 50, 171–181. <https://doi.org/10.1016/j.ijinfo-mgt.2019.05.014>
- Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 71, 62–77. <https://doi.org/10.1016/j.dss.2015.01.009>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management*, 53(1), 1–21. <https://doi.org/10.1016/j.im.2015.08.001>
- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. In *Foundations and Trends in Marketing* (Vol. 11, Issue 1). <https://doi.org/10.1561/17000000057>
- Chen, H. S., & Jai, T.-M. (Catherine). (2019). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal*, 1–17. <https://doi.org/10.1080/02642069.2019.1603296>
- 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>
- DLA Piper. (2020). *DLA Piper GDPR Data Breach Survey: January 2020* (Issue January).
- eBay Inc. (2014, May 21). *eBay Inc. To Ask eBay Users To Change Passwords*. Ebay. <https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords/>
- Equifax. (2017, September 7). *Equifax Announces Cybersecurity Incident Involving Consumer Information* | Equifax. Equifax Website. <https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628>
- Fast, N. J., & Jago, A. S. (2020). Privacy matters... or does It? Algorithms, rationalization, and the erosion of concern for privacy. *Current Opinion in Psychology*, 31(2), 44–48. <https://doi.org/10.1016/j.copsyc.2019.07.011>
- Hayes, A. F., Montoya, A. K., & Rockwood, N. J. (2017). The analysis of mechanisms and their contingencies: PROCESS versus structural equation modeling. In *Australasian Marketing Journal* (Vol. 25, Issue 1, pp. 76–81). Elsevier Australia. <https://doi.org/10.1016/j.ausmj.2017.02.001>
- 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>
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World - From Edge to Core*.
- Target Corporation. (2013, December 9). *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores*. A Bullseye View. <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car>

3. Article

Friesenecker, M., Gotsch, M., Schögel, M. (2022). Knowing is Half the Battle – The Effect of SME Marketers' Privacy Literacy on Privacy Orientation. *Marketing Review St. Gallen*, 2, 36-43.

Knowing is half the Battle - The Effect of Marketers' Privacy Literacy on SMEs' Privacy Orientation

Matthias Friesenecker, BA HSG

matthias.friesenecker@gmail.com

MindShare AG

Manessestrasse 85

8045 Zürich

Switzerland

Mauro Luis Gotsch, MA HSG

mauro.gotsch@unisg.ch / ORCID: 0000-0002-5319-2347

Institute of Marketing and Customer Insight, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

Prof. Dr. Marcus Schögel

marcus.schoegel@unisg.ch

Institute of Marketing and Customer Insight, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

CRedit author statement:

Matthias Friesenecker: Conceptualisation, Formal analysis, Investigation, Writing – Original Draft, Data Curation

Mauro Gotsch: Methodology, Writing – Review & Editing, Validation, Supervision, Formal analysis, Visualisation

Marcus Schögel: Validation, Resources, Project administration, Funding acquisition

Abstract

In the face of far-reaching privacy regulations such as the General Data Protection Regulation of the EU (GDPR), Marketing as a function needs to formulate long-term privacy goals to not become a central driver of risky customer data processing. Marketers are in a unique position to promote and enforce firm-wide data privacy measures; both by specifying its own data needs and by promoting adequate protection measures on a touchpoint level. This is especially true in small and medium-sized enterprises (SME), where marketers often exert direct control over touchpoints such as company websites. Yet, to utilise this potential, marketers require a basic level of privacy literacy. Using survey data of 55 SMEs, we evaluated the link between marketers' privacy literacy and their SME's website privacy orientation. The results show that most marketers in the sample do not demonstrate a higher privacy literacy than the general public. Additionally, almost half of the websites analysed did not implement all the privacy measures demanded under the GDPR. These first results establish a link between high privacy literacy and website privacy orientation.

Keywords: *Privacy Literacy, Information privacy, Privacy concern, Survey, Privacy strategy, OPLIS*

Core Hypothesis

- Since marketers in SMEs have more direct control over their firm's touchpoints, the level of their privacy literacy will help to determine the privacy orientation of these touchpoints.
- Marketers with a higher privacy literacy will perceive a higher risk for customers to share personal data via their firm's website.
- The privacy orientation of most SME websites will be geared towards the minimum legal requirements instead of the customers' potential privacy benefits.
- Marketers with an academic or professional background in IT will exhibit a higher general privacy literacy.
- A customer-oriented privacy policy implemented by SME marketers could help them exceed current privacy regulations while building the internal know-how and customer trust essential for the usage of data-intensive marketing technologies.

Managerial Implications

- Marketers in SMEs show little in terms of above average privacy literacy and about one in five of SME websites in the sample did not even feature an explicit privacy policy. This unpreparedness suggests a higher privacy risk when sharing customer data with SMEs.
- Swiss SMEs should invest in meeting the GDPR's six basic principles – not only because they most likely apply to them, but also because they represent a shift to a more customer-oriented privacy strategy.
- Investing in privacy trainings for marketers could improve the privacy orientation of data collecting touchpoints and thus reduce legal and image risks.
- Moving from a compliance-oriented towards a customer-oriented privacy strategy requires marketers with a high general privacy literacy.
- Hiring marketers with an IT-background is a short-term solution to raise the privacy literacy within a given firm.

Introduction

While big enterprises like Google, Amazon, Facebook, Apple or Microsoft are under intense scrutiny regarding their data privacy practices (see e.g., Stuart, 2021), comparatively little attention has been paid to the privacy practices of small and medium enterprises (SME). Naturally, SMEs generally collect and utilise far less customer data and have access to less advanced analytical capabilities (Bianchini & Michalkova, 2019). However, as a result, both research about and tools regarding SME privacy practices and IT-security have so far been “largely neglected” (Heidt et al., 2019, p. 1286). As SMEs’ capabilities and access to data processing tools (e.g., AI-aided customer relationship management software) are expected to increase (Bianchini & Michalkova, 2019; Coleman et al., 2016; Sen et al., 2016), this knowledge gap could become a risk factor. In light of far-reaching privacy regulations such as the General Data Protection Regulation of the EU (GDPR) and the “exceptional vulnerability” of SMEs to cyber-attacks (Van Haastreht et al., 2021, p. 1), more research to understand and improve SMEs’ privacy orientation is needed. However, since SMEs tend to be more “resource constrained” (Hernández-Linares et al., 2021, p. 179) and potential solutions should therefore build upon already existing capabilities or functions.

Past research has showcased a variety of approaches to improve a firm’s privacy orientation and marketing as a function “is often specifically named as being the central node of the modern privacy debate” (Gotsch & Schögel, 2021, p. 24). In SMEs, marketing capabilities are both used to “attain superior business results” (Lekmat et al., 2018, p. 213) and are often concentrated in the hands of a few natural persons (Camra-Fierro et al., 2012). This means, the control of data-collecting touchpoints like websites are often directly shaped by a single person or a small team. SME marketers are therefore in a unique position to both specify their firm’s informational needs to reduce surplus data being collected (Zuboff, 2019) and to ensure the satisfaction of customers’ privacy demands throughout their journey. Yet, to utilise this potential, it is likely that SME marketers require a basic level of privacy literacy (Baruh et al., 2017). Hence, this study aims to answer the following question:

***RQ:** Does the privacy literacy of marketers working in a business-to-consumer SME influence the privacy orientation of their firm’s website and privacy policy?*

A quantitative approach following a three-step procedure was chosen to provide first insights into the link between privacy literacy in marketers and privacy orientation. In a first step, the privacy literacy of SME-employees with influence over their firm’s touchpoints was recorded using a structured online questionnaire. In a second step, the corresponding privacy statements and websites were analysed. This was done on the basis of the legal minimum requirements defined within the GDPR and recorded by means of a structured evaluation form. Finally, the link between privacy literacy and data protection orientation of the website was tested using a multiple regression approach together with an analysis of variance (ANOVA).

Theoretical Basis

Privacy is a construct that is “notoriously hard to capture” (Koops et al., 2017, p. 487), as it has psychological, philosophical, ethical and legal dimensions. For the purpose of this study, Nissenbaum’s (2010, p. 4) definition covers the most important aspects of informational privacy as a “claim to appropriate flows of personal information” within the “distinctive social context” of a customer-firm interaction. Hence, for an SME’s privacy policy to be “privacy-oriented”, it should allow the customer to easily view and adjust the level of how much they can be “sensed” by said SME through the data shared with them (Belanger et al., 2002, p. 245; Parker, 1974, p. 273; Petronio, 2010, p. 179).

While most modern data privacy laws set a baseline of protection which should be upheld by any entity collecting data (“privacy by design”, GDPR, Art. 25), the sharing of personal data is still largely treated as a matter of personal responsibility. Yet, consent-driven privacy self-management faces the “inherent limitation” (Barocas & Nissenbaum, 2014, p. 31; Solove, 2013, 2021) of most customers being unable to overcome the “rational, irrational and structural” factors influencing their decision-making process (Gotsch & Schögel, 2021, p. 4). As a result, customers’ expressed privacy concerns often do not match with their level of disclosed personal data across various platforms (Acquisti, 2004; Norberg & Horne, 2007).

This limitation can be partially addressed by increasing the privacy literacy of all the parties involved. Trepte et al. (2015, p. 339) elaborate on this notion and state that privacy literacy is a combination of factual or declarative (“knowing that”) and procedural (“knowing how”) knowledge on the protection of one’s own privacy.

Generally, increasing privacy literacy within a firm’s human-resource pool to achieve a higher privacy orientation overall has been recommended within several studies (Amiri et al., 2018; Bulgurcu et al., 2017; Gotsch & Schögel, 2021; Kokolakis, 2017; Schögel, 2016; Solove, 2013; Taneja et al., 2014). However, the link between marketers’ privacy literacy and touchpoint privacy orientation has not been established so far. This study aims to test the feasibility of this recommendation within the SME context, where such a connection is more direct than in a large firm. Hence, we hypothesise:

H1: *The presence of SME-marketers with a high privacy literacy will increase the privacy orientation of the touchpoints under their influence.*

Since the decision to collect personal data from a SME’s perspective is also a rational weighing of customer risks and benefits, it is assumed that marketers perform a privacy calculus similar to their customers (Dinev & Hart, 2006; Zhu et al., 2017). To properly assess both the benefits and risks of their customer’s disclosure of data, marketers need a certain level of privacy literacy (Trepte et al., 2015).

H2a: SME-marketers' privacy literacy positively affects the perceived risks of customers disclosing personal data over touchpoints under their control.

H2b: SME-marketers' privacy literacy negatively affects the perceived benefits of customers disclosing personal data over touchpoints under their control.

While privacy literacy is assumed to have a direct effect on the privacy orientation of touchpoints, it is also likely, that this effect is partially mediated by the privacy calculus, as it is with customers' protective behaviour (see e.g., Yun et al., 2019).

H3a: SME-marketers' perceived risks of customers disclosing personal data over touchpoints under their control positively influences the privacy orientation of said touchpoints.

H3b: SME-marketers' perceived benefits of customer's disclosing personal data over touchpoints under their control negatively influences the privacy orientation of said touchpoints.

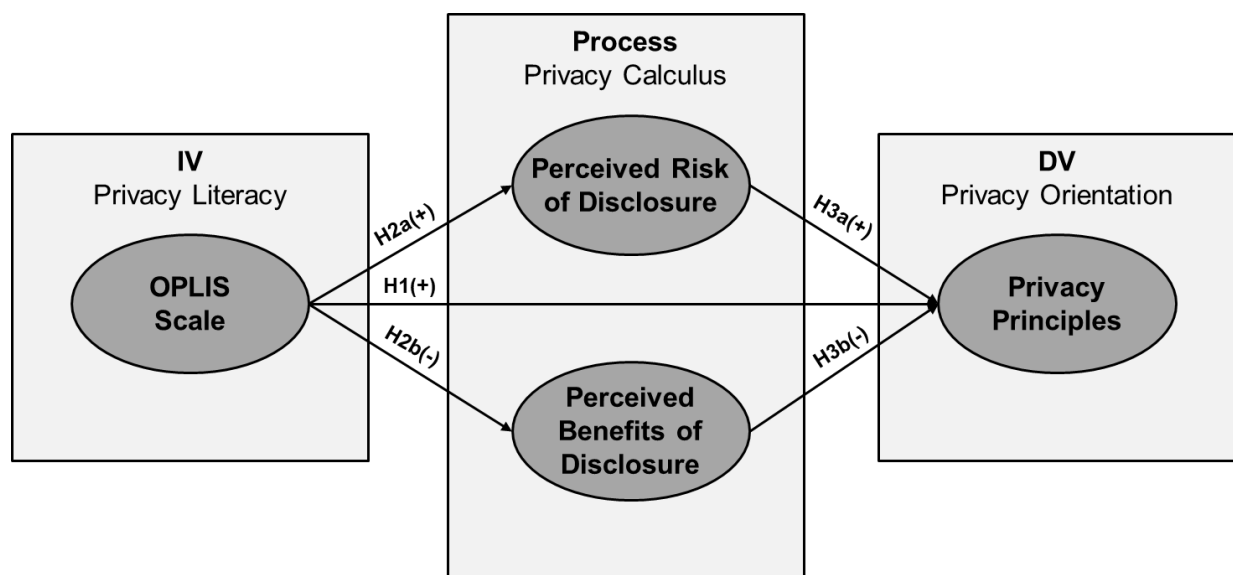


Figure 3-1 Hypotheses & research design

Methodology

The data was collected in two steps: first via an online survey, manually targeted towards SME-owners or employees with marketing responsibility and second by using a structured evaluation form for the corresponding websites and privacy policies. The data set was collected using direct mailings to SME marketers from Switzerland. A firm was determined to be an SME if it employs less than 250 people (Bfs, 2020). Additionally, all the SMEs in the sample had to operate within a business-to-consumer (B2C) context with access to their customers'

personal data. The final sample came down to 55 SMEs operating a B2C business within Switzerland or Lichtenstein. Of those SMEs, micro firms (<10 employees) made up almost half of the sample, followed by small firms with approx. 40% (<50 employees) and finally medium companies with about 10% (<250 employees).

The questionnaire the SMEs were sent was structured in two parts – first asking for demographics and measuring the calculus and various control variables (e.g., IT-background). Second, the Online Privacy Literacy Measurement Scale (OPLIS) developed by Trepte et al. (2015, p. 338) was used to measure privacy literacy. The scale was developed on the basis of a qualitative content analysis of research articles and adapted to be deployed in the German-speaking market (Masur et al., 2020). It was reduced by Masur et al. (2017, p. 256) to a 20-item validated scale, able to “predict the implementation of data protection measures”. To evaluate SMEs’ privacy orientation, the evaluation method by Martin et al. (2017, p. 42) was used. It treats SMEs’ privacy policies as meaningful proxies for their actual privacy practices.

Hence, for each SME, their privacy policies and their primary website were analysed. The evaluation was based on the legal requirements of the GDPR. The following aspects were taken into account:

- Provides support for exercising the right to object (opt-out options).
- Explanation of what data are collected (type and scope of data collection).
- Explanation of how data are used (purpose or use)
- Explanation of how data will be shared in the course of exchange
- Provides contact information for privacy inquiries
- Informs about the use of cookies on the website
- Informs about (or offers) the possibility to deactivate cookies
- Informs if and which analysis tools are used (e.g., Google Analytics)
- Information about users’ rights such as the right to information, deletion, correction and transfer of personal data
- Deploys cookie banners on pages utilizing them

The stricter requirements of the GDPR were applied to judge the Swiss SMEs’ privacy policies, because it is assumed that the majority of data collecting companies in Switzerland are affected by EU law due to the market location principle (see GDPR Art. 13, Ebert & Widmer, 2018, p. 12; FDPIC, 2018, p. 3; Möhle, 2021). We chose to sample Swiss SMEs, because despite most likely having to adapt GDPR guideline, they in general demonstrate a low expertise about these principles (Ebert & Widmer, 2018, p. 11).

Results

The data of the 55 SMEs was compiled by one author and checked for accuracy (e.g., by re-reading privacy policies) as well as prepared for analysis by the other. All data was compiled and analysed using IBM SPSS Statistics.

Privacy Literacy within SMEs

In order to put the overall privacy literacy of the SME participants in the proper context, their results were compared to the norm table for privacy literacy within the general German population from the OPLIS guide created by Masur, et. al (2020, p. 13). It shows that the population average of 12 was slightly but not significantly lower than the SME-mean of 13.2 correctly answered questions. In total, only around 60% of SMEs demonstrated a privacy literacy that is above the population average. Unsurprisingly, the 11 SME participants with a background in IT were found to have a significantly higher ($p<0.01$) mean OPLIS score, than other participants.

OPLIS is designed to measure privacy literacy across four knowledge dimensions. Figure 4 shows the cumulative percentage of how high the knowledge levels are across the dimensions within the sample. It shows that there are knowledge gaps relating to the data processing practices of third-party institutions as well as the current legal practices. Both of these dimensions are critical in the assessment of potential risks of disclosure of personal data (Masur et al., 2017), which in turn might also explain the gap in cyber security capabilities between SMEs and larger firms (Heidt et al., 2019; Van Haastrecht et al., 2021). These findings are also in line with previous studies, which suggest that privacy literacy training is of low importance in SMEs (Ebert & Widmer, 2018; Heidt et al., 2019).

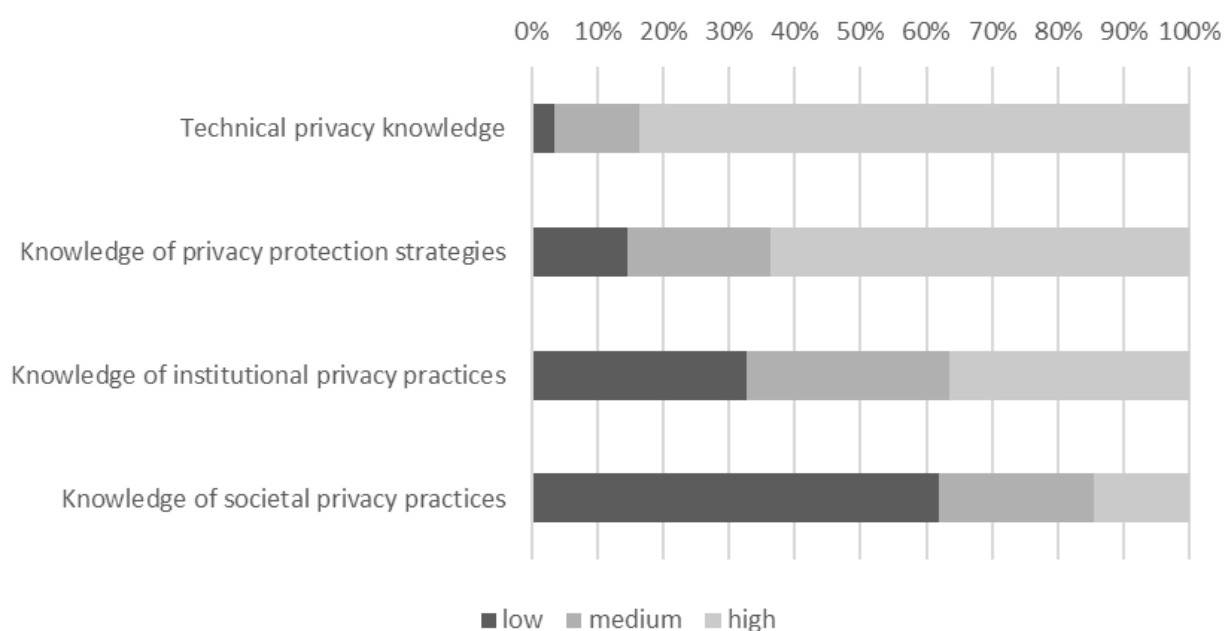


Figure 3-2 OPLIS knowledge levels (n=55)

Website Privacy Orientation

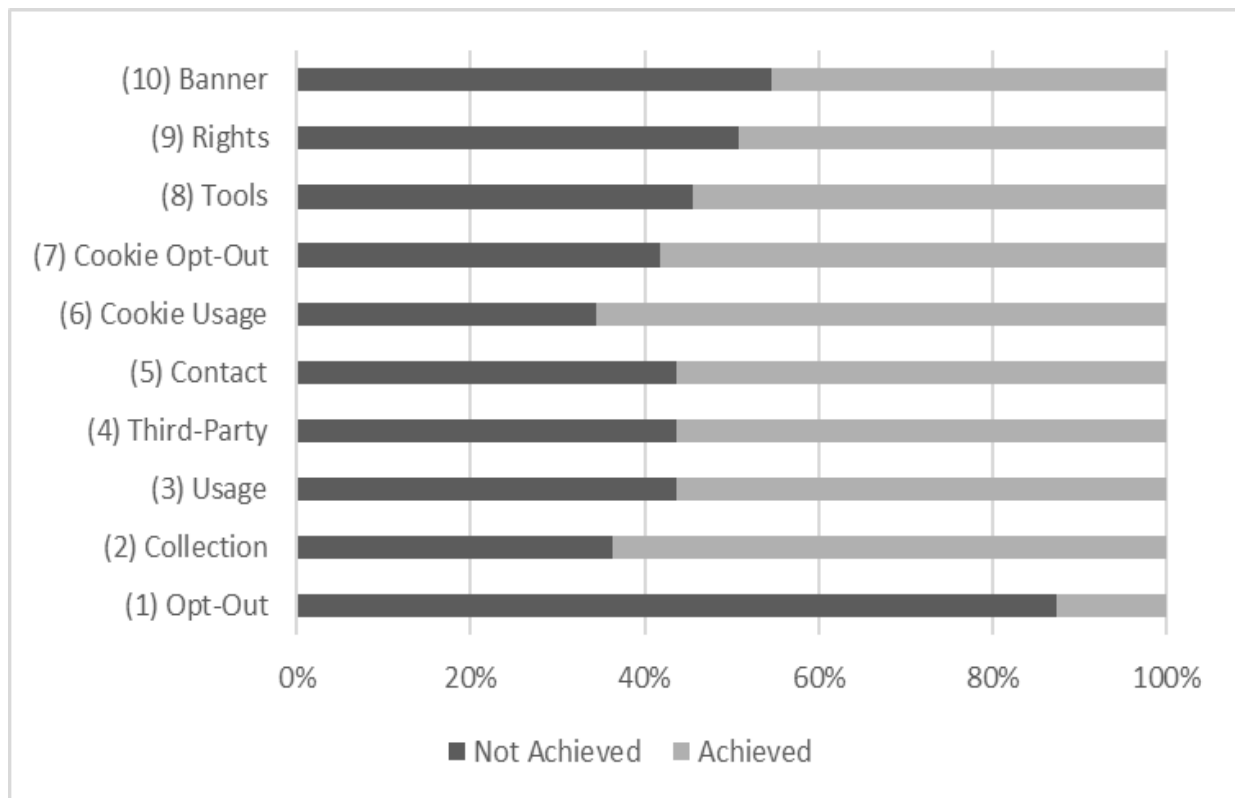


Figure 3-3 Website privacy orientation items (n=55)

The data on the privacy orientation of the SMEs was collected in a two-month period by one researcher, directly following upon a participant answering the questionnaire. Once the dataset of 55 SMEs was collected, another researcher reviewed all the criteria again, to ensure a reliable reading while decreasing the chance of misinterpretation. Figure 5 shows the individual percentages of requirements met by the SMEs.

The informational requirements (points 1 to 5) were met by the majority of SMEs in the sample (56%). SMEs usually informed customers that personal data would be collected, although it was not always specified exactly which data would be stored.

When providing contact information for privacy inquiries, most of the SMEs listed their standard address (info@XYZ). This suggests that there is no specific office or person entrusted with the task – further supporting the idea of SME-marketers being able to exercise direct control over collected customer data.

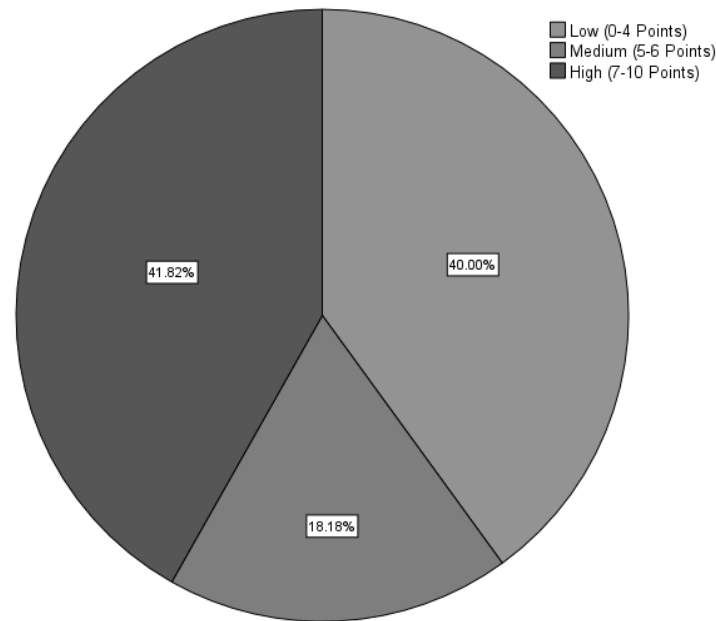


Figure 3-4 Privacy orientation of SME websites (n=55)

Overall, a majority of SMEs showed a medium to high privacy orientation on their website and privacy policy (see fig. 5). However, considering the measurement was derived from the minimum requirements found in the GDPR, the SMEs are only oriented towards minimal compliance. Almost all privacy policies in the sample provide customers with some information on how data is collected, but without mentioning any specifics. This finding is in line with a larger shift in the “landscape of privacy policies” triggered by the ratification of the GDPR: coverage of privacy policies might have improved, but often at the cost of reduced specificity (Linden et al., 2020, p. 47).

The Connection between Privacy Literacy & Orientation

The descriptive results paint a picture of how privacy is understood and practiced within the SMEs in the sample, but it does not provide additional information on the relationship between the variables. Figure 7 shows the correlations between all the variables in the proposed model.

	OPLIS	Per. Risk	Per. Benefits	Privacy Orient.
OPLIS	1	.421**	.026	.313**
Per. Risk	.421**	1	.248*	.103
Per. Benefits	.026	.248*	1	-.151
Privacy Orient.	.313**	.103	-.151	1

*Figure 3-5 Correlations between model variables / * sign. at the 0.05 level (2-tailed) / ** sign. at the 0.01 level (2-tailed)*

Since several of the independent variables were found to be significantly correlated, the variance inflation factors were calculated to test for multicollinearity, but none of them exceeded the value of 2. While the focus lied predominantly on testing the research model presented in figure 1, alternative models were calculated to test the mediating effect of the privacy calculus, control for SME variables (e.g., industry) and interactions. However, these models did not show significant loadings (i.e., a $p < .05$) and hence we proceeded to evaluate the original model's fit and path coefficient results shown in figure 6.

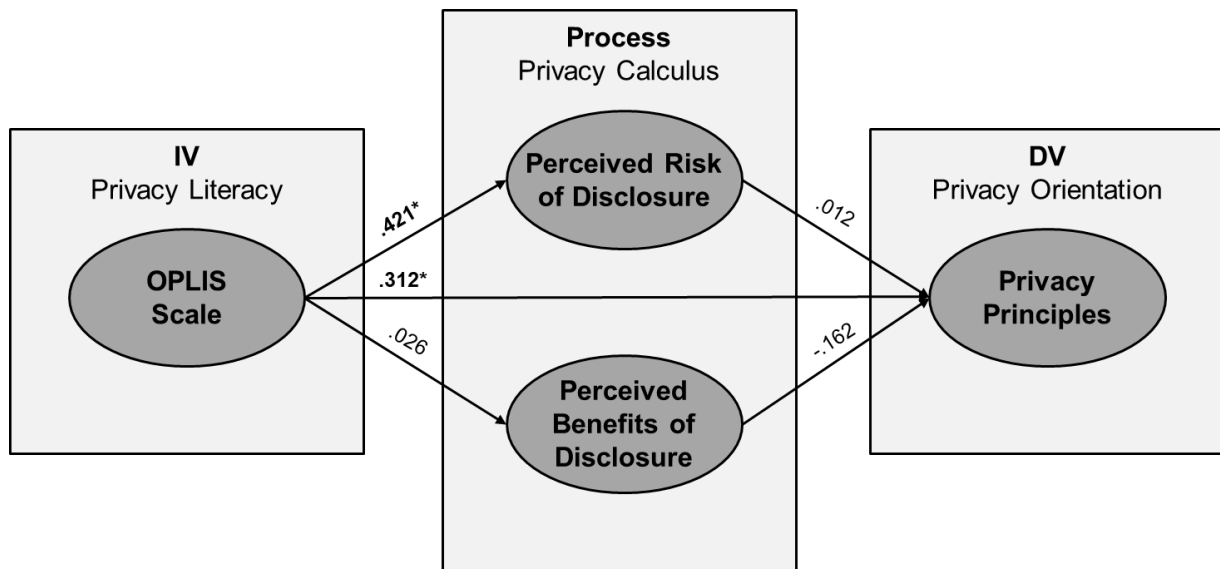


Figure 3-6 Model with standardised path coefficients / *sign. at the 0.01 level

With the rather small $R^2 = .123$, the models' errors are only about 5% smaller on average than those of the constant-only model. The direction of the effects is as hypothesised, with privacy literacy increasing perceived risks and privacy orientation and perceived benefits decreasing privacy orientation. However, only the first two paths showed a significant effect.

To test the effect on a group level, the sample was then divided according to the OPLIS ranking suggested by Masur et. al (2020). Three groups were formed with low OPLIS scores (<11 Pt.), medium OPLIS scores (12-15 Pt.) and high OPLIS scores (>15 Pt.). The difference in the mean value of the privacy orientation between the three groups is statistically significant ($p=0.041$). While the mean of the medium group showed no significant difference to the others (5.2), in companies with a low privacy literacy, the privacy orientation of the website (3.5) was found to be significantly lower than that of companies with a high privacy literacy (6.5). Despite the limited sample, first indices for privacy literacy affecting the privacy orientation in SME touch-points could therefore be found.

Discussion

We examined how privacy literacy of SME-marketers impacts their privacy calculus and the privacy orientation of the touchpoints under their control. By using a multiple regression approach together with an analysis of variance, we were able to support the hypothesis of privacy literacy influencing privacy orientation but had to reject our proposed model of how this influence manifests in a cause-and-effect relationship.

Hypothesis	Variables	Result
H1	Privacy Literacy & Privacy Orientation	Supported
H2a	Privacy Literacy & Perceived Risk	Supported
H2b	Privacy Literacy & Perceived Benefits	Not Supported
H3a	Perceived Risk & Privacy Orientation	Not Supported
H3b	Perceived Benefits & Privacy Orientation	Not Supported

Figure 3-7 Hypothesis and results in overview

Even though privacy literacy served as a significant predictor for the privacy orientation of the SMEs touchpoints, the privacy calculus could not be supported as the process used by marketers to translate knowledge into action. Seeing how SME-marketers with a high privacy literacy still perceived the threats of disclosure to be higher than those with lower literacy, suggests that the decision to follow stricter privacy measures is not driven by a customer-centric logic. It is likely, that even within the SMEs shorter chain of command, the environmental context (e.g., less strict privacy laws in Switzerland), technical hurdles (e.g., out-of-the-box websites), and firm-specific considerations (e.g., marketing culture) have a larger influence than customer considerations (see also Sarathy & Robertson, 2003). Additionally, in line with the study by Ebert & Widmer (2018, p. 3), Swiss SMEs also do not seem to regard privacy as an important strategic mission.

The survey on privacy literacy showed that the knowledge level of SME-marketers was only slightly above the population average. This hints towards insufficient knowledge among SMEs in the area of data protection and modern privacy practices – especially considering the comparatively low difficulty of the OPLIS-scale.

The analysis of the websites and the data privacy statements showed that at least half of the SMEs only barely comply with current legal requirements. For every fifth firm, an explicit privacy policy was missing from the website. It can be assumed, that many SMEs still work to a considerable extent with potentially problematic data regarding their compliance with the GDPR. The majority of companies with a good data protection orientation met the data protection requirements under the GDPR. However, the stricter provisions of the GDPR regarding

a transparent and understandable use of customer data (e.g., what kind of user profiles are created based on sales data?) or renouncement of social media plugins (i.e., usage of social network data for retargeting) were hardly met by any SME in the sample.

The hypothesis that higher privacy literacy leads to higher data protection orientation was supported. However, due to the comparatively low contribution of privacy literacy and the privacy calculus on data privacy orientation, considerations for the customers' view are unlikely to drive further privacy enhancements.

Conclusion

Marketing strategies across industries are increasingly based on the processing of customer data. Along with these practices, privacy concerns in the population have increased as well (see e.g., Auxier et al., 2019; Veritas, 2017). At the institutional level, companies are facing stricter legislation with the introduction of the GDPR and the potential expansion of the nDSG in Switzerland (Pfister, 2021). Marketers, as key users of customer data, are thus increasingly caught in the tension between data processing and protection.

In this context, this study researched whether the privacy literacy of SME marketers in a B2C context has an impact on the privacy orientation of their SME. By means of a standardised questionnaire, 55 SME marketers were surveyed about their privacy literacy and a sum index was calculated. Furthermore, the websites and the privacy statements of the corresponding SMEs were evaluated on the basis of a GDPR-oriented control form. Finally, it was investigated whether there was a cause-and-effect relationship between the privacy literacy of SME marketers and the data protection orientation of their SME.

The results show that the majority of SME marketers in the sample do not demonstrate a significantly higher privacy literacy than the general public. Additionally, almost half of the websites analysed did not implement all privacy measures demanded under the GDPR. A SME's industry was no significant predictor to this end as well. While the privacy literacy of SME marketers served as a predictor of implementation of said measures, it is not done via the hypothesised privacy calculus. Hence, other factors not relating to the customers' potential risks and benefits drove the implementation of privacy measures within these SMEs. These results are in line with the previously reported reactive and compliance-oriented stance of SMEs when it comes to data privacy and cyber security (Ebert & Widmer, 2018; Heidt et al., 2019; Lopes & Melão, 2016; Van Haastrecht et al., 2021). Additionally, a qualitative finding in the analysis of the privacy statements was the predominant citation of articles of law that were difficult to understand, and not communicatively oriented toward customers.

Since the privacy calculus is unlikely to serve as a mediator between privacy literacy and privacy orientation, testing other process variables is still necessary in future research. Examining

an SME's structure, IT-budgets, data-processing practices or training efforts might produce a more complete understanding of how privacy literacy affects privacy orientation.

It is expected that SMEs will increasingly try to build the capabilities to use big data applications to carve out a competitive advantage within their industries (Bianchini & Michalkova, 2019; Sen et al., 2016). However, the current compliance and self-management focused privacy strategy "cannot achieve the goals demanded of it" (Solove, 2013, p. 1903). Hence, a shift towards a more proactive privacy strategy – investing early into the resources and the knowledge-base to build privacy compliant and secure data processes is needed. On the one hand, to keep up with current privacy legislation, and on the other, to meet the growing customer demand for privacy (Palmatier & Martin, 2019, p. 176).

We have shown that marketers acquiring a basic level of privacy literacy can contribute to the building of these resources and overall privacy orientation. Therefore, further investments into employee privacy trainings are a good start in the fight against privacy violations – after all, knowing the how and what of privacy is half the battle.

References

- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Pre-Proceedings to EC'04, May 17-20, New York*, 1–9.
- Amiri, I., Wang, L., Levy, Y., & Hur, I. (2018). An Empirical Study on the Factors Contributing to Disclosing Personal Information Online: Insecurity in the Digital Age. *Twenty-Fourth Americas Conference on Information Systems*, 1–10.
- Auxier, B. Y. B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and Privacy: Concerned, Confused, and Feeling a Lack of Control Over Their Personal Information. *Pew Research Center, November*, 1–63.
- Barocas, S., & Nissenbaum, H. (2014). Computing Ethics: Big Data's End Run Around Procedural Privacy Protections Recognizing the inherent limitations of consent and anonymity. *Communications of the ACM*, 57(11), 31–33. <https://doi.org/10.1145/2668897>
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, 11, 245–270.
- Bfs. (2020, August 28). *Kleine und mittlere Unternehmen* | Bundesamt für Statistik. Bundesamt Für Statistik. <https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaef-tigte/wirtschaftsstruktur-unternehmen/kmu.html>
- 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>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2017). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. In *MIS Quarterly* (Vol. 34, Issue 3). <https://doi.org/10.2307/25750690>
- Camra-Fierro, J., Centeno, E., Pérez-Cabañero, C., González-Cruz, T., & Cruz-Ros, S. (2012). Do family SME managers value marketing capabilities' contribution to firm performance? *Marketing Intelligence & Planning*, 30(2), 116–142. <https://doi.org/10.1108/02634501211211948>
- Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorell, X., & Reis, M. S. (2016). How Can SMEs Benefit from Big Data? Challenges and a Path Forward. *Quality and Reliability Engineering International*, 32(6), 2151–2164. <https://doi.org/10.1002/QRE.2008>
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Ebert, N., & Widmer, M. (2018). *Datenschutz in Schweizer Unternehmen 2018*. ZHAW Zürcher Hochschule für Angewandte Wissenschaften. <https://doi.org/10.21256/ZHAW-4001>
- FDPIC. (2018). *The GDPR and its consequences for Switzerland* (Issue July). Federal Data Protection and Information Commissioner (FDPIC).
- 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>
- 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>
- Hernández-Linares, R., Kellermanns, F. W., & López-Fernández, M. C. (2021). Dynamic capabilities and SME performance: The moderating effect of market orientation. *Journal of Small Business Management*, 59(1), 162–195. <https://doi.org/10.1111/jsbm.12474>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, 64(November), 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Koops, B. J., Newell, B. C., Timan, T., Škorvák, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. In *University of Pennsylvania Journal of International Law* (Vol. 38, Issue 2).

- Lekmat, L., Selvarajah, C., & Hewege, C. (2018). Relationship between Market Orientation, Entrepreneurial Orientation, and Firm Performance in Thai SMEs: The Mediating Role of Marketing Capabilities Laddawan. *International Journal of Business and Economics*, 17(3), 213–237.
- Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, 1, 47–64. <https://doi.org/10.2478/popets-2020-0004>
- Lopes, L. A., & Melão, N. F. (2016). Website content and design in SME: Insights from Portugal. *International Journal of Electronic Business*, 13(1), 70–97. <https://doi.org/10.1504/IJEB.2016.075343>
- 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>
- Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica*, 63(4), 256–268. <https://doi.org/10.1026/0012-1924/A000179>
- Masur, P. K., Teutsch, D., & Trepte, S. (2020). *OPLIS Manual*. Universität Hohenheim.
- Möhle, J.-P. (2021). Totalrevision des Schweizer Datenschutzgesetzes – Ende gut, alles gut? *Datenschutz Und Datensicherheit - DuD 2021* 45:9, 45(9), 598–602. <https://doi.org/10.1007/S11623-021-1498-Y>
- Nissenbaum, H. (2010). Privacy in Context Technology, Policy, and the Integrity of Social Life. In *Privacy in Context*. Stanford University Press.
- Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. *Psychology & Marketing*, 24(10), 829–847. <https://doi.org/10.1002/mar.20186>
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Parker, R. B. (1974). A Definition of Privacy. *Rutgers Law Review*, 27(2), 275–297. <https://heinonline.org/HOL/Page?handle=hein.journals/rutlr27&id=283&div=23&collection=journals>
- Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, 2(3), 175–196. <https://doi.org/10.1111/j.1756-2589.2010.00052.x>
- Pfister, W. (2021, August 4). “Für KMU ist es von Vorteil, sich auf das neue Datenschutzgesetz vorzubereiten.” *KMU Portal, WBF: Eidgenössisches Departement Für Wirtschaft, Bildung Und Forschung*. <https://www.kmu.admin.ch/kmu/de/home/aktuell/interviews/2021/fuer-kmu-ist-es-von-vorteil-sich-auf-das-neue-datenschutz-gesetz-vorzubereiten.html>
- Sarathy, R., & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. In *Source: Journal of Business Ethics* (Vol. 46, Issue 2).
- Schögel, M. (2016). Marketing Automation, Machine Learning und Artificial Intelligence. *Marketing Review St. Gallen*, 4, 3.
- Sen, D., Ozturk, M., & Vayvay, O. (2016). An Overview of Big Data for Growth in SMEs. *Procedia - Social and Behavioral Sciences*, 235, 159–167. <https://doi.org/10.1016/J.SBSPRO.2016.11.011>
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, 89(1), 1–51.
- Stuart, T. (2021). Too little too late? An exploration and analysis of the inadequacies of antitrust law when regulating GAFAM data-driven mergers and the potential legal remedies available in the age of Big Data. <https://doi.org/10.1080/17441056.2021.1909234>, 17(2), 407–436.
- Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, 38, 159–173. <https://doi.org/10.1016/j.chb.2014.05.027>
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law* (pp. 333–365). Springer. https://doi.org/10.1007/978-94-017-9385-8_14
- Van Haastreht, M., Sarhan, I., Shojafar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. *ACM International Conference Proceeding Series*, 1–12. <https://doi.org/10.1145/3465481.3469199>
- Veritas. (2017). *2017 Veritas Gdpr Report*. Veritas Schweiz AG.

- Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information and Management*, 56(4), 570–601. <https://doi.org/10.1016/j.im.2018.10.001>
- Zhu, H., Ou, C. X. J., van den Heuvel, W. J. A. M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, 54(4), 427–437. <https://doi.org/10.1016/j.im.2016.10.001>
- Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, 28(1), 10–29. <https://doi.org/10.1177/1095796018819461>

4. Article

Gotsch, M. (2022). Customer Centricity & Datenschutz – Die Geschichte eines Missverständnisses. *Marketing Review St. Gallen*, 2, 12-19.

Translated from German to English by the author.

Customer Centricity & Data Privacy: A Story of Misunderstandings

Mauro Luis Gotsch, MA HSG

mauro.gotsch@unisg.ch / ORCID: 0000-0002-5319-2347

Institute of Marketing, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

Abstract

The argument of customer centricity has been used to justify excessive customer data collection for well over 20 years now. However, reducing the value of customers to mere data points that can be further processed in aggregated data sets, often leaves the original definition of customer centricity behind. This paper shows why a return to the original definition makes sense for marketers and can at the same time contribute to the data privacy of customers.

Keywords: *privacy marketing, data processing, surveillance capitalism*

Core Theses

- The argument of customer centricity has been and still is often used inconsistently to justify excessive customer data collection.
- Automatic or agnostic data collection is often neither legal thanks to modern data privacy laws, sustainable, or customer-oriented due to an increasing demand for data privacy.
- A return to the basics of customer centricity can help marketers establish forward-looking data processing practices.
- Investing in customer-centric privacy practices early on builds the necessary trust and knowledge required to apply innovative marketing technologies.

Practical Implications

- Check how much excess data is generated by your touchpoints and where this data is stored and processed.
- Invest early in customer-centric structures and processes that are necessary for a tighter purpose binding of customer data processing.
- Increase the amount of data collected only if existing personnel already have the necessary technological and analytical skills to process it.
- Invest in anonymisation and encryption technology across all used data architectures.

Introduction

In many companies, the digitalisation of customer processes is being driven by the term customer centricity. Yet, it often remains unclear whether customer centricity is cited as a strategy, structure, orientation, or sales argument. What is clear, however, is that customer-centric digitalisation should generate all data necessary to personalise company services (see e.g., Day, 2003; Gulati & Oldroyd, 2005a; Latinovic & Chatterjee, 2019). The underlying assumption is that the more customer data is being collected, the more product development and sales opportunities will arise. However, as target customers are reduced to mere data points, it becomes increasingly easier to view them only as such or to even sell them as a product to third parties. In the past, these data sets were used to engineer marketing algorithms and targeted advertising campaigns. Recently, aggregating data and using it in artificial intelligence training sets has evolved into its own distinct business model (Lobschat et al., 2021).

This equation of data collection and customer centricity has been pushed since the late 1990s, especially by digital platforms such as Google and Amazon, applied in popular discourse (Galbraith, 2005; Gulati & Oldroyd, 2005b; Shah et al., 2006; Sheth et al., 2000; Waisberg & Kaushik, 2009), and often accepted as “the holy grail of marketing” to this day (Latinovic & Chatterjee, 2019, p. 3).

However, amid an increased vulnerability of consumer data privacy and rising global demand for more data privacy, a key question emerges: How customer-centric and sustainable are these business models? This positioning paper argues that a return to the original marketing goal of customer centricity is necessary: to place the satisfaction of customer needs in co-creation with one's own clientele at the centre of entrepreneurial action. This requires a basis of trust, which can only be realised with a strategic privacy orientation.

Customer obsession, data collection, and behavioural surplus

In 1997, Jeff Bezos outlined the strategic pillars that continue to define Amazon to this day. Likely the best-known of these pillars is Bezos' often quoted “customer obsession” (Denning, 2013). His goal was a culture built on data-driven familiarity—almost data-driven intimacy—with customers. Rossmann, former executive at Amazon, described the culture as follows: “It's everyone's job to know the customer and get excited about them. [...] Know the details of the customer experience and find out what causes friction for customers [in the buying process]” (Rossmann, 2019). To this day, Amazon lists “becoming the world's most customer-centric company” as the core of its mission (Amazon, 2021).

Translated into strategy, this can be summed up as recording and storing every customer interaction across every available Amazon touchpoint. Whether it is via the Amazon online storefront, Prime Video, Kindle, Twitch, Audible, Wholefoods physical stores, or the Alexa

virtual assistant, every second of interaction is stored to serve the mantra of customer obsession. Far from just service-related behavioural data (e.g., usage time), this creates a surplus of seemingly worthless customer information. It is this “behavioural surplus” that drives the engine of modern digital platforms (Zuboff, 2019, p. 13). For example, Alexa and its connected ecosystem of home and kitchen appliances serve as a veritable personal supply chain of intimate life data. This data is fed into various machine learning algorithms to optimise the customer experience across all platforms or to design completely new products (Amazon, 2018). Whether this process is always completely legal was called into question in 2021 with a 746 million EUR GDPR fine levied against Amazon. The original complaint, which triggered the lawsuit that was still ongoing at the time of publication, claimed that Amazon’s processing of personal data was not based on “free consent” (Burgess, 2021).

Nevertheless, the success of this tapping of anticipatory customer data has greatly benefited Amazon: The majority of US households are estimated to have an active Amazon Prime account (Kats, 2020) and the company continues to be used as a benchmark for the entire retail industry (Jindal et al., 2021).

Amazon has also successfully duplicated and sold this same strategy to its competitors in recent years. Thanks to the easy integration of products into the Amazon Marketplace (Ritala et al., 2014) and the integration of Alexa into products by third-party developers, numerous companies have access to select parts of the Amazon data supply chain.

It is therefore no wonder that “data collection for more customer centricity” still constitutes a popular dogma for many businesses (see e.g., Microsoft, 2020, p. 5). But if “more customer data” is so often the answer, what was the original question?

How customer centricity is falling behind

The concept of customer centricity is mostly used by companies to publicly imply ‘the customer is important to us.’ However, despite—or perhaps because of—the popularity of the term, it is discussed rather controversially in marketing literature (Fader, 2012; Habel et al., 2020; Shah et al., 2006). According to one contemporary definition, a company is customer-centric if it “places the interests of its customers at the centre of its entrepreneurial activities [...] by introducing customer-centric organisational structures, customer-centric information technologies and customer-centric marketing strategies” (Habel et al., 2020, p. 25). The concept is thus positioned as the antithesis to product centricity (Fader, 2012; Galbraith, 2005; Shah et al., 2006). Most literature on customer centricity revolves around two issues: the lack of a common understanding of what factors constitute customer centricity (see e.g., Shah et al., 2006), and the benefits of customer centricity from a business perspective (see e.g., Gummesson, 2008; J. Y. Lee et al., 2015). But even the aspects of customer centricity that are clearly defined in theory are rarely encountered in practice.

Customer-centric organisational structures are estimated to be used by less than 30% of Fortune 500 companies (J. Lee et al., 2015; Ulaga, 2018). This is because customer-centric structures increase both the cost and complexity of customer interactions. At the same time, these costs may not be outweighed in all market positions by the difficult-to-measure benefits of a customer-centric organisation (Habel et al., 2020; J. Y. Lee et al., 2015).

Within customer-centric information technologies “customers are an integral and critical part of the [technology’s] development” (Liang & Tanniru, 2006, p. 11). Open software architectures, such as the Wikipedia architecture, allow for the dynamic development of systems in tandem with customer needs but are rarely used by companies due to a lack of complete control (Wagner & Majchrzak, 2006).

The question remains then, whether we can at least observe customer-centric marketing strategies. Here we come back to Amazon’s customer obsession: Bezos’ strategy originally pursued a purely customer-centric service logic (Bettencourt et al., 2014; Vargo & Lusch, 2004) with his online bookstore. The “job-to-be-done” was not to sell a particular book to customers, but to offer each user a suitable read. The interactive rating by customers and the associated recommendation algorithm are an example of customer orientation in platform design (Liang & Tanniru, 2006). This is why Amazon allowed competing bookstores and independent publications on its platform early on: more providers meant more choices for the customer, as well as a better understanding of their interests. The assumption was also that reduced search efforts and storage costs, would allow niche products to be sold more often (Meiseberg, 2016). Amazon has since proven that this same logic can be scaled in other product categories as well.

However, the openness of Amazon’s platforms also meant that the majority of offers soon came from product- or market-oriented companies. For these suppliers, the Amazon algorithm does not serve to fulfil a “job-to-be-done” with the customer (Christensen et al., 2016) but to increase sales. The question for a supplier is not “What need does the customer satisfy with our product?” but “What can we do to make the customer consume our product?” (Riedmann-Streitz, 2018, p. 213). Amazon recognised this as an opportunity and soon positioned itself as an interesting partner for the advertising industry; “the driver for Amazon’s business success became not only the transaction and the associated revenue such as commission, but the time the platform is used” (Krämer, 2018, p. 16).

Digital platforms alongside Amazon have undergone a similar evolution. Google realised early on that profit lay not in the customer need of finding relevant data alone, but in selling predictive models to the advertising industry (Zuboff, 2019). Facebook has long been known not only as a social media company but, thanks to scandals like Cambridge Analytica (Isaak & Hanna, 2018), as a dystopian product platform (Wakefield, 2021), which according to whistle-blower Frances Haugen “puts its astronomical profits before human welfare” (Haugen, 2021). In virtually all digital platforms, the customer is now traded as a product in one form or another (Park et al., 2018). The more a customer can be reduced to a data point, the easier it

is to sell them as a product. The original idea of data-driven customer centricity is thus left in the dust entirely (Riedmann-Streitz, 2018, p. 212).

From a marketing perspective, this is undoubtedly lucrative but likely unsustainable. From a business perspective, because it increases both the eventual cost of a data leak (Chen & Jai, 2019; Cheng et al., 2017; Choong et al., 2017; Janakiraman et al., 2017) as well as data processing costs, e.g., investment in data architectures that are not needed (Experian, 2020).

From a customer perspective, because their potential costs can range from echo chambers, price discrimination, and psychological damage to identity theft (Acquisti et al., 2020, p. 748). Privacy concerns are therefore increasingly being voiced by the public (Acquisti et al., 2020; Cisco, 2019; Plangger & Montecchi, 2020; Salesforce, 2019) and customers are slowly learning how to defend themselves against unwanted data requests with VPNs and adblockers (Howe & Nissenbaum, 2017). In such an environment, it will not be enough to collect as much data as possible; instead, fundamental trust based on an understanding of customer needs will be essential (Gotsch & Schögel, 2021). Jumping on the same trends as Amazon requires major resources and customer data. Nevertheless, small and medium-sized enterprises have shown that they, too, can execute a functioning customer-centric strategy with far less resources at-hand (Coleman et al., 2016).

Customer-centric equals privacy-driven

Amazon's success demonstrates that the goal of data privacy from a corporate perspective cannot be to avoid data processing all together. Instead, companies should be looking to process data to improve their products rather than selling them (Fader, 2012). Improving in this case means that data is processed only to "look for more customer needs to satisfy" (Galbraith, 2005, p. 11). However, this query should be for the services currently being used, not for hypothetical future products.

This is the core idea of customer centricity: to "generate customer intelligence" by "actively engaging customers in marketing and innovation processes to co-create value with them" (Lamberti, 2013, p. 594). At the same time, customer centricity shifts the focus of organisational processes from the product offered to the customer experience as a whole, with the aim of improving value creation in relation to the individual customer (Lamberti, 2013; Prahalad & Ramaswamy, 2004; Wind & Rangaswamy, 2001).

This is also a desirable approach from a privacy perspective. Findings in psychology stated that data privacy needs of individuals are best captured through dialogue: "Negotiation of privacy rules is necessary to mitigate or prevent violations by [data] co-owners" (Petronio, 2010, p. 181). In a product-oriented company, the workforce is typically organised around sales and production (West & Wildeman, 2009), which discourages a company-wide dialogue on

data privacy due to fragmented data structures between departments (Kim et al., 2016). A customer-centric company, however, is focused on the needs of individual customer groups and can deploy resources across departments to meet them more efficiently (Lessmann & Voß, 2009; Sheth et al., 2000).

Finally, in order to eliminate the current information asymmetry in the data exchange between customers and companies (Acquisti & Varian, 2005; Eastlick et al., 2006; Varian, 1996), marketers need to be able to reach out to their customers and proactively educate them about potential opportunities and threats beyond their privacy policies (Milne & Bahl, 2010). This is only possible if data processing endeavours are valued individually and that this value creation is reflected in the company's performance measures (Lamberti, 2013).

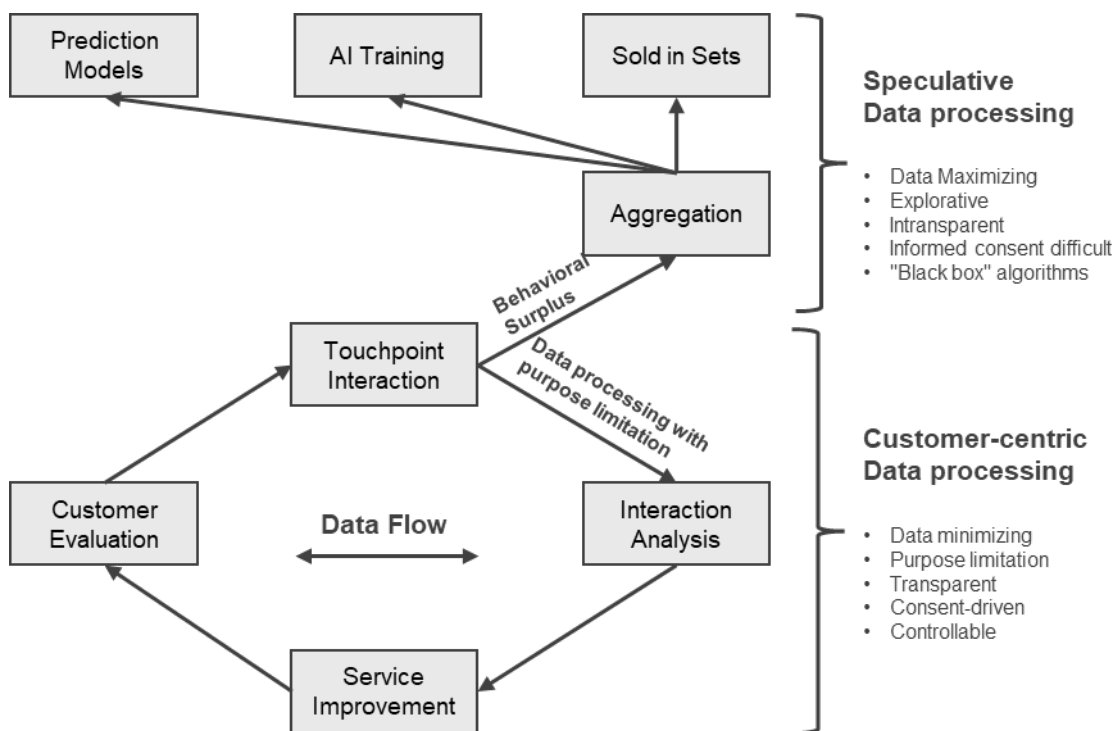


Figure 4-1 Customer-oriented and speculative data flows (adapted from Zuboff, 2019)

Responsible and customer-centric

In recent years, The market power of digital platforms such as Amazon has vacated the meaning of customer centricity. Instead of a collaborative fulfilment of the customer's "job-to-be-done," products and services are created for a multitude of data supply chains under the guise of customer centricity. The benefits of the data collected are rarely transferred directly and to the full extent to these same customers (Acquisti et al., 2020, p. 747). The collection and aggregation of such data surplus is still propagated too often, especially in marketing, despite

tougher data protection laws. Yet, some developments already point to the lucrative return to a privacy-oriented customer centricity:

- Customers across the world have an innate need for (digital) privacy that is currently not being met by most data-collecting companies (Lombardi & Ciceri, 2016; Newell, 1995; Oulasvirta et al., 2012).
- The erosion of data privacy through AI-driven (marketing) technologies (Fast & Jago, 2020; Reinsel et al., 2018) increases both the demand for privacy and the opportunity for competitive differentiation by using privacy as a strategic focal point (Palmatier & Martin, 2019).
- Customers' need for privacy is inadequately met by relying on self-regulation through a reactive, compliance-driven privacy strategy (Acquisti et al., 2020; Slepchuk & Milne, 2020; Solove, 2013, 2021; Varian, 1996). This is because under prevailing law, obtaining customer consent is easy, even with guiding design, while using protective technologies involves further resources (i.e., time and money) from the customer's perspective (Nouwens et al., 2020; Waldman, 2020).
- Marketing as a function has the capabilities to pursue a proactive privacy strategy (Palmatier & Martin, 2019; Rapp et al., 2009), while marketing theory (with customer centricity) enables the creation of an overarching evaluation framework for privacy strategies (Gotsch & Schögel, 2021).
- It has already been shown that a sustainable and proactive approach to privacy concerns has benefits in the areas of legal safeguarding (Solove, 2013), resource and talent management (Anhalt-Depies et al., 2019), branding (Fazzini, 2019; McGee et al., 2017) and the collection of high-quality customer data (Wang & Yu, 2015).

With customer-centric privacy strategies, companies in select markets are thus more likely to sustainably meet the increasing demand for data privacy and gain a competitive first mover advantage (Martin & Murphy, 2017, p. 152).

Several companies have already started to disrupt their industry's standard on data processing. Even cross-industry initiatives, such as the Privacy Icons Association launched by Migros, Swisscom, SBB, and Credit Suisse, show how comparatively simple means can be used to increase the transparency of data requests (Hotz & Glatthaar, 2020). Start-ups for so-called data clean rooms like Decentriq (Sturzenegger, 2021) or for synthetic data like Statice (Statice.ai, 2021) prove that even privacy-preserving collaborations between companies are possible. In a similar vein, the messenger app Threema, with its consistent data protection branding and focus, has managed to replace competitors such as WhatsApp as the permitted communication channel for the Swiss army (Hollenstein & Novak, 2022).

It is up to such future-oriented companies to prove that data-driven marketing and data privacy need not be contradictory. This requires a return to the promise of customer centricity: aligning with the needs of the customer rather than the value of customer data.



Figure 4-2 Customer-oriented view of data protection (based on Gotsch & Schögel, 2021)

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, 30(4), 736–758. <https://doi.org/10.1002/jcpy.1191>
- Acquisti, A., & Varian, H. R. (2005). Conditioning Prices on Purchase History. *Marketing Science*, 24(3), 367–381. <https://doi.org/10.1287/mksc.1040.0103>
- Amazon. (2021). *Our mission*. About Amazon. <https://www.aboutamazon.co.uk/uk-investment/our-mission>
- Amazon, R. R. (2018). Machine Learning @ Amazon. *SIGIR '18: The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval*, 1337–1338. <https://doi.org/10.1145/3209978.3210211>
- Anhalt-Depies, C., Stenglein, J. L., Zuckerberg, B., Townsend, P. M., & Rissman, A. R. (2019). Tradeoffs and tools for data quality, privacy, transparency, and trust in citizen science. *Biological Conservation*, 238, 1–7. <https://doi.org/10.1016/j.biocon.2019.108195>
- Bettencourt, L. A., Lusch, R. F., & Vargo, S. L. (2014). A Service Lens on Value Creation: Marketing's Role in Achieving Strategic Advantage. *California Management Review*, 57(1), 44–66.
- Burgess, M. (2021, September 4). *Why Amazon's £636m GDPR fine really matters* | WIRED UK. Wired. <https://www.wired.co.uk/article/amazon-gdpr-fine>
- Chen, H. S., & Jai, T.-M. (Catherine). (2019). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal*, 1–17. <https://doi.org/10.1080/02642069.2019.1603296>
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining Knowl Discov*, 7, 1211. <https://doi.org/10.1002/widm.1211>
- Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the Brand: Evaluating the Cost of Security Breach from a Marketer's Perspective. *American Journal of Management*, 11(1), 59–68. <https://articlegate-way.com/index.php/JMDC/article/view/1644/1561>
- Christensen, C., Hall, T., Dillon, K., & Duncan, D. (2016, September). *Know Your Customers' "Jobs to Be Done."* Harvard Business Review. <https://hbr.org/2016/09/know-your-customers-jobs-to-be-done>
- Cisco. (2019). *Consumer Privacy Survey - The growing imperative of getting data privacy right*. <https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf>
- Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorell, X., & Reis, M. S. (2016). How Can SMEs Benefit from Big Data? Challenges and a Path Forward. *Quality and Reliability Engineering International*, 32(6), 2151–2164. <https://doi.org/10.1002/qre.2008>
- Day, G. S. (2003). Creating a Superior Customer-Relating Capability. *MIT Sloan Management Review*, 44(3), 77–82. https://repository.upenn.edu/marketing_papershttps://repository.upenn.edu/marketing_papers/427
- Denning, S. (2013). How Amazon practices the three laws of Agile management. *Strategy & Leadership*, 47(5), 36–41. <https://doi.org/10.1108/SL-07-2019-0104>
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. <https://doi.org/10.1016/j.jbusres.2006.02.006>
- Experian. (2020). Benchmark Report Benchmark report 2020 Global data management research. *Experian Data Management Research*.
- Fader, P. (2012). *Customer Centricity - Focus on the Right Customers for Strategic Advantage* (2nd ed.). Wharton Digital Press.
- Fast, N. J., & Jago, A. S. (2020). Privacy matters... or does It? Algorithms, rationalization, and the erosion of concern for privacy. *Current Opinion in Psychology*, 31(2), 44–48. <https://doi.org/10.1016/j.copsyc.2019.07.011>
- Fazzini, K. (2019). *Apple's big bet on privacy has risks*. CNBC. <https://www.cnbc.com/2019/01/10/apple-privacy-big-bet-risks.html>
- Galbraith, J. R. (2005). *Designing the customer-centric organization: a guide to strategy, structure, and process* (1st ed.). Jossey-Bass.
- 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>

- Gulati, R., & Oldroyd, J. B. (2005a). The Quest for Customer Focus. *HBR*, 92(April), 92–1010. <https://hbr.org/2005/04/the-quest-for-customer-focus>
- Gulati, R., & Oldroyd, J. B. (2005b). The Quest for Customer Focus. *Harvard Business Review*. <https://hbr.org/2005/04/the-quest-for-customer-focus>
- Gummesson, E. (2008). Extending the service-dominant logic: from customer centricity to balanced centricity. *Journal of the Academy of Marketing Science*, 36, 15–17. <https://doi.org/10.1007/s11747-007-0065-x>
- Habel, J., Kassemeyer, R., Alavi, S., Haaf, P., Schmitz, C., & Wieseke, J. (2020). When do customers perceive customer centricity? The role of a firm's and salespeople's customer orientation. *Journal of Personal Selling & Sales Management*, 40(1), 25–42. <https://doi.org/10.1080/08853134.2019.1631174>
- Haugen, F. (2021, October 5). *Facebook Whistleblower Frances Haugen Opening Statement*. C-Span Video. <https://www.youtube.com/watch?v=Lq32sECQ9g8>
- Hollenstein, E., & Novak, E. (2022, January 5). *Threema wird Pflicht im Militär – Schweizer Armee verbietet Whatsapp*. Tagesanzeiger. <https://www.tagesanzeiger.ch/schweizer-armee-verbietet-whatsapp-631981142651>
- Hotz, J., & Glatthaar, M. (2020, November 30). Verkehrsschilder für den Datenschutz – Privacy Icons. *Privacy Icons*. <https://privacy-icons.ch/verkehrsschilder-fuer-den-datenschutz/>
- Howe, D. C., & Nissenbaum, H. (2017). Engineering Privacy and Protest: a Case Study of AdNauseam. *CEUR Workshop Proceedings*, 57–64.
- Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56–59. <https://doi.org/10.1109/MC.2018.3191268>
- Janakiraman, R., Lim, J. H., & Rishika, R. (2017). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing*, 82(2), 85–105. <https://doi.org/10.1509/jm.16.0124>
- Jindal, R. P., Gauri, D. K., Li, W., & Ma, Y. (2021). Omnichannel battle between Amazon and Walmart: Is the focus on delivery the best strategy? *Journal of Business Research*, 122, 270–280. <https://doi.org/10.1016/J.JBUSRES.2020.08.053>
- Kats, R. (2020, March 1). Amazon's Move to One-Day Shipping Propels Sales - Insider Intelligence Trends, Forecasts & Statistics. *EMarketer Insider Intelligence*.
- Kim, J., Ha, H., Chun, B. G., Yoon, S., & Cha, S. K. (2016). Collaborative analytics for data silos. *2016 IEEE 32nd International Conference on Data Engineering, ICDE 2016*, 743–754. <https://doi.org/10.1109/ICDE.2016.7498286>
- Krämer, A. (2018). Customer Centricity und deren Monetarisierung am Beispiel Amazon Prime. *Marketing Review St. Gallen*, 4, 12–20.
- Lamberti, L. (2013). Customer centricity: the construct and the operational antecedents. *Journal of Strategic Marketing*, 21(7), 588–612. <https://doi.org/10.1080/0965254X.2013.817476>
- Latinovic, Z., & Chatterjee, S. C. (2019). Customer Centricity in the Digital Age. *MIT Sloan Management Review, Summer 2019*, 60(4), 3. <https://sloanreview.mit.edu/article/customer-centricity-in-the-digital-age/>
- Lee, J., Sridhar, S., & Palmatier, R. W. (2015). Customer-centric org charts aren't right for every company. *Harvard Business Review*.
- Lee, J. Y., Sridhar, S., Henderson, C. M., & Palmatier, R. W. (2015). Effect of customer-centric structure on long-term financial performance. *Marketing Science*, 34(2), 250–268. <https://doi.org/10.1287/mksc.2014.0878>
- Lessmann, S., & Voß, S. (2009). A reference model for customer-centric data mining with support vector machines. *European Journal of Operational Research*, 199(2), 520–530. <https://doi.org/10.1016/J.EJOR.2008.12.017>
- Liang, T.-P., & Tanniru, M. (2006). Customer-Centric Information Systems. *Journal of Management Information Systems*, 23, 9–15. <https://doi.org/10.2753/MIS0742-1222230301>
- 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>
- Lombardi, D. B., & Ciceri, M. R. (2016). More than defense in daily experience of privacy: The functions of privacy in digital and physical environments. *Europe's Journal of Psychology*, 12(1), 115–136. <https://doi.org/10.5964/ejop.v12i1.948>
- 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>

- Mcgee, H., Hsieh, N., & Mcara, S. (2017). Apple : Privacy vs . Safety (A). *Harvard Business School*, November, 1–34. <https://store.hbr.org/product/apple-privacy-vs-safety-a/316069?sku=316069-PDF-ENG>
- Meiseberg, B. (2016). The Effectiveness of E-tailers' Communication Practices in Stimulating Sales of Niche versus Popular Products. *Journal of Retailing*, 92(3), 319–332. <https://doi.org/10.1016/J.JRETAI.2016.02.002>
- Microsoft. (2020). Customer centricity - A key priority across all lines of business. *Microsoft Dynamics*.
- Milne, G. R., & Bahl, S. (2010). Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis. In *Journal of Public Policy & Marketing* (Vol. 29, Issue 1).
- Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology*, 15(2), 87–104. [https://doi.org/10.1016/0272-4944\(95\)90018-7](https://doi.org/10.1016/0272-4944(95)90018-7)
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Association for Computing Machinery (Ed.), *CHI* (pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376321>
- Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N., & Myllymäki, P. (2012). Long-term Effects of Ubiquitous Surveillance in the Home. *UbiComp*, 41–50.
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Park, Y. J., Chung, J. E., & Shin, D. H. (2018). The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. *American Behavioral Scientist*, 62(10), 1319–1337. <https://doi.org/10.1177/0002764218787863>
- Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, 2(3), 175–196. <https://doi.org/10.1111/j.1756-2589.2010.00052.x>
- Plangger, K., & Montecchi, M. (2020). Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, 50, 32–44. <https://doi.org/10.1016/j.intmar.2019.10.004>
- Prahalad, C. K., & Ramaswamy, V. (2004). Co-creation experiences: The next practice in value creation. *Journal of Interactive Marketing*, 18(3), 5–14. <https://doi.org/10.1002/dir.20015>
- Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). Advertising and Consumer Privacy: Old Practices and New Challenges. *Journal of Advertising*, 38(4), 51–61. <https://doi.org/10.2753/JOA0091-3367380404>
- Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World - From Edge to Core*.
- Riedmann-Streitz, C. (2018). Redefining the Customer Centricity Approach in the Digital Age. *International Conference of Design, User Experience, and Usability*, 10918 LNCS, 203–222. https://doi.org/10.1007/978-3-319-91797-9_15
- Ritala, P., Golnam, A., & Wegmann, A. (2014). Coopetition-based business models: The case of Amazon.com. *Industrial Marketing Management*, 43(2), 236–249. <https://doi.org/10.1016/J.INDMARMAN.2013.11.005>
- Rossmann, J. (2019). *Think Like Amazon: 50 1/2 Ideas to Become a Digital Leader*. McGraw-Hill Education.
- Salesforce. (2019). *State of the connected customer*.
- Shah, D., Rust, R. T., Parasuraman, A., Staelin, R., & Day, G. S. (2006). The path to customer centricity. *Journal of Service Research*, 9(2), 113–124. <https://doi.org/10.1177/1094670506294666>
- Sheth, J. N., Sisodia, R. S., & Sharma, A. (2000). The Antecedents and Consequences of Customer-Centric Marketing. In *Journal of the Academy of Marketing Science* (Vol. 28, Issue 1).
- Slepchuk, A. N., & Milne, G. R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, 31, 89–93. <https://doi.org/10.1016/j.copsyc.2019.08.007>
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, 89(1), 1–51.
- Statice.ai. (2021). The path to data anonymity. *Statice White Paper*.
- Sturzenegger, D. (2021, November 11). *New features and technical documentation for Decentriq's data clean rooms*. Decentriq Blog. <https://blog.decentriq.com/product-update-new-features-and-technical-documentation-for-decentriqs-data-clean-rooms/>
- Ulag, W. (2018). The journey towards customer centricity and service growth in B2B: a commentary and research directions. *AMS Review*, 8(1), 80–83. <https://doi.org/10.1007/S13162-018-0119-X>
- Vargo, S. L., & Lusch, R. F. (2004). Evolving to a New Dominant Logic for Marketing. *Journal of Marketing*, 68(1), 1–17. <https://doi.org/10.1509/JMKG.68.1.1.24036>

- Varian, H. R. (1996). Economic Aspects of Personal Privacy. In W. H. Lehr & L. M. Pupillo (Eds.), *Cyber Policy and Economics in an Internet Age* (1st ed., Vol. 43, pp. 127–137). Springer. https://doi.org/https://doi.org/10.1007/978-1-4757-3575-8_9
- Wagner, C., & Majchrzak, A. (2006). Enabling Customer-Centricity Using Wikis and the Wiki Way. *Journal of Management Information Systems*, 23(3), 17–43. <https://doi.org/10.2753/MIS0742-1222230302>
- Waisberg, D., & Kaushik, A. (2009). Web Analytics 2.0: Empowering Customer Centricity. *SEMJ*, 2(1).
- Wakefield, J. (2021, November 4). *Facebook's metaverse plans labelled as "dystopian" and "a bad idea"* -. BBC News. <https://www.bbc.com/news/technology-59154520>
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the "privacy paradox." *Current Opinion in Psychology*, 31(2), 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- Wang, Z., & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Computer Law and Security Review*, 31(6), 782–792. <https://doi.org/10.1016/j.clsr.2015.08.006>
- West, D., & Wildeman, R. C. (2009). *Product-Centric Development Is A Hot New Trend*.
- Wind, J., & Rangaswamy, A. (2001). Customerization: The next revolution in mass customization. *Journal of Interactive Marketing*, 15(1), 13–32. [https://doi.org/10.1002/1520-6653\(200124\)15:1<13::aid-dir1001>3.0.co;2-#](https://doi.org/10.1002/1520-6653(200124)15:1<13::aid-dir1001>3.0.co;2-#)
- Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, 28(1), 10–29. <https://doi.org/10.1177/1095796018819461>

5. Article

Gotsch, M. & Schögel, M. (2021). Addressing the Privacy Paradox on the Organisational Level – Review and Future Directions. *Management Review Quarterly*, 1-34.

Addressing the Privacy Paradox on the Organisational Level - Review and Future Directions

Mauro Luis Gotsch, MA HSG

mauro.gotsch@unisg.ch / ORCID: 0000-0002-5319-2347

Institute of Marketing, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

Prof. Dr. Marcus Schögel

marcus.schoegel@unisg.ch

Institute of Marketing and Customer Insight, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

CRedit author statement:

Mauro Gotsch: Methodology, Conceptualisation, Formal Analysis, Investigation, Writing – Original Draft, Visualisation, Data Curation, Writing – Review & Editing, Validation

Marcus Schögel: Supervision, Validation, Resources, Project Administration, Funding Acquisition

Abstract

The discrepancy between informational privacy attitudes and actual behaviour of consumers is called the “privacy paradox”. Researchers across disciplines have formulated different theories on why consumers’ privacy concerns do not translate into increased protective behaviour. Over the past two decades multiple differing explanations for the paradox have been published. However, authors generally agree that companies are in a strong position to reduce consumers’ paradoxical behaviour by improving their customers’ informational privacy. Hence, this paper aims at answering the question: How can companies address the privacy paradox to improve their customers’ information privacy? Reviewing a sample of improvement recommendations from 138 papers that explore 41 theories in total, we determined that companies can generally align their privacy practices more closely with customers’ expectations across 4 inter-connected managerial processes: (1) strategic initiatives, (2) structural improvements, (3) human resource management, and (4) service development. The findings of this systematic literature review detail how companies can address both the rational and irrational nature of the privacy decision-making process. Furthermore, we propose a dynamic model able to identify weaknesses and strengths in companies’ privacy orientation.

Keywords: *Privacy paradox, Information privacy, Privacy concern, Decision-making, Privacy strategy, Systematic literature review*

Introduction

The “Social Media Age of Privacy” (Yun et al., 2019, p. 573) started about 20 years ago . With it came an increased concern regarding personal information privacy, commonly defined as the concern of consumers about companies’ privacy practices which could compromise their ability to control their personal information (Smith et al., 1996, p. 191). This escalation of concerns continues to this day, with 81% of U.S adults feeling like “they have no or little control over the data companies collect from them” and thinking the “potential risks of companies collecting data about them outweigh the potential benefits” (Auxier et al., 2019, p. 4). However, early studies observed that customers’ stated high privacy concerns did neither translate into a lower willingness to share personal data (Acquisti, 2004) nor into increased protective behaviour (Norberg & Horne, 2007). This value-action gap, which Barnes (2006) popularised under the term “privacy paradox”, is still a prevalent topic amongst privacy researchers across various disciplines.

In their systematic literature review, Barth & de Jong (2017) examined 32 decision models from journal articles on the topic of the privacy paradox. They arrived at the conclusion that consumers’ privacy behaviour is probably only predictable to a limited extent, as several moderating variables influence customer behaviour. For this reason, the recommendation was made to orientate data-intensive services more strongly towards the customers’ needs: “The creation of data protection awareness in combination with tools that support users in their data protection decisions should help them to avoid paradoxical behaviour”(Barth & de Jong, 2017, p. 1051). Martin & Murphy (2017, p. 153) also support this conclusion in their literature review on the role of privacy in marketing: “Although a coherent subset of theoretic approaches has provided a robust understanding through deep insights, in some respects this focus has limited our view of privacy too much to individual silos (...) Future research directions should embody a holistic approach, blending the many consumer, organisational, ethical, and legal concerns that feature in contemporary data privacy questions.” In other words, companies are in a strong position to reduce consumers’ paradoxical behaviour by improving their customers’ informational privacy. Despite the prevalent recommendation for companies to adapt a “more proactive approach” (Dinev et al., 2015, p. 652), current literature across disciplines does not sufficiently address the privacy paradox on an organisational level . Hence, this paper aims at answering the following question: How can companies address the privacy paradox and improve their customers’ information privacy?

In this paper, we review 138 papers with 41 different theoretical approaches to the privacy paradox and evaluate their recommendations on what companies could learn from their studies. We begin by staking out our theoretical position and its importance for data collecting companies. Afterwards, we detail our methodological approach and the steps taken in searching and appraising the past twenty years of privacy paradox research. Our findings elaborate on how the recommendations of these papers can be structured in order to create a dynamic model of how to address the privacy paradox on the organisational level. We conclude the

article by discussing our review's contributions and limitations and finish by identifying avenues for future research.

Theory

Greenaway & Chan (2005, p. 172) identified three "levels" information privacy research is usually conducted on: the "personal" level (consumer research), the "sectoral/national" level and the underrepresented "organisational" level. The first level is the most well-represented within information privacy research, as consumer concerns about and reactions towards privacy are directly observable (Amiri et al., 2018; Barth & de Jong, 2017; Feng & Xie, 2019; Kokolakis, 2017). The sectoral level is focused on policies and regulations intended to protect privacy (e.g. Citron, 2009; Mcneely & Hahm, 2014; Richards, 2008; Whitman, 2004). Greenaway & Chan (2005, p. 190) suggested the "middle" level of the "organisational view" as a necessary addition, reasoning that "organisations are increasingly required to develop and implement information privacy policies and programs" to protect consumer privacy. However, even though "information privacy research can be conceptualised as a multi-level concept", it "is very rarely researched as such" (Bélanger & Crossler, 2011, p. 1028) as most research either starts from or is concerned with addressing challenges arising on the personal level. We argue in line with both new and old marketing research on the topic (K. D. Martin & Murphy, 2017; Palmatier & Martin, 2019, p. 58; Sarathy & Robertson, 2003; H. Wang et al., 1998): To tackle the increasing privacy vulnerability of consumers, privacy processes and outcomes should be increasingly studied on the organisational level.

Theoretical Gap

The lack of research considering the organisational level can be illustrated by the large number of literature reviews featuring extensive insights on the personal or sectoral level, while either completely omitting the organisational level from their research question (e.g. R. Bandara et al., 2017) or only summarizing the effect organisational privacy practices have on individuals (e.g. Beke et al., 2018). The few reviews explicitly addressing the organisational level note the "surprisingly" low number of "studies on the organisational level" (Bélanger & Crossler, 2011, p. 1029) while "advocating for a holistic way of thinking about organisational use of consumer data" (K. D. Martin & Murphy, 2017, p. 153).

Of course, this is not to suggest that previous privacy research offers no insights on how to address the privacy paradox on the organisational level. As Bélanger & Crossler (2011, p. 1027) note, the results of these studies offer a variety of implications on other levels. Yet, so far, the

majority of studies are not conducted on the organisational level and the plethora of implications from results on other levels have not been systematically analysed. This paper's theoretical contribution is centred specifically around these implications.

The lack of papers from an organisational perspective and the inconsistent measuring of many privacy constructs (Smith et al., 2011, p. 997) make it difficult to conduct a meta-analysis. Yet, by focusing on recommendations arising from papers basing their insights on established theoretical frameworks, we are able to sketch out a dynamic model which has the potential to serve as a unifying basis upon which future studies on the organisational level can be built.

The Privacy Paradox

Six years ago, Dienlin & Trepte (2015, p. 295) declared the privacy paradox to be “a relic of the past”. Their argument was based on the “principle of compatibility” – stating that attitudes such as privacy concerns serve as better predictors for behaviour when measured at the same level of specificity (Ajzen, 2011; Ajzen & Fishbein, 1970, 1977). In their own words: “Broad and abstract attitudes such as privacy concerns are less likely to predict narrow behaviours such as the use of public versus private profiles on SNSs [social networking systems]” (Dienlin & Trepte, 2015, p. 286). They conclude that, if the level of specificity is matched, “paradoxical” behaviour will disappear. This argument highlights an old problem; as Smith et al. (2011, p. 997) also noted: “Because of the near impossibility of measuring privacy itself (...), almost all empirical privacy research in the social sciences relies on measurement of a privacy-related proxy of some sort.” While this argument does justice to the highly contextual nature of individuals' privacy decision making (Mourey & Waldman, 2020), it is ultimately still based on the assumption of rational disclosure – i.e. only one part of the privacy paradox.

Individual choice can only explain the observed paradoxical behaviour under a rather narrow “zone of effectiveness” (Reidenberg et al., 2014, p. 517) where requests to share data are infrequent, the risks of disclosure are comprehensible and consumers have an incentive to take requests seriously (Richards & Hartzog, 2019, p. 1492). As long as the “irrational” side of individual privacy decisions (Gambino et al., 2016; S. Sundar & Kim, 2019; S. S. Sundar et al., 2013) and the structural hurdles to informed consent (Mourey & Waldman, 2020; Reidenberg et al., 2014; Richards & Hartzog, 2019; Solove, 2013, 2021; Waldman, 2020) are not taken into account, our understanding of the privacy paradox remains incomplete.

Hence, addressing the privacy paradox on an organisational level necessitates the often demanded “holistic perspective” (Bélanger & Crossler, 2011, p. 1027; K. D. Martin & Murphy, 2017, p. 153), i.e. trying to unify the rational, irrational and structural approaches in order to reduce the discrepancy between expressed privacy concerns and actual privacy behaviour. Any model attempting to do so must first consider the well-established theories used to

“solve” the privacy paradox on a personal and societal level. From their arguments, a theoretical basis for organisational privacy research can be drawn.

Why Should Companies Care?

While there are many scientific and ethical reasons to research information privacy, from a firm’s perspective the goal is to “first satisfy their customers” (Gunther, 2009, p. 18). Hence, trying to reduce the discrepancy between customers’ globally increasing demands for more privacy (Clemons et al., 2014) and the predicted rise in data collection needs of new (marketing) technologies (Palmatier & Martin, 2019, p. 58) should be a central concern of marketers. Big data technologies have a high potential for use in marketing, but rely heavily on consumer trust (C. Bauer & Lasinger, 2014; C. Bauer & Strauss, 2016; Michler et al., 2020). Accordingly, by building the necessary capabilities to address the privacy paradox (i.e., aligning the rational, irrational and structural privacy conditions with the customers’ expectations), companies could gain a strategic advantage in the market today (Li, Yu, & He, 2019; Seo et al., 2018). These capabilities have already been linked to higher trust and customer satisfaction (Dehghanpouri et al., 2020; Eastlick et al., 2006; Featherman et al., 2010; Wu et al., 2012), willingness to share data (Dinev & Hart, 2006; Hui et al., 2007; Morlok, 2016), damage control for data breaches (A. Malhotra & Malhotra, 2011) and even firm performance (K. D. Martin et al., 2017).

However, since no cohesive overarching framework of how to address the privacy paradox on an organisational level exists (Palmatier & Martin, 2019, p. 180), different organisational capabilities were examined and measured across all of these studies. Additionally, most of these studies looked at individual privacy measures (e.g., transparency and control) and their effects on customer behaviour. So far, there is little comparability between these results. Nevertheless, taken together, they at least provide enough evidence to suggest a “first-mover advantage on consumer privacy protection” (K. D. Martin & Murphy, 2017, p. 152).

Method

We performed a literature review of publications researching the privacy paradox and offering implications or recommendations for companies on how to address it. The review aimed to

- (1) highlight the different theories used in the literature to answer the question posed in the introduction;
- (2) organise and classify said recommendations according to the management process they intend to impact;

(3) create a dynamic model able to classify future recommendations and identify weaknesses and strengths in companies' privacy orientation; and

(4) identify gaps in the current literature to indicate future research directions.

The review phases conducted correspond to the four phases described by Okoli (2015, p. 884): planning; literature selection; data extraction; and execution (see fig. 1). This method was chosen as it synthesises the methodology from diverse fields and allows for the analysis of both quantitative and qualitative results. This was necessary as the reviewed papers originated from different fields, including marketing, information system science, psychology, socio-psychology, ethics and law and used both qualitative and quantitative research designs. Furthermore, Okoli's (2015, p. 905) process is designed to both assure rigor through reproducibility and increase the chance not to leave out any relevant literature. Additionally, to guide the qualitative nature of the data extraction in this review, the approach of Bandara et al. (2015, p. 160) was used, as recommended by Okoli (2015, p. 895), to supplement the overall structure.

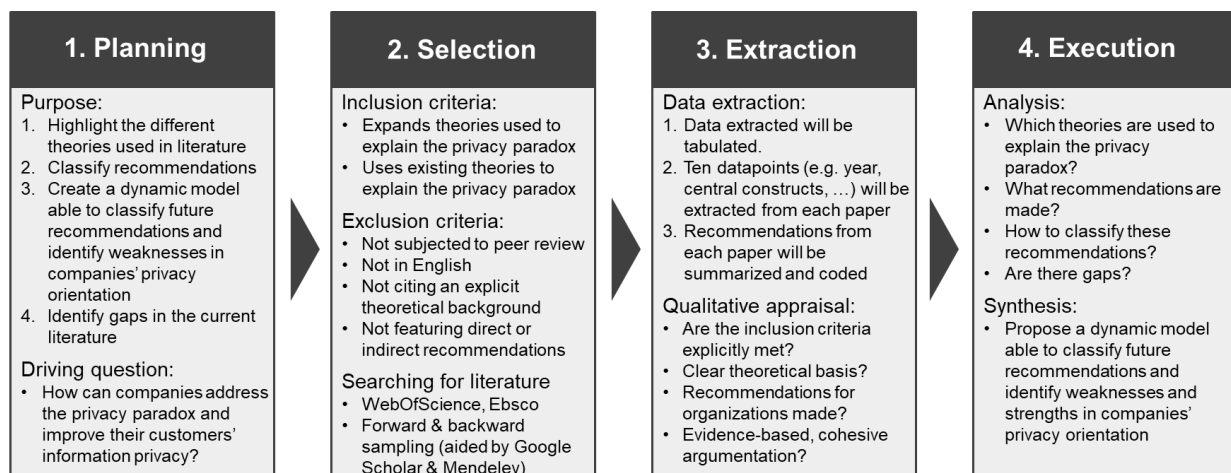


Figure 5-1 Guide to the four phases of a literature review (based on Okoli, 2015, p. 885)

Planning Phase

In the planning phase, the paper's four goals and the driving question of "How can companies address the privacy paradox to improve their customers' informational privacy" were defined. The systematic literature review was chosen due to the available wealth of information aimed at answering the privacy paradox across disciplines. Most of these papers feature recommendations on how addressing the paradox may help both customers and firms in the long run. However, since there is no cohesive overarching model to categorise these recommendations, the effects of privacy strategies are often measured through expressed privacy concerns (Dinev et al., 2012) and therefore lack comparability. Any model attempting to create a framework which would allow comparability between different privacy strategies must therefore draw

its conclusions from arguments derived from well-established theories which have been shown to have predictive power both in, and outside of, privacy research (see goals 1 and 2 of this review). Hence, the results of the review should guide managers in their endeavours to align their company's data collection practices with their customers' expectations as well as help researchers identify future research directions.

To coordinate and inform all researchers involved in the review process, a protocol based on Kitchenham & Charters (2007, p. 54) was drafted. Due to the comparatively small team size involved in this review, no further training steps were taken.

Selection Phase

The selection phase consists of defining a practical screening process with inclusion and exclusion criteria and utilizing these to search for relevant literature (Okoli, 2015, p. 893).

Our review considered papers published between January 1st 2001 and December 1st 2020. These dates were chosen to incorporate privacy research since the beginning of the "Social Media Age" of privacy, as this was the time period the privacy paradox was first considered as such (Yun et al., 2019, p. 573). To cover the broad spectrum of privacy literature across disciplines, we placed no restrictions on the chosen research method – as long as it aimed at expanding or using existing theory to find an answer to (a part of) the privacy paradox. Papers not explicitly mentioning the privacy paradox were not automatically excluded, as the term is not equally widespread across disciplines (see e.g. Child et al., 2009). However, we rejected any papers not subjected to peer review (i.e., most book chapters) or not written in English (to ensure equal comprehensibility for all researchers involved).

We utilised a hierarchical search strategy for the literature search process to capture relevant articles from multiple fields, starting with the most reliable sources. To this end, the databases Web of Science and EbscoHost were searched using the terms "privacy paradox" or "privacy behaviour" or "privacy protection" (or a combination thereof) in the title, abstract or keywords. These two platforms were prioritised due to their interdisciplinary nature and collection of peer-reviewed articles and conference proceedings. We repeated the process on Google Scholar to ensure we obtained a comprehensive selection of papers across multiple sources and disciplines. Since the search yielded 9'250 papers (often duplicated) even after applying all the exclusion criteria, only the topmost 100 articles were screened. This initial search yielded 456 papers – not counting duplicates. As recommended by Bandara et al. (2015, p. 184), we used backward and forward sampling to increase the quality of the sample overall. For backward sampling we used the references found in literature reviews and meta-analyses published in journals with an impact score higher than 2 across different disciplines (psychology, marketing, information system science, socio-psychology). Finally, forward sampling was carried out (using Mendeley & Google Scholar) for often-cited papers published in A or

A+ journals across the same disciplines (psychology, marketing, information system science, socio-psychology). The complete list came down to 538 papers to be screened.

The papers were screened manually. Papers neither citing an explicit theoretical background nor proposing a new theory to explain the privacy paradox (or a related question) as well as papers not proposing direct or indirect implications to improve privacy orientation at an organisational level were rejected. Whenever a paper had been published in more than one journal or conference report, only the most complete version was chosen. After two rounds of screening, the initial selection was reduced to 289 papers.

The selection process is illustrated in Fig. 2 to show “the initial number of identified studies and the number of studies eliminated at each stage of the literature search process” as recommended by Kuckertz & Block (2021, p. 3).

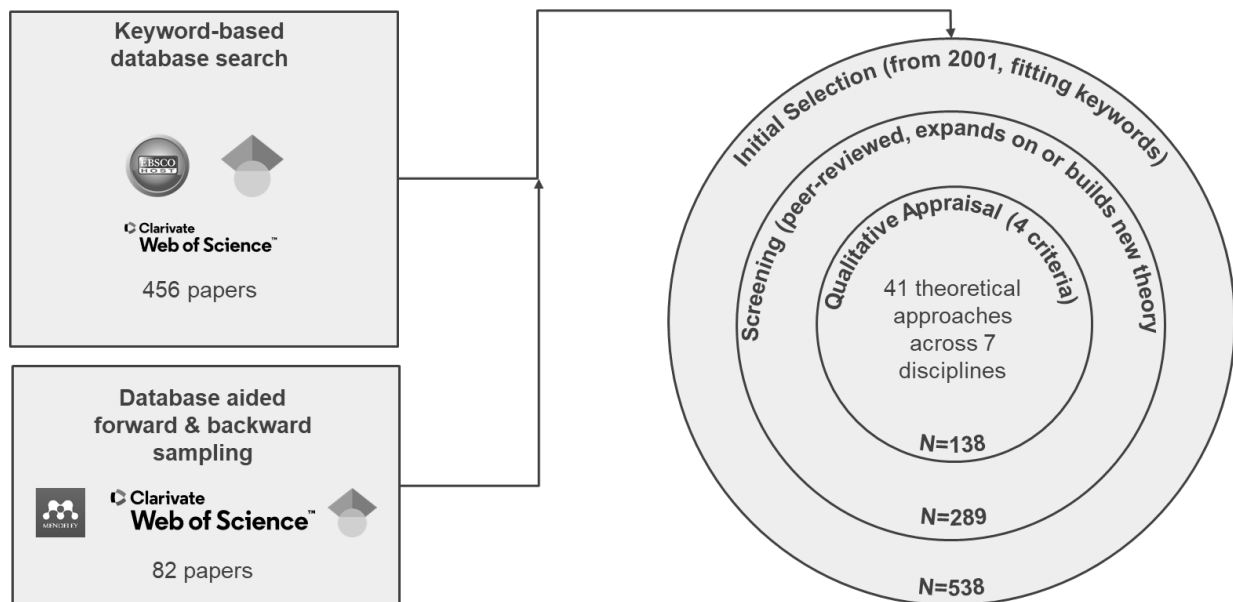


Figure 5-2 Literature selection process

Extraction Phase

During the extraction phase, the first data points are collected, and the selection of papers is further reduced through a qualitative appraisal of their content.

We extracted ten data points for each paper – amongst them identifiers such as the author and title, classifications such as research stream and theories cited, and the recommendations made to address the privacy paradox on an organisational level. The data per paper was extracted and tabulated by one researcher and checked by another one.

For the appraisal of quality, we used a qualitative approach in combination with a scoring system recommended by Kitchenham & Charters (2007, p. 53) to further refine the number of papers considered. This approach was chosen over a quantitative method to accommodate for the diverse nature of privacy research (i.e., different disciplines as well as research designs). The questions driving the appraisal were:

Question 1: Are the inclusion criteria explicitly defined in the paper?

- Yes – they are explicitly defined in the paper.
- Partially – the criteria are implicitly met.
- No – the inclusion criteria are neither met nor are they implicitly referable.

Question 2: Is the paper based on or expands on one or multiple clearly defined theory/theories?

- Yes – the theoretical approach is explicitly defined in the paper.
- Partially – the theoretical approach can be inferred from citations and/or variables used.
- No – the paper makes no mention to the chosen theoretical approach.

Question 3: Does the paper offer any practical implications on how to address the privacy paradox on an organisational level?

- Yes – the recommendations are clearly defined in their own paragraph.
- Partially – the recommendations can be inferred from the paper's conclusion.
- No – the paper offers neither recommendations nor inferences on how to address the privacy paradox on an organisational level.

Question 4: Are the recommendations within the paper based on evidence and a cohesive argumentation?

- Yes – the recommendations follow logically and directly from the paper's results.
- Partially – the recommendations follow logically from the paper's results.
- No – the recommendations are not connected to the paper's results.

"Yes" answers yielded 1 point, "partially", 0.5 points and "no", 0 points. All papers with one or more "nos" were rejected, and so were papers scoring no more than 2 points.

After this qualitative appraisal, the final sample comprised 138 papers which were considered for the execution phase.

Execution Phase

During the execution phase, the screened, selected, and scored papers are combined to “make comprehensive sense” (Okoli, 2015, p. 899) of their content.

As a first step, we aggregated a list of all the theories used to explain the privacy paradox. This was done to ensure that the intended model was based on established theories covering the rational, irrational and structural elements making up the privacy paradox. Among the 138 papers, 42 different theories across 7 academic disciplines were used. Other descriptive statistics, such as the years of publication, the research design, etc., were also summarised.

We coded the recommendations using the inductive process described by Bandara et al. (2015, p. 169) to capture the recommendations found in the literature to address the privacy paradox on an organisational level. The grounded theory approach was chosen to arrive at a clear data structure which could serve as the foundation for “a vibrant inductive model grounded in data” (Gioia et al., 2013, p. 22).

After an initial round of coding covering all the recommendations, the resulting codes and memos were surveyed. Codes which were sufficiently similar in terminology and meaning were merged. This led to a classification of thirteen second-order themes related to resolving the privacy paradox. Based on this codebook, the intercoder reliability was tested with unaffiliated PhD students, resulting in an intercoder reliability of 64.28 % (calculated according to the Holsti method; (Mao, 2018)). After discussing the results with the students, the descriptions in the codebook were updated and narrowed. A second round of testing with other researchers resulted in a 71.42% intercoder reliability, falling within an acceptable reliability window, especially considering the sample size and the possible number of codes per question (Hruschka et al., 2004, p. 317).

As a final step, we aggregated these 13 themes into four dimensions. To test their reliability, we asked three researchers to cluster the themes themselves based on the information in the codebook. The four resulting aggregate dimensions cover the managerial processes through which the privacy paradox can be addressed: (1) strategic initiatives; (2) structural improvements; (3) human resource (HR) management; and (4) service development (see fig. 3).

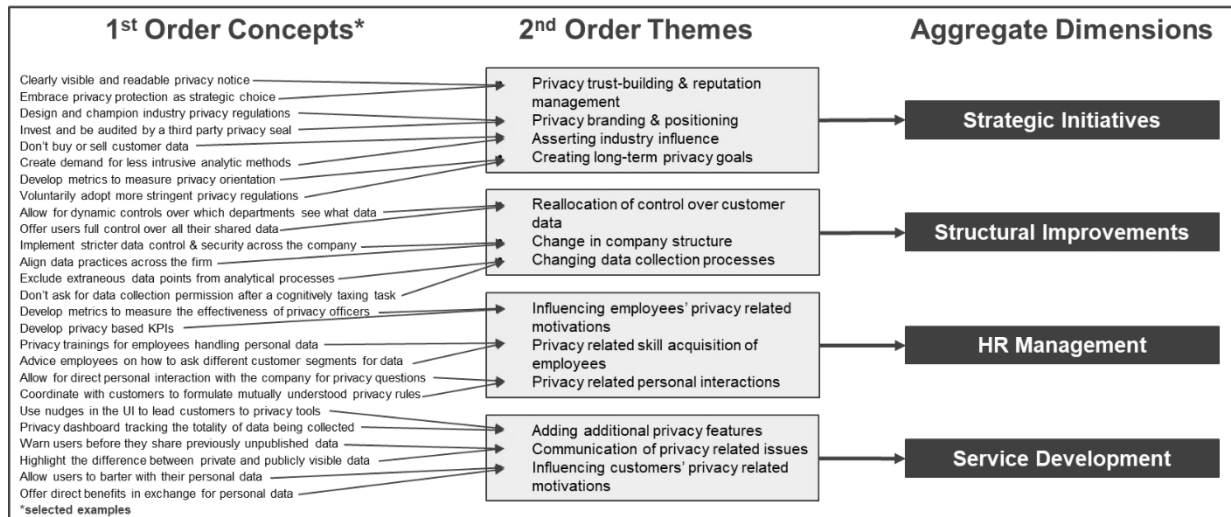


Figure 5-3 Data structure of the literature review (based on Gioia et al., 2013, p. 21)

This data structure was the basis which enabled a deeper exploration of the research question. Specifically, it guided the inquiry about (1) what recommendations are made to address the privacy paradox on an organisational level, (2) what (if any) gaps are there in the literature addressing the privacy paradox. The results and the connection between these themes are discussed in the following section.

Addressing the Privacy Paradox

The four aggregate dimensions mentioned above give a bird's eye view on what management processes the recommendations have an impact on. Together they form the parts of a dynamic model on how to address the privacy paradox on the organisational level. 'Addressing' hereby refers to the potential actions a company can take to align customers' privacy concerns and expectations with its actual data collection and processing activities.

The dynamic nature of the model is owed to the need to depict "complex changes relating to all aspects of an organisation" (Leonard & McAdam, 2004, p. 258) along a temporal axis while allowing for recursive behaviour (A. Bauer et al., 2000). The four dimensions represent four, sequentially interdependent approaches that help companies align their privacy practices more closely with their customers' expectations (see fig. 10).

The code for 'service development' is cited the most, with 67 citations within the sample, followed by the code for 'strategic initiatives' with 43 citations. 'Structural improvements' and 'HR management' appear 38 and 35 times, respectively. This is not surprising, considering that both psychology and marketing papers are often concerned with solutions to the paradox on a personal level, while sociology, information system science and management papers usually take a more structural approach. However, these numbers make no statement on the depth or

quality of the recommendations, nor do they provide any insight on the connection between the codes.

Most ‘solutions’ to the privacy paradox are either based on the assumption of a (semi-rational) “risk-benefit calculation” or the assumption of “little to no risk assessment” being possible for individuals (e.g. due to knowledge deficiencies) (Barth & de Jong, 2017, p. 1043). The presented model tries to bridge this gap by considering both explanations as valid, depending on the context. Hence, while individual aggregate dimensions might be more efficient in addressing one end of this dichotomy, they are formed to address both.

The connections between the aggregate dimensions and the second-order themes were inductively inferred from the source material by looking at the temporal or directional relationships used in the papers’ arguments. Wirtz & Lwin (2009, p. 204), for example, write on the subject of privacy goals: “Reducing privacy concerns may be sufficient for first-time or one-off transactions but will not be sufficient in relationship marketing, where an ever deeper understanding of customers, their background, motivations, and consumption patterns will enhance service delivery.” This passage is illustrative of how privacy goals inform trust-building activities while leading to more meaningful personal interactions and ultimately individual privacy features. Additionally, the regulatory focus theory used in the same paper suggests that customers learn from interactions with companies by reacting to the companies’ motivational systems, further cementing the view that companies’ actions should precede their customers’ reactions. Interpretations of such passages were collected in memos and later used to construct the model, the sub-models and their interrelationships, as suggested by Bandara et al. (2015, p. 170).

The sub-models and their most central connections are discussed in detail in the following paragraphs.

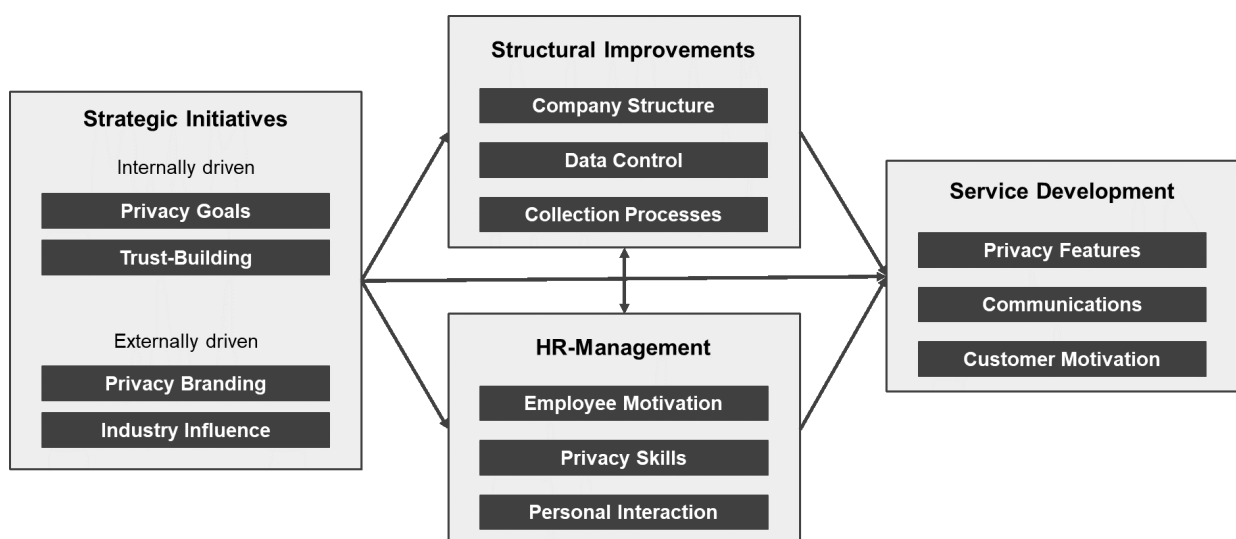


Figure 5-4 Relationship between the aggregate dimensions

Strategic Initiatives

The codes aggregated in this dimension all aim at addressing the privacy paradox through a strategic management focus, i.e., they seek to “guide those aspects of general management that have material effects on the survival and success of the business enterprise” as a whole and in the long term (Teece et al., 1997). Therefore, these recommendations should reduce paradoxical behaviour by “identifying difficult-to-imitate internal and external competences” (Teece et al., 1997) most likely to improve privacy capabilities within a firm or to signal high privacy standards to the market. In accordance with the “dynamic capabilities” perspective on strategic management, both externally focused strategic orientation and internally driven initiatives, such as setting privacy goals and engaging in trust-generating tactics (see fig. 4), form the basis all other privacy efforts have to build on (Zhou & Li, 2010).

Privacy Goals

The code for privacy goals is featured most prominently across marketing papers, with 8 out of the total of 11 citations. Their recommendations aim to eliminate paradoxical behaviour on the customer’s side by creating a privacy-aware culture within a company. It is usually framed as the first step to undertake, or as Lanier & Saini (2008, p. 28) put it: “Firms should look beyond being reactive, and instead embrace proactive approaches to managing privacy. Two areas in which this proactive adaptation can play out include organisational structure and strategy.” Thus, these strategies aid customers in their risk-benefit calculation by explicitly declaring privacy as being central to a company’s strategy (Lanier & Saini, 2008). A fitting example for this strategy is the crypto-messenger Threema, which is able to uphold a high standard of privacy since almost every one of its visible features is subservient to their users’ privacy (Bickelmann, 2021).

Alternatively, measures such as implementing internal fair data usage procedures (Son & Kim, 2008), investing heavily in the company’s information systems for added security and transparency (Teng et al., 2019), or “dismantling the epistemic and normative power of the claim that privacy is a matter of individual control of information” within one’s company culture (Hull, 2015, p. 99) address the structural hurdles causing the privacy paradox.

Taken together, the sample’s recommendations still give an incomplete picture of what constitutes an “aware” or “proactive” privacy culture. Future studies aimed at defining the “cultural web” of organisational privacy culture (rituals, symbols, heroes, values; Sun, 2008, p. 139) may enable us to measure their effects on customer privacy outcomes.

Trust-Building

Trust is one of the central variables affecting the success of privacy measures (Wirtz & Lwin, 2009), customer support of big data technologies (C. Bauer & Strauss, 2016; Michler et al., 2020) and the negative consequences of privacy turbulences for firms (K. D. Martin et al., 2017). While many of the recommendations in this review ultimately aim at earning the trust of customers, this code only addresses strategic initiatives with the explicit goal of building or rebuilding a basis of privacy-related and sustained trust. Since “trust is an important condition” (Dinev & Hart, 2006, p. 76) for any other privacy initiatives, it works in tandem with the long-term privacy goals to create the conditions for all other privacy efforts (see fig. 5).

However, most papers are unspecific in their recommendations on how to build such a basis. In general, the call for “investments in trust generating tactics” (Bansal et al., 2016, p. 13) is followed by recommendations to generate positive experiences first, e.g. by offering social interactions at crucial moments or by offering less (or non) data-intensive alternatives to new customers first (Guo et al., 2016).

In this way, customers are able to more realistically evaluate the potential benefits of a given service before deciding to disclose information, thus reducing paradoxical behaviour. Therefore, companies should actively measure their customers’ trust over time (Schade et al., 2018) or whether customers perceive their services and actions as “fair” (Wirtz & Lwin, 2009). Both aspects are indices of whether customers are able to perceive the benefits of a potential disclosure of data and whether internally driven privacy goals and externally driven privacy branding positions are successful.

Privacy Branding

Privacy branding helps address the privacy paradox by signalling a company’s stance on privacy in relation to its competitors. This either means positioning a product using higher or clearer privacy standards as a selling point (see e.g. Fazzini, 2019 for an example) or by using third party privacy seals to signal a privacy benchmark met by the company (Mothersbaugh et al., 2012). Either way, these efforts help customers make a more informed decision when evaluating offers. As Martin & Murphy (2017, p. 151) put it: “As companies continue to grapple with consumer information privacy questions, and as long as they compete in markets where privacy protections can be differentiated and are valued by customers, using privacy as a (branding) strategy remains a viable option to marketers.” Of course, privacy branding can only be effective in the long term if it is either backed up by a privacy seal which independently searches for and reports infringements (Hui et al., 2007) or if it is backed by long-term privacy efforts which are believably signalled to the market (Tang et al., 2008).

As such, privacy branding is highly dependent on existing trust-building initiatives and an internal vision for a company's privacy goals. Future research regarding the "drivers of brand extension success" (Völckner & Sattler, 2006, p. 18) or the "stretchability" (Ahluwalia, 2008, p. 337) of data collecting brands may shed further light on how privacy branding can contribute to aligning consumers' privacy expectations more closely with firms' data collection processes.

Industry Influence

The final code within this aggregate dimension combines recommendations regarding collaborations, joint ventures or agreements with vertical or horizontal industry participants to create more favourable privacy outcomes for customers. Similar to privacy branding, the goal is to address the privacy paradox by increasing signal accuracy regarding privacy practices. Hence, recommendations range from emphasizing privacy concerns as an entire industry (Oetzel & Gonja, 2011) to distancing the company from industry actors with questionable privacy practices (Casadesus-Masanell & Hervas-Drane, 2015; Hui et al., 2007). A current example are Apple's continued efforts to make Facebook's data tracking activities through their apps more transparent (Rodriguez, 2021). Since the negative spill-over effects of a privacy breach (e.g. through a data leak) are felt throughout the industry, such efforts aid both in generating trust and in believable privacy branding (K. D. Martin et al., 2017). Additionally, such efforts are often driven by a firm's internally defined privacy goals.

Furthermore, addressing structural barriers for customers trying to act on their privacy preferences also requires asserting influence on the respective industry sector. Common recommendations are pro-actively trying to establish an industry standard in privacy management (Karwatzki et al., 2017; Plangger & Montecchi, 2020) or creating an industry-wide demand for privacy friendly data collection processes (K. Martin, 2020).

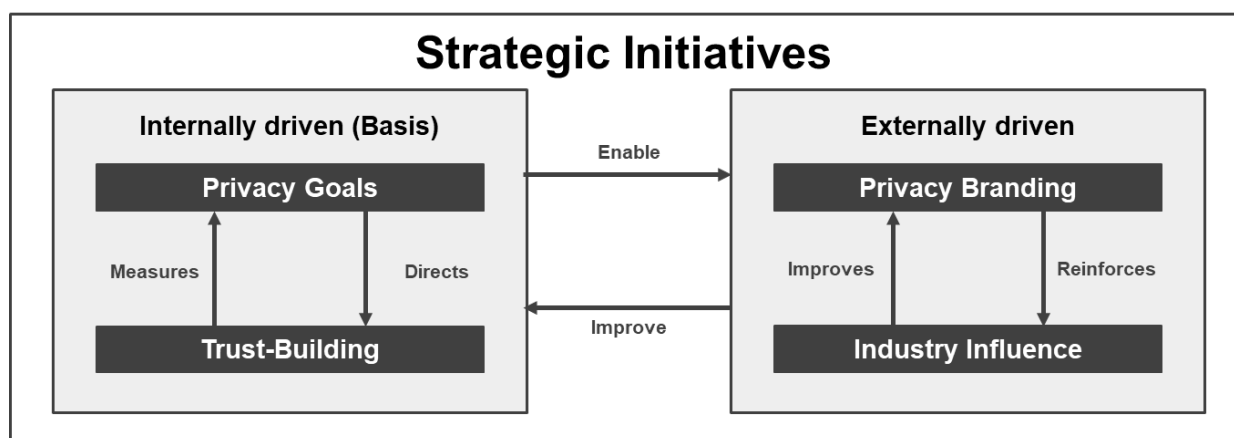


Figure 5-5 Connections between strategic initiative codes

Structural Improvements

An often-cited explanation for consumers' paradoxical behaviour is the one-sided power relationship when it comes to sharing personal data. The privacy calculus, resource exchange theory or social contract theory try to analyse privacy behaviour in terms of a market exchange: customers exchanging data for personalised services. Of course, this assumes that this exchange is initiated by the consumer and that it is based on a balanced power relationship. The codes aggregated under this dimension mostly try to address the prevalent power imbalance by changing the company structure. The connections between the individual codes largely follow the relationships found in information system science. Specifically, the company structure is essential "in leveraging the technological architecture" (i.e. the collection processes) to "encourage sharing and collaboration across boundaries within the organisation" (i.e. allowing the design of company-wide data control initiatives; see fig. 6) (Gold et al., 2001)

Company Structure

In order to adopt long-term privacy goals such as the 10 principles of the General Data Protection Regulation (GDPR; Art. 5–11), changes in company structure, hierarchy or business model often become necessary (see e.g. Teixeira et al., 2020). Recommendations like appointing and empowering a Chief Privacy Officer (CPO) (Solove, 2013), banning the transmission of highly personal information across departments (Hermalin & Katz, 2006), or abandoning revenue streams based on predatory data practices (Waldman, 2020) serve to enforce compliance with strategic privacy initiatives. This addresses the privacy paradox by more closely aligning the actual risk of disclosure with customers' expectations. Unfortunately, there are few structural recommendations which go beyond compliance and trying to work with the customer to profit from data collection while addressing the privacy paradox. The advice that comes closest is the suggestion by Child, Haridakis, & Petronio (2012, p. 1871) to take a more customer-centric approach to understand how they "experience privacy missteps, miscalculations, and regretted disclosures." Yet, in order to take that step, a more customer-centric company structure may be necessary to both collect data and address the diverse privacy needs of customers, which in turn would shape data control and collection processes.

Data Control

Most of the danger related to the loss of privacy stems from a loss of control over the flow of personal data (Nissenbaum, 2010). The code "Data Control" applies to all recommended changes in control structures (viewing-privileges, collection privileges, usage privileges, modification privileges) relating to customer data within a firm. The argumentation behind redistributing control over data usually stems from theories which postulate that customers will

protect themselves if given the chance to. Hence, recommendations for “consumer empowerment” through “control over their private data flow” (Prince, 2018, p. 30) are often repeated. Specifically, users should be able to “add, delete, and modify at will, the information in the organisation’s databases” (N. K. Malhotra et al., 2004, p. 350) – if possible for each individual datapoint (Ozdemir et al., 2017). These recommendations are in line with the GDPR’s stance on data ownership and help to resolve the privacy paradox by allowing customers to more effectively leverage their personal data. Hence, data control recommendations should also extend to who within a company is able to utilise customer data. Unfortunately, almost none of the recommendations give clear instructions on this matter. The advice that comes closest is the suggestion by Raento & Oulasvirta (2008) to offer customers the choice to modify their shared data depending on the target audience. A guideline on how to translate such a system into a corporate context to address the privacy paradox is largely missing.

At the same time, it is important to acknowledge that customers might not protect themselves even if they have the means to do so (see, e.g., protection motivation theory, third person effect theory, etc.). Hence, data control options can only ever be effective when paired with employee training and transparency efforts – as will be discussed in the following paragraphs.

Collection Processes

While the company structure largely determines where customer data is used, the collection processes determine how data is generated and ultimately utilised. This code incorporates all recommendations regarding the instruments, methods and processes used to collect, filter, aggregate and analyse customer data. Their goal is to address the privacy paradox in two ways: On the one hand, by trying to reduce biases and increase transparency at the point of disclosure, e.g. by not asking for customer data after cognitively taxing tasks (Alashoor & Baskerville, 2015; Barth et al., 2019) or by using just-in-time alerts to pro-actively warn users about the context of their disclosure before doing so (S. S. Sundar et al., 2020). On the other hand, the recommendations aim at reducing the actual risk of unwanted disclosure, e.g. by restricting data collection to specific time periods or contexts (Williams et al., 2016) or by focusing data collection only on highly specific but relevant data points (Choi et al., 2018). Outside the sample, literature concerned with data security and anonymisation already offers a wealth of concrete and implementable recommendations to address the privacy paradox by improving collection processes (see e.g. Freudiger et al., 2014; Mohassel & Zhang, 2017; Vergara-Laurens et al., 2017). Thus, the goal of further research should be to incorporate these insights into the larger organisational privacy discussion and expand on how they organise data control.

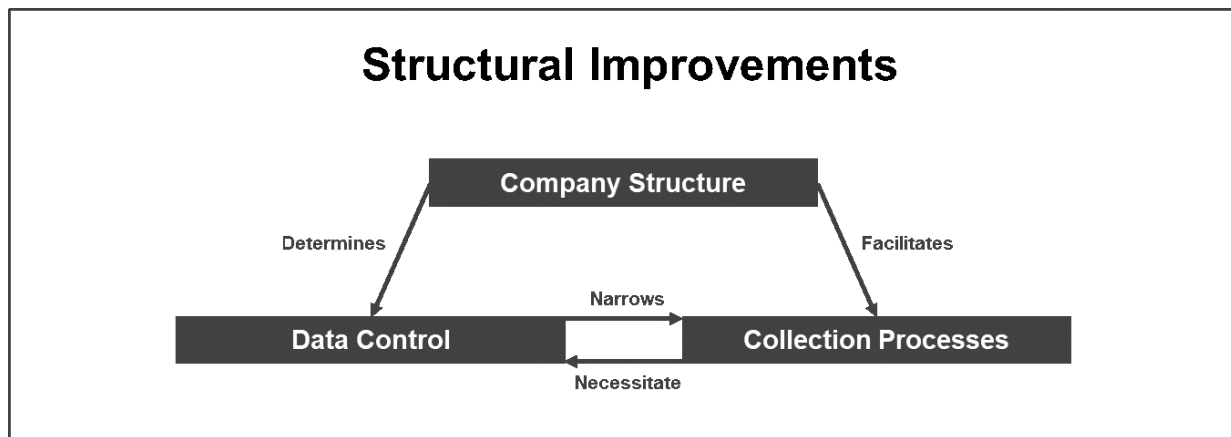


Figure 5-6 Connections between structural improvement codes

HR Management

Human resources, both as the workforce and as a business function, has long been recognised as an important strategic lever which creates value by “contributing directly to the implementation of operating and strategic objectives of firms” (Becker & Gerhart, 1996, p. 780). Value generation through (1) acquiring a “human capital resource pool” (i.e. skills and abilities), (2) the “specification of required human resource behaviours”, and finally measuring the (3) firm-level outcomes (Wright & McMahan, 1992, p. 299) work the same way in a privacy context. The three codes and their relationships within this dimension are analogous to this process (see fig. 7). A variety of (1) “privacy skills” is necessary to implement even the most basic privacy goals (e.g., having a CPO). Translating privacy goals into action requires codifying them in (2) “employee motivation” through KPIs or other incentive structures before the results can be studied and honed through (3) “personal interactions” with the customer. Since this process is aided by the company structure but not dictated by it, the two aggregate dimensions of “structural improvements” and “HR Management” are considered to have a joint effect on a company’s privacy outcomes (see fig. 4).

Privacy Skills

Privacy orientation requires a human resource capital pool that includes legal experts, data security experts, system engineers, privacy officers and many more. The recommendation to invest early in the human capital necessary to leverage privacy-enhancing technologies (e.g. anonymisation, statistical modelling, etc.) is repeated throughout the sample (Amiri et al., 2018; Bulgurcu et al., 2017; Kokolakis, 2017; Solove, 2013; Taneja et al., 2014). The benefits of reducing paradoxical behaviour by lowering the customers’ actual risk of exposure may be secondary for the company when compared to the potential strategic value conveyed by a skilled workforce of data security and analytics experts. As Anhalt-Depies et al. (2019, p. 7)

put it: “It is possible to provide high-quality, spatially explicit data (...) while protecting sensitive information in ways that provide protections to privacy and resources. However, doing this well requires significant investment in (understanding) technological solutions, data policies, and transparency efforts.”

Moreover, the acquisition of soft skills is not to be neglected, especially in companies with close customer contact. Therefore, recommendations such as those by Steiner & Maas (2018) who advise to co-create the value produced by sharing data by accommodating customers throughout the customer journey present an interesting avenue for further research.

Employee Motivation

By far the most underrepresented code is concerned with initiatives, performance indicators or nudges designed to influence employees’ motivation to proactively pursue protective measures regarding customers’ privacy. This is likely due to the organisational perspective on privacy being underrepresented in the sample in general and because even simple measures (e.g., nudges for back-end systems) are difficult to study. In detail, the recommendations suggest to reduce internal hurdles for employees to use privacy controls (Acquisti et al., 2016; Taneja et al., 2014), e.g. by affording extra time for privacy-critical processes or by using external instruments to reward employees for compliance (Bulgurcu et al., 2017). However, the question whether internal privacy-related KPIs or rewards programs can effectively address the privacy paradox on an organisational level remains under-researched. Since this code ultimately aims at controlling privacy-related HR goals while providing guidance for personal interactions, expanding it with concrete recommendations (e.g., employee privacy literacy tests) represents a valuable future research direction.

Personal Interaction

Customer-facing employees are essential for instilling trust throughout the customer journey (“moments of trust” – e.g., by purposefully conducting sales talks in a secluded and private room). As the cues-filtered-out theories suggest, personal interactions convey more information more efficiently – even in a privacy context (Pöttsch et al., 2010). Hence, personal interactions along the customer journey help make a company’s privacy policy both more tangible to the customer and more believable (Morey & Krajecki, 2016, p. 179; Pöttsch et al., 2010). The opportunity to speak with a company representative effectively reduces privacy concerns while increasing perceived rewards of disclosure, thus reducing paradoxical behaviour. As the final step in the process of anchoring privacy skills within a company’s HR pool, personal interactions also serve as a key source of learning for employees and thus help align a firm’s privacy protections with their customers’ demands.

Exactly where and when to employ human interaction touchpoints to efficiently address privacy concerns while setting up feedback loops presents a promising avenue for future research.



Figure 5-7 Connections between HR management codes

Service Development

Most recommendations in the sample revolve around improving customers' privacy at potential points of data collection, e.g., by increasing an app's number of data control settings or by improving how these features get communicated. Usually, these recommendations aim at addressing the privacy paradox by giving the customers both more control over and transparent information on requested data flows. The importance of creating services with both transparency and control in mind has been established (Beke et al., 2018, p. 8) and was largely incorporated into the GDPR's central principle of "Privacy by Design" (Art. 47 GDPR). However, while this current paradigm is a step towards more privacy protection, it cannot fully circumvent the privacy paradox due to the numerous problems with consent-driven disclosure (Richards & Hartzog, 2019; Solove, 2013). Hence, the codes "privacy features" and "communications" are two sides of the same coin, the former necessitating a dialogue with the customer base to function as designed, the latter providing insights into which improvements are demanded by the customer. Both determine the context of customers' motivation on the how and why they will engage with a company's privacy features.

Future studies will have to build on these foundations to actively gauge customers' privacy needs (Matz et al., 2020) across various contexts. The codes within this aggregate dimension are meant to guide such efforts.

Privacy Features

Unlike the codes “collection processes” or “data control”, “privacy features” refers to any design choices within an individual product or service that increase the transparency of the collected data and give users more (granular) control over data flows. Of course, an increase in control does not only mean giving customers an easy way to opt out of sharing data (Dienlin & Metzger, 2016; Dinev et al., 2009), it also means allowing for audience management of this data (de Wolf & Pierson, 2014), providing selective options for anonymity and confidentiality (Dinev et al., 2012) or creating a privacy dashboard showing all currently shared data or its value to the customer and the company (Hallam & Zanella, 2017). Naturally, the effectiveness of these privacy features is highly dependent on corresponding communication efforts and the inclusion into other service developments. These individual privacy features only represent the final step to address the privacy paradox. However, current research already provides ample evidence for the importance of privacy features (C. Bauer & Lasinger, 2014; C. Bauer & Strauss, 2016; Michler et al., 2020) as well as many rather detailed design instructions for both improving the rational and irrational sides of customers’ privacy decision-making process (see e.g. Acquisti et al., 2017).

Communications

Almost a third of all the papers in the sample give a recommendation on or stress the importance of engaging the customer in a privacy dialogue, i.e., information campaigns or communication strategies aimed at improving customers’ privacy-related knowledge. The reasoning is that a reduced informational asymmetry between customers and companies will diminish paradoxical behaviour through more informed choices. As Boerman et al. put it (2018, p. 19): “People are aware of the threat to their online privacy. However, many people do not know what to answer in questions about highly effective behaviours – which is an indication for little knowledge. (...) People could be educated about the severity of the threat by explaining to them how the collection, usage, and sharing of their personal data online could be a threat to one’s privacy.” Apart from educating customers in general, recommendations are also made on how to improve the readability of privacy notices (Hann et al., 2007), emphasizing the positive aspects of privacy when communicating (Huang & Bashir, 2020) or by simply putting the value proposition of disclosure before the actual disclosure (Baruh et al., 2017).

While the call for more transparency addresses the privacy paradox in the long run, an emphasis on the details of data collection might inflate customers’ perceived risk, thus punishing such efforts (see e.g. Kim et al., 2019). Apart from the aforementioned personal interactions, there are not enough recommendations in the sample for circumventing this effect.

Customer Motivation

Individual data points are almost valueless, as their value is only realised by bundling them into data sets to be used in statistical modelling. While the case of monetary compensation for customer data has been made (Hann et al., 2007), it is likely to exacerbate paradoxical behaviour by playing to hyperbolic discounting biases or even increasing privacy concerns (Chen et al., 2017). However, other recommendations within this code cover incentives, rewards, or nudges designed to influence customers' motivation to proactively pursue protective measures regarding their privacy. Often and clearly highlighting the social value of using privacy controls might incentivise customers to protect themselves and others (Morlok, 2016). The same could be achieved by piquing users' curiosity by an incremental release of information about privacy protection (Kitkowska et al., 2020).

However, what motivates customers with regard to their privacy is highly individual and is probably not easily predictable in general (Barth & de Jong, 2017). Hence, firms could survey and segment their customer base for incentives which would effectively motivate them to engage in a privacy dialogue. Further research on such a direction is still needed.

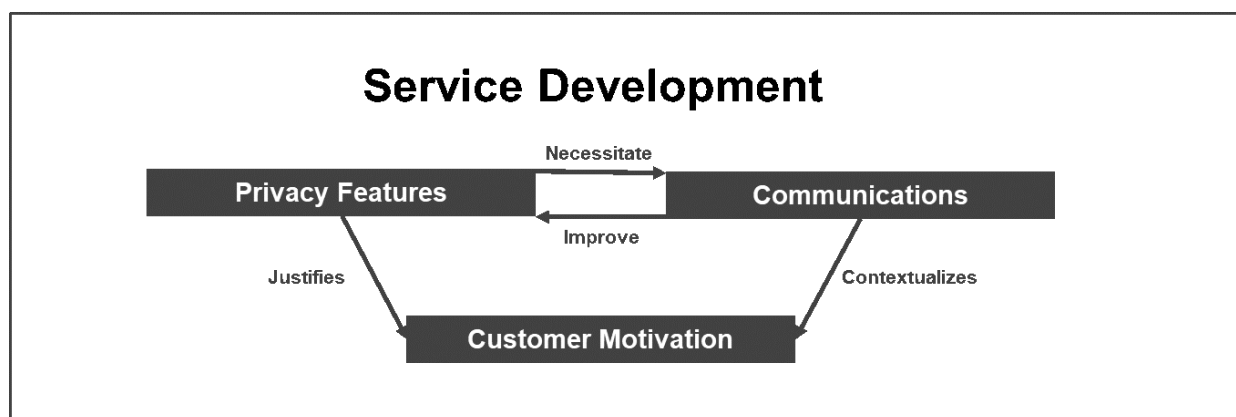


Figure 5-8 Connections between service development codes

Theoretical Approaches to the Paradox

Our understanding of the privacy paradox has grown over the past two decades beyond the dichotomous view of rationality vs. irrationality. However, the nature and appearance of the paradox is highly context- and personality-sensitive (Bansal et al., 2016; Dinev et al., 2012; James et al., 2015; Morlok, 2016; Plangger & Montecchi, 2020; Waters & Ackerman, 2011). This is reflected in the increased use of the 'Antecedents – Privacy Concerns – Outcomes' (APCO) model (Dinev et al., 2015) outside of IS research streams and in the fact that more than half of all analysed papers utilise two or more theories to explain the privacy paradox (see fig. 9).

However, the privacy calculus is still the most frequently used model within the sample. Its user-centric assumptions have been especially useful in driving recommendations for the "HR management" and "service development" dimensions (Dinev et al., 2012; Kehr et al., 2015;

Keith et al., 2014; Zhu et al., 2017). This is not surprising as, from a marketing manager's point of view, addressing the privacy paradox by aiding the customer in aligning their semi-rational calculation with their actual behaviour should be a primary goal. After all, offering immediately perceivable benefits tied to the disclosure of data while increasing transparency by guiding the customer "throughout their journey" is a fixture of customer centricity literature (Lemon & Verhoef, 2016, p. 89).

Theoretical approaches to the privacy paradox		
Theories based on a (biased) risk-benefit calculation	Theories based on little to no risk assessment	Theories based on systemic or societal hurdles
1. APCO 2. Privacy Calculus 3. CPMT 4. Gossip Theory 5. Commitment-Trust Theory of Relationship Marketing 6. PMT 7. TRA & TBP 8. Expectancy Theory 9. Privacy Regulation Theory 10. Prospect Theory 11. Uses and gratification 12. Resource Exchange Theory 13. Reactance Theory 14. Media Richness Theory 15. Utility Maximization Theory 16. Social Contract Theory	17. Bounded Rationality 18. Theory of incomplete Information 19. Cues-filtered out Theory 20. Third Person Effect Theory & Optimistic Bias Theory 21. Ritualized Media Use & Routine Activity Theory 22. Dual Process Model of Cognition & ELM 23. Cognitive Absorption Theory 24. Adaptive Cognition Theory 25. Two-Component Model of Self-Presentation Online 26. Feelings-as-Information Theory 27. Hyperbolic Discounting & Self-Control Bias 28. Cognitive Heuristics 29. Symbolic Interactionism 30. Attribution Theory 31. Regulatory Focus Theory 32. Quantum Theory 33. Construal Level Theory 34. Information Gap Theory	35. Public Value Theory 36. (Adaptive) Structuration Theory 37. Social Representation Theory 38. Peer Pressure & Conformity 39. Social Cognition Theory 40. Resource-based View 41. Institutional Theory

Figure 5-9 Categorisation of theories (adapted from Barth & de Jong, 2017, p. 1043)

While this marketing-oriented approach may help improve customers' decision-making processes, it largely fails to address the many systemic problems reinforcing the privacy paradox. Assuming the decision to disclose personal information is based on little to no risk assessment, the only way to reduce paradoxical behaviour is to lower the actual risks of disclosure. The theory of bounded rationality or theories which take the emotional reality of privacy into account (e.g. the feelings-as-information theory) suggest several nudges within the collection processes (Acquisti et al., 2017) to address the privacy paradox. So far, these insights have been mostly applied to collection processes and not to organisations at large.

The discussion of how to address the structural problems driving paradoxical behaviour has so far been mostly the domain of law- and policy-oriented papers (Reidenberg et al., 2014; Richards & Hartzog, 2019; see e.g. Solove, 2013, 2021). How to apply these insights on an organisational level is so far under-researched. The theories represented within this sample (e.g., the structuration theory and the resource-based view) hint towards the feasibility of other management theories as potentially viable avenues to address systemic privacy problems on the organisational level.

By only considering recommendations born out of well-established theories whose merits have been tested across different contexts and disciplines, the soundness of the theoretical basis of our suggested model is ensured. Additionally, the model highlights the viable theoretical pathways to research privacy on an organisational level for future studies.

Discussion

The purpose of this systematic review is to summarise and structure the recommendations from the past 20 years of privacy paradox research on how to address paradoxical behaviours by customers on an organisational level. We were able to review and code the recommendations from 138 papers and captured a theoretical process of how and where to best reduce paradoxical behaviour – i.e. “claiming to have privacy concerns but disclosing private information nonetheless” (Barth & de Jong, 2017, p. 1050). In the following paragraphs, the main conclusions drawn from the papers are analysed, and directions for future research directions will be given.

Classification of Organisational Privacy Processes

We have shown that the recommendations from the past two decades paint a complex picture of how the privacy paradox can be addressed on the organisational level. By aggregating these processes within four dimensions, we hope to provide a common underlying structure for further research on improving customers' informational privacy. As Forrester (1968, p. 413), the originator of industrial dynamics, put it: “The nonlinear, multiple, feedback loop structuring of systems with associated dynamic principles should grow into a foundation and a central core to unify management education” – or in the case of this paper: organisational privacy processes.

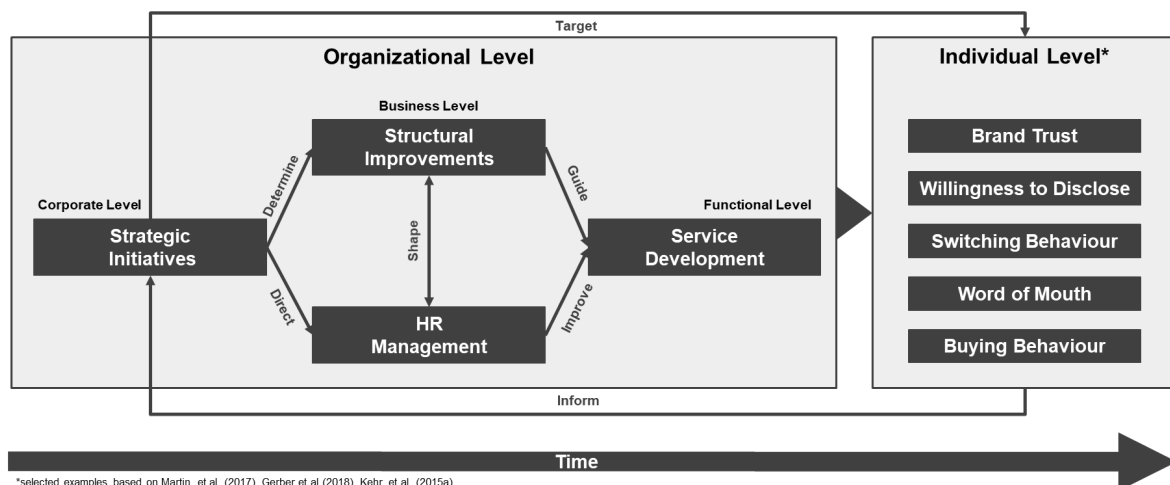


Figure 5-10 Dynamic model for addressing the privacy paradox as a firm

The model shows that addressing the privacy paradox on an organisational level requires a privacy orientation guided by a corporate strategy throughout the business units and down to different functional areas. The temporal dimension is suggested by two arguments. Firstly, the corporate and business level aggregate dimensions largely comprise codes with recommendations that cannot be implemented as short-term patches. Secondly, from a strategic management perspective, the cumulative learning of both the organisation (Argote et al., 2003) and the customer “are based on the total purchase and consumption experiences with a product or service over time” (Y. Wang & Lo, 2003, p. 492). From literature on trust recovery after data breaches we also know that a reorientation of data collection processes takes considerable time (K. D. Martin et al., 2017; Wirtz & Lwin, 2009). Hence, from a resource-based view, a superior privacy orientation cannot arise from any single one of the discussed recommendations, but rather from a “complex combination of processes, routines, technologies and individual skills” (Y. Wang & Lo, 2003, p. 495).

While there are currently no studies on the direct effect of the processes outlined in the four dimensions on the individual level, theories like the APCO model suggest that strategic initiatives and structural improvements may affect individuals’ privacy concerns (Dinev et al., 2015, p. 643). At the same time, the changes brought on by the dimensions ‘HR management’ and ‘service development’ may directly affect the situational privacy calculus (Kehr et al., 2015) and behavioural reactions of customers (Dinev et al., 2015, p. 643). Apart from structural improvements invisible to the customers, companies should therefore be able to communicate and practice data collection in closer alignment with their customers’ expectations.

The Central Role of the Organisational Level

We argue that management science in general, and marketing management in particular, are well suited and underutilised streams of research to address the privacy paradox on an organisational level. Since marketing management has always been a multidisciplinary science researching the “activity, set of institutions, and processes for creating, communicating, delivering, and exchanging offerings that have value for customers, clients, partners, and society at large” (Wilkie & Moore, 2011, p. 64), it would make sense for it being used to unify the neighbouring fields of privacy research into a cohesive framework. This is not without precedence: Wang, Lee & Wang (1998, p. 70) recognised the erosion of the customers’ need for privacy through “internet marketing” at an early stage and called for an “overall privacy framework” to “achieve the vision of the perfect marketplace that will change the face of commerce as we know it today.” Additionally, even before the height of “the third Era of Privacy” (Westin, 2003, p. 443), there have been successful attempts by marketers to define guidelines on how and when organisations should protect their customers’ privacy (Nowak & Phelps, 1995, p. 57).

Finally, companies have all the tools at their disposal to not only reduce customers' vulnerability to the invasion of their privacy but also to make a positive change in their respective markets. As Sarathy & Robertson (2003, p. 142) put it: "Firms will need to pay continuous attention to privacy issues if consumer goodwill and successful marketing are to be achieved." Marketing as a function is often specifically named as being the central node of the modern privacy debate: caught in the "perpetual tension" between the data needs of advanced analytics and the rising informational privacy needs of their customers (Michler et al., 2020; Palmatier & Martin, 2019). We therefore propose that management science and the organisational perspective in particular offer a hitherto under-researched avenue for effectively addressing the privacy paradox.

Gaps and Future Research

Despite each paper in the sample giving direct or indirect recommendations for addressing the privacy paradox on an organisational level, very few of the sampled research designs aimed at doing so from the outset. The majority of recommendations are extrapolated from effects tested on a personal level. It is therefore not surprising that the most detailed recommendations are aimed at communicating privacy processes and measures, adding additional privacy features or addressing collection processes as a whole. Based on these recommendations, we offer avenues for future research which we think will provide useful insights for developing an organisational response to the privacy paradox. In doing so, we hope to contribute to establishing privacy orientation as a viable and actionable strategy. The following list is not intended to be exhaustive; it just highlights the most noticeable research gaps found in our sample:

- **Privacy goals:** What elements and themes define an organisational privacy culture? When and under what conditions can companies transition from a compliance-oriented privacy culture towards a customer-oriented privacy culture?
- **Trust building:** When and under what conditions can firms rebuild customers' trust after past privacy failures? How can the effectiveness of such trust-generating tactics be measured? Do customers differentiate between general brand trust and privacy trust?
- **Privacy branding:** When and under what conditions is privacy branding effective in reducing privacy concerns amongst customers? What are the drivers of brand extension success with regard to customer privacy? What determines the stretchability of a brand regarding the successful incorporation of privacy-oriented messages to customers?
- **Industry influence:** Do industry-level privacy initiatives encourage deeper consumer-company relationships? When and under what conditions are companies' efforts to

assert industry influence with regard to encouraging stricter privacy policies noticed by customers?

- **Company structure:** Could more customer-centric company structures be used to improve organisational privacy?
- **Privacy skills:** What skills should be actively improved within a company's human resource pool to improve customers' privacy outcomes? Within which departments can privacy trainings generate the most impact?
- **Employee motivation:** When and under what circumstances are privacy-oriented key performance indicators effective in improving customers' informational privacy?
- **Personal interactions:** When and under what circumstances can personal interactions throughout the customer journey aid customers' privacy calculus?
- **Customer motivation:** What motivates customers to engage a firm in a privacy dialogue? What incentives motivate customers to use protective privacy measures?

Research Limitations

Due to the limited research addressing the privacy paradox on an organisational level, this review opted to analyse recommendations and implications across different disciplines and levels. This means that the coding is mostly based on the researchers' arguments, not their direct research results. Hence, while the logical congruence of individual recommendations with their corresponding study results were qualitatively appraised, they are still often based on untested claims. For example, Dinev et al. (2012) demonstrated that anonymity, secrecy and confidentiality positively influence survey participants' perceived privacy. Hence the recommendation "to develop (website) privacy control features (...) to maintain the anonymity, secrecy, and confidentiality of their personal information" (Dinev et al., 2012, p. 309) may be logically sound, even when extended to a company's data collection as a whole, but it still is an untested claim. By focusing on arguments based on well-established theories only, we aim to maintain a high level of scientific rigor. Still, the presented dynamic model is to be understood as a theoretical framework which serves as a foundation for further research, not a predictive model based on experimental data.

Furthermore, privacy is a highly contextually dependent and fluid concept (Schaub et al., 2015), which is nevertheless treated as a stable concept in a lot of studies (Xu et al., 2011). Criticism has also been expressed regarding the fact that various prior measurements do not distinguish between "privacy", "informational privacy" or "perceived privacy" and related concepts such as "psychological privacy" or "social privacy" (Dienlin & Trepte, 2015). Similarly, some studies may be suspected to violate the "principle of compatibility" (Ajzen, 2011) – i.e. measuring privacy concerns at a low level of specificity while researching within a highly specific context. By incorporating recommendations based on such measurements, this study might exaggerate the general effectiveness of certain recommendations.

Finally, while we strove for high transparency and replicability of the review process, the qualitative appraisal of sources and the coding of recommendations might still be prone to institutional biases, despite actively working to increase intercoder reliability (for details on the codes and processes used see the supplemental materials).

Conclusion

The purpose of this paper was to review the recommendations made in the past 20 years of privacy paradox research on how to address it on an organisational level. We determined that companies can generally align their privacy practices with customers' expectations across four inter-connected managerial processes: (1) strategic initiatives, (2) structural improvements, (3) human resource management, and (4) service development. The overall findings detail how companies can address both the rational and irrational nature of the privacy decision-making process.

With this model, we are trying to dispel the notion that a focus on privacy law compliance is enough to help customers avoid paradoxical behaviour. Barocas & Nissenbaum (2009) highlighted the three biggest problems with their "notice and consent" rationale: (1) Sharing data with other companies usually includes third-party access. This means that customers would need to understand which actors have access to what data for what purposes and what privacy policy applies to any of those transactions to make an informed choice. (2) In many countries privacy policies may be changed with an advance warning of just thirty days. (3) With the "ever-increasing number of players in the ad network and exchange space", understanding the flow of data becomes impossible for customers. Hence, several researchers within the sample have questioned the reliability of self-regulation and passive customer empowerment (Acquisti et al., 2015; Barocas & Nissenbaum, 2014; Cate & Mayer-Schönberger, 2013; Sanchez-Rola et al., 2019; Solove, 2013). Therefore, should a company wish to sustainably address the privacy paradox, it would have to move beyond the reactive thinking of privacy law compliance. In doing so, companies can hope to differentiate themselves from other industry actors (K. D. Martin & Murphy, 2017, p. 151), streamline data collection processes (Choi et al., 2018), acquire a future-oriented human resource pool (Bulgurcu et al., 2017) and improve an important part of each customer's journey.

The dynamic model presented within this paper serves as a foundation for guiding further privacy research in an organisational context. We believe that looking at the problem through a marketing management lens has the potential to both unearth new methods of addressing the privacy paradox and to gain insights into whether privacy could be leveraged by companies to obtain a strategic advantage. To expand on the conclusion of Barth & De Jong's (2017, p. 1052) literature review on the privacy paradox: Attempts to theoretically explain the privacy paradox are not scarce; however, ways "to practically solve the problem of the privacy paradox are still scarce and we feel the subject (still) deserves far more research attention".

Supplemental materials published with this article are available at:

<https://link.springer.com/article/10.1007/s11301-021-00239-4#Sec36>

References

- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Pre-Proceedings to EC'04, May 17-20, New York*, 1–9.
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. In *Science* (Vol. 347, Issue 6221, pp. 509–514). American Association for the Advancement of Science. <https://doi.org/10.1126/science.aaa1465>
- 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 Reference Format. *ACM Computing Surveys*, 50(3), 1–41. <https://doi.org/10.1145/3054926>
- Acquisti, A., Taylor, C., Wagman, L., Boheme, R., Bonatti, A., Calo, R., Cooper, J., Goldfarb, A., Grossklags, J., Hoofnagle, C., Hui, K.-L., Jentzsch, N., Kim, J.-H., Malin, B., Nissenbaum, H., Odlyzko, A., Picker, R., Png, I., Preibusch, S., ... Acquisti, F. (2016). The Economics of Privacy †. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Ahluwalia, R. (2008). How far can a brand stretch? Understanding the role of self-construal. *Journal of Marketing Research*, 45(3), 337–350. <https://doi.org/10.1509/jmkr.45.3.337>
- Ajzen, I. (2011). Is Attitude Research Incompatible With the Compatibility Principle. In R. M. Arkin (Ed.), *Most underappreciated: 50 prominent social psychologists describe their most unloved work* (pp. 583–605). Oxford Scholarship Online. <https://doi.org/10.1093/acprof:osobl/9780199778188.003.0029>
- Ajzen, I., & Fishbein, M. (1970). The prediction of behavior from attitudinal and normative variables. *Journal of Experimental Social Psychology*, 6(4), 466–487. [https://doi.org/10.1016/0022-1031\(70\)90057-0](https://doi.org/10.1016/0022-1031(70)90057-0)
- Ajzen, I., & Fishbein, M. (1977). Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research. *Psychological Bulletin*, 87(5), 888–918. <https://doi.org/https://doi.org/10.1037/0033-2909.84.5.888>
- Alashoor, T., & Baskerville, R. (2015). The Privacy Paradox: The Role of Cognitive Absorption in the Social Networking Activity. *Proceedings of the 22nd Americas Conference on Information Systems*, 1–20.
- Amiri, I., Wang, L., Levy, Y., & Hur, I. (2018). An Empirical Study on the Factors Contributing to Disclosing Personal Information Online: Insecurity in the Digital Age. *Twenty-Fourth Americas Conference on Information Systems*, 1–10.
- Anhalt-Depies, C., Stenglein, J. L., Zuckerberg, B., Townsend, P. M., & Rissman, A. R. (2019). Tradeoffs and tools for data quality, privacy, transparency, and trust in citizen science. *Biological Conservation*, 238, 1–7. <https://doi.org/10.1016/j.biocon.2019.108195>
- Argote, L., McEvily, B., & Reagans, R. (2003). Managing knowledge in organizations: An integrative framework and review of emerging themes. *Management Science*, 49(4), 571–582. <https://doi.org/10.1287/mnsc.49.4.571.14424>
- Auxier, B. Y. B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and Privacy: Concerned, Confused, and Feeling a Lack of Control Over Their Personal Information. *Pew Research Center, November*, 1–63.
- Bandara, R., Fernando, M., & Akter, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. In C. / P. / CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANAGEMENT / HCist - International Conference on Health and Social Care Information Systems and Technologies (Ed.), *Procedia Computer Science* (Vol. 121, pp. 562–567). Elsevier B.V. <https://doi.org/10.1016/j.procs.2017.11.074>
- Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support. *Communications of the Association for Information Systems*, 34, 154–204. <https://doi.org/https://doi.org/10.17705/1CAIS.03708>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management*, 53(1), 1–21. <https://doi.org/10.1016/j.im.2015.08.001>

- Barnes, S. B. (2006). A privacy paradox: Social Networking in the United States. *First Monday*, 11(9). <https://doi.org/https://doi.org/10.5210/fm.v11i9.1394>
- Barocas, S., & Nissenbaum, H. (2009). On Notice: The Trouble with Notice and Consent. *Engag. Data Forum First Int. Forum Appl. Manag. Pers. Electron. Inf.*, 1–6.
- Barocas, S., & Nissenbaum, H. (2014). Computing Ethics: Big Data's End Run Around Procedural Privacy Protections Recognizing the inherent limitations of consent and anonymity. *Communications of the ACM*, 57(11), 31–33. <https://doi.org/10.1145/2668897>
- Barth, S., & de Jong, M. D. T. (2017). The Privacy Paradox - Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior - A Systematic Literature Review. *Telematics and Informatics*, 34, 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55–69. <https://doi.org/10.1016/j.tele.2019.03.003>
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Bauer, A., Reiner, G., & Schamschule, R. (2000). Organizational and quality systems development: An analysis via a dynamic simulation model. *Total Quality Management*, 11(4–6), 410–416. <https://doi.org/10.1080/09544120050007715>
- Bauer, C., & Lasinger, P. (2014). Adaptation strategies to increase advertisement effectiveness in digital media. *Management Review Quarterly*, 64, 101–124. <https://doi.org/10.1007/s11301-014-0101-0>
- Bauer, C., & Strauss, C. (2016). Location-based advertising on mobile devices A literature review and analysis. *Management Review Quarterly*, 66, 159–194. <https://doi.org/10.1007/s11301-015-0118-z>
- Becker, B., & Gerhart, B. (1996). The impact of human resource management on organizational performance: Progress and prospects. *Academy of Management Journal*, 39(4), 779–801. <https://doi.org/10.2307/256712>
- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. In *Foundations and Trends in Marketing* (Vol. 11, Issue 1). <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>
- Bickelmann, J. (2021, January 24). Sag mir, wo du schreibst. *Der Tagesspiegel*, 18.
- 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>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2017). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. In *MIS Quarterly* (Vol. 34, Issue 3). <https://doi.org/10.2307/25750690>
- Casadesus-Masanell, R., & Hervás-Drane, A. (2015). Competing with privacy. *Management Science*, 61(1), 229–246. <https://doi.org/10.1287/mnsc.2014.2023>
- Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. *International Data Privacy Law*, 3(2), 67–73.
- 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>
- 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>
- Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the Blogging Privacy Management Measure. *Journal of the American Society for Information Science and Technology*, 60(10), 2079–2094. <https://doi.org/10.1002/asi.21122>

- 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>
- Citron, D. K. (2009). Cyber Civil Rights. *Boston University Law Review*, 89(1), 61–126.
- Clemons, E. K., Wilson, J., & Jin, F. (2014). Investigations into Consumers Preferences Concerning Privacy: An Initial Step Towards the Development of Modern and Consistent Privacy Protections Around the Globe. In IEEE (Ed.), *47th Hawaii International Conference on System Science* (pp. 4083–4092). <https://doi.org/10.1109/HICSS.2014.504>
- de Wolf, R., & Pierson, J. (2014). Who's my audience again? Understanding audience management strategies for designing privacy management technologies. *Telematics and Informatics*, 31(4), 607–616. <https://doi.org/10.1016/j.tele.2013.11.004>
- Dehghanpouri, H., Soltani, Z., & Rostamzadeh, R. (2020). The impact of trust, privacy and quality of service on the success of E-CRM: the mediating role of customer satisfaction. *Journal of Business & Industrial Marketing*, 1–17. <https://doi.org/10.1108/JBIM-07-2019-0325>
- 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>
- Dienlin, T., & Trepte, S. (2015). Putting the Social (Psychology) into Social Media: Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors. *European Journal of Social Psychology*, 45(3), 285–297. <https://doi.org/10.1002/ejsp.2038>
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Dinev, T., Mcconnell, A. R., Smith, H. J., & Jeff, H. (2015). Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4), 639–655. <https://doi.org/10.1287/isre.2015.0600>
- Dinev, T., Xu, H., & Smith, H. J. (2009). Information privacy values, beliefs and attitudes: An empirical analysis of web 2.0 privacy. *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*, 1–10. <https://doi.org/10.1109/HICSS.2009.255>
- 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>
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. <https://doi.org/10.1016/j.jbusres.2006.02.006>
- Fazzini, K. (2019). *Apple's big bet on privacy has risks*. CNBC. <https://www.cnbc.com/2019/01/10/apple-privacy-big-bet-risks.html>
- Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24(3), 219–229. <https://doi.org/10.1108/08876041011040622>
- Feng, Y., & Xie, Q. (2019). Privacy Concerns, Perceived Intrusiveness, and Privacy Controls: An Analysis of Virtual Try-On Apps. *Journal of Interactive Advertising*, 19(1), 43–57. <https://doi.org/10.1080/15252019.2018.1521317>
- Forrester, J. W. (1968). Industrial Dynamics—After the First Decade. *Management Science*, 14(7), 398–415. <https://doi.org/10.1287/mnsc.14.7.398>
- Freudiger, J., Rane, S., Brito, A. E., & Uzun, E. (2014). Privacy Preserving Data Quality Assessment for High-Fidelity Data Sharing. *WISCS '14: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 21–29. <https://doi.org/10.1145/2663876.2663885>
- Gambino, A., Kim, J., Sundar, S. S., Ge, J., & Rosson, M. B. (2016). User disbelief in privacy paradox: Heuristics that determine disclosure. *Conference on Human Factors in Computing Systems - Proceedings*, 07-12-May, 2837–2843. <https://doi.org/10.1145/2851581.2892413>
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, 16(1), 15–31. <https://doi.org/10.1177/1094428112452151>

- Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge Management: An Organizational Capabilities Perspective. *Journal of Management Information Systems*, 18(1), 185–214. <https://doi.org/10.1080/07421222.2001.11045669>
- Greenaway, K. E., & Chan, Y. E. (2005). Theoretical Explanations for Firms' Information Privacy Behaviors. *Journal of the Association for Information Systems*, 6(6), 171–198. <https://doi.org/10.17705/1jais.00068>
- Gunther, R. E. (2009). Peter Drucker-the grandfather of marketing: an interview with Dr. Philip Kotler. *Journal of the Academy of Marketing Science*, 37, 17–19. <https://doi.org/10.1007/s11747-008-0105-1>
- Guo, X., Zhang, X., & Sun, Y. (2016). The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, 16, 55–65. <https://doi.org/10.1016/j.el-erap.2015.11.001>
- Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217–227. <https://doi.org/10.1016/j.chb.2016.11.033>
- 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>
- 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>
- Hruschka, D. J., Schwartz, D., St.john, D. C., Picone-Decaro, E., Jenkins, R. A., & Carey, J. W. (2004). Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research. *Field Methods*, 16(3), 307–331. <https://doi.org/10.1177/1525822X04266540>
- 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
- Hui, K., Teo, H. H., & Lee, S.-Y. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31(1), 19–33.
- Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17, 89–101. <https://doi.org/10.1007/s10676-015-9363-z>
- James, T. L., Nottingham, Q., Collignon, S. E., Warkentin, • Merrill, & Ziegelmayer, J. L. (2015). The interpersonal privacy identity (IPI): development of a privacy as control model. *Information Technology and Management*, 17, 341–360. <https://doi.org/10.1007/s10799-015-0246-0>
- Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, 34(2), 369–400. <https://doi.org/10.1080/07421222.2017.1334467>
- 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>
- Keith, M. J., Babb, J. S., & Lowry, P. B. (2014). A longitudinal study of information privacy on mobile devices. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3149–3158. <https://doi.org/10.1109/HICSS.2014.391>
- 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>
- Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *Keele University and Durham University Joint Report*, 1–65.
- 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.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, 64(November), 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>

- Kuckertz, A., & Block, J. (2021). Reviewing systematic literature reviews: ten key questions and criteria for reviewers. *Management Review Quarterly* 2021, 1–6. <https://doi.org/10.1007/S11301-021-00228-7>
- Lanier, C. D., & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12(1), 1–48.
- Lemon, K. N., & Verhoef, P. C. (2016). Understanding Customer Experience Throughout the Customer Journey. *Journal of Marketing*, 80, 69–96. <https://doi.org/10.1509/jm.15.0420>
- Leonard, D., & McAdam, R. (2004). Total quality management in strategy and operations: Dynamic grounded models. *Journal of Manufacturing Technology Management*, 15(3), 254–266. <https://doi.org/10.1108/17410380410523489>
- Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 14(1), 44–59. <https://doi.org/10.1177/1094670510383409>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>
- Mao, Y. (2018). Intercoder Reliability Techniques: Holsti Method . In M. Allen (Ed.), *The SAGE Encyclopedia of Communication Research Methods* (1st ed., pp. 741–743). SAGE Publications. <https://doi.org/10.4135/9781483381411>
- Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. *Business Ethics Quarterly*, 30(1), 65–96. <https://doi.org/10.1017/beq.2019.24>
- 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., & 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>
- Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current Opinion in Psychology*, 31(2), 116–121. <https://doi.org/10.1016/j.copsyc.2019.08.010>
- Mcneely, C. L., & Hahm, J. on. (2014). The big (data) bang: Policy, prospects, and challenges. *Review of Policy Research*, 31(4), 304–310. <https://doi.org/10.1111/ropr.12082>
- Michler, O., Decker, R., & Stummer, C. (2020). To trust or not to trust smart consumer products: a literature review of trust-building factors. *Management Review Quarterly*, 70, 391–420. <https://doi.org/10.1007/s11301-019-00171-8>
- Mohassel, P., & Zhang, Y. (2017). SecureML: A System for Scalable Privacy-Preserving Machine Learning. 2017 *IEEE Symposium on Security and Privacy*, 19–38. <https://doi.org/10.1109/SP.2017.12>
- Morey, T., & Krajecki, K. (2016). Personalisation, data and trust: The role of brand in a data-driven, personalised, experience economy. *Journal of Brand Strategy*, 5(2), 178–185.
- Morlok, T. (2016). Sharing is (not) caring - The role of external privacy in users' information disclosure behaviors on social network sites. *PACIS*, 75–92. <http://aisel.aisnet.org/pacis2016/75>
- Mothersbaugh, D. L., Foxx Li, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information Background Disclosure and Disclosure Antecedents. *Journal of Service Research*, 15(1), 76–98. <https://doi.org/10.1177/1094670511424924>
- Mourey, J. A., & Waldman, A. E. (2020). Past the Privacy Paradox: The Importance of Privacy Changes as a Function of Control & Complexity. *Journal of the Association for Consumer Research*, 5(2), 1–38. <https://doi.org/https://doi.org/10.1086/708034>
- Nissenbaum, H. (2010). Privacy in Context Technology, Policy, and the Integrity of Social Life. In *Privacy in Context*. Stanford University Press.
- Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. *Psychology & Marketing*, 24(10), 829–847. <https://doi.org/10.1002/mar.20186>
- Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when “privacy” matters. *Journal of Direct Marketing*, 9(3), 46–60. [https://doi.org/10.1002/\(SICI\)1522-7138\(199723\)11:43.0.CO;2-F](https://doi.org/10.1002/(SICI)1522-7138(199723)11:43.0.CO;2-F)
- Oetzel, M. C., & Gonja, T. (2011). The online privacy paradox: A social representations perspective. *Conference on Human Factors in Computing Systems - Proceedings*, 2107–2112. <https://doi.org/10.1145/1979742.1979887>

- Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, 37(43), 879–910.
- Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, 6, 642–660. <https://doi.org/10.1057/s41303-017-0056-z>
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Plangger, K., & Montecchi, M. (2020). Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, 50, 32–44. <https://doi.org/10.1016/j.intmar.2019.10.004>
- Pötzsch, S., Wolkerstorfer, P., & Graf, C. (2010). Privacy-Awareness Information for Web Forums: Results from an Empirical Study. In ACM (Ed.), *NordiCHI* (pp. 363–372). ACM.
- Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human Computer Studies*, 110(March 2016), 21–32. <https://doi.org/10.1016/j.ijhcs.2017.10.003>
- Raento, M., & Oulasvirta, A. (2008). Designing for privacy and self-presentation in social awareness. *Personal and Ubiquitous Computing*, 12(7), 527–542. <https://doi.org/10.1007/s00779-008-0200-9>
- Reidenberg, J. R., Russell, C. N., Callen, A. J., Qasir, S., & Norton, T. (2014). Privacy Harms and the Effectiveness of the Notice and Choice Framework. *Journal of Law and Policy for the Information Society*, 11(2), 485–524.
- Richards, N. M. (2008). Intellectual privacy. *Texas Law Review*, 87(2), 387–445.
- Richards, N. M., & Hartzog, W. (2019). The Pathologies of Digital Consent. *Washington University Law Review*, 1461–1503. <https://papers.ssrn.com/abstract=3370433>
- Rodriguez, S. (2021, February 1). Facebook strikes back against Apple privacy change, prompts users to accept tracking to get 'better ads experience.' *CNBC*. <https://www.cnn.com/2021/02/01/facebook-strikes-back-against-apple-ios-14-idfa-privacy-change.html>
- Sanchez-Rola, I., Dell'amico, M., Kotzias, P., Eurecom, D. B., Bilge, L., Vervier, P.-A., Santos, I., & Balzarotti, D. (2019). Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. *AsiaCCS*, 12, 340–351. <https://doi.org/10.1145/3321705.3329806>
- Sarathy, R., & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. In *Source: Journal of Business Ethics* (Vol. 46, Issue 2).
- Schade, M., Piehler, R., Warwitz, C., & Burmann, C. (2018). Increasing consumers' intention to use location-based advertising. *Journal of Product and Brand Management*, 27(6), 661–669. <https://doi.org/10.1108/JPBM-06-2017-1498>
- Schaub, F., Könings, B., & Weber, M. (2015). Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, 14(1), 34–43. <https://doi.org/10.1109/MPRV.2015.5>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989–1015.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), 167–196.
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, 89(1), 1–51.
- Son, B. J.-Y., & Kim, S. S. (2008). Internet User's Information Privacy-Protective Responses: A Taxonomy and Nomological Model. *MIS Quarterly*, 32(3), 503–529.
- Steiner, P. H., & Maas, P. (2018). When customers are willing to disclose information in the insurance industry: A multi-group analysis comparing ten countries. *International Journal of Bank Marketing*, 36(6), 1015–1033. <https://doi.org/10.1108/IJBM-12-2016-0183>
- Sun, S. (2008, December). Organizational Culture and Its Themes. *International Journal of Business and Management*, 137–141.
- Sundar, S., & Kim, J. (2019). Machine heuristic: When we trust computers more than humans with our personal information. *Conference on Human Factors in Computing Systems - Proceedings*, 1–9. <https://doi.org/10.1145/3290605.3300768>

- Sundar, S. S., Kang, H., Zhang, B., Go, E., & Wu, M. (2013). Unlocking the Privacy Paradox: Do Cognitive Heuristics Hold the Key? *Conference on Human Factors in Computing Systems - Proceedings, April*, 811–816. <https://doi.org/10.1145/2468356.2468501>
- Sundar, S. S., Kim, J., Rosson, M. B., & Molina, M. D. (2020). Online Privacy Heuristics that Predict Information Disclosure. *Conference on Human Factors in Computing Systems - Proceedings*, 1–12. <https://doi.org/10.1145/3313831.3376854>
- Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, 38, 159–173. <https://doi.org/10.1016/j.chb.2014.05.027>
- Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems*, 24(4), 153–173. <https://doi.org/10.2753/MIS0742-1222240406>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Teixeira, G. A., da Silva, M. M., & Pereira, R. (2020). The Critical Success Factors of GDPR Implementation: a Systematic Literature Review. *Digital Policy, Regulation and Governance*, 21(4), 402–418. <https://doi.org/https://dx.doi.org/10.1108/DPRG-01-2019-0007>
- Teng, P. K., Heng, B. L. J., & Wong Abdullah, S. I. N. (2019). Distinctive Comparison of Consumers' Mobile Payment Adoption between China and Malaysia. *Asia Proceedings of Social Sciences*, 2(3), 57–61. <https://doi.org/10.31580/apss.v2i3.258>
- Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2017). Privacy-Preserving Mechanisms for Crowdsensing: Survey and Research Challenges. In *IEEE Internet of Things Journal* (Vol. 4, Issue 4, pp. 855–869). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/JIOT.2016.2594205>
- Völckner, F., & Sattler, H. (2006). Drivers of brand extension success. *Journal of Marketing*, 70(2), 18–34. <https://doi.org/10.1509/jmkg.70.2.18>
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the “privacy paradox.” *Current Opinion in Psychology*, 31(2), 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- 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, Y., & Lo, H.-P. (2003). Customer-focused performance and the dynamic model for competence building and leveraging A resource-based view. *Journal of Management Development*, 486–526. <https://doi.org/10.1108/02621710310478486>
- Waters, S., & Ackerman, J. (2011). Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure. *Journal of Computer-Mediated Communication*, 17(1), 101–115. <https://doi.org/10.1111/j.1083-6101.2011.01559.x>
- Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431–453. <https://doi.org/10.1111/1540-4560.00072>
- Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. In *Source: The Yale Law Journal* (Vol. 113, Issue 6). The Yale Law Journal Company, Inc.
- Wilkie, W. L., & Moore, E. S. (2011). Expanding our understanding of marketing in society. *Journal of the Academy of Marketing Science*, 40, 53–73. <https://doi.org/10.1007/s11747-011-0277-y>
- Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-things. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 644–652. <https://doi.org/10.1109/ARES.2016.25>
- Wirtz, J., & Lwin, M. O. (2009). Regulatory Focus Theory, Trust, and Privacy Concern. *Journal of Service Research*, 12(2), 190–207. <https://doi.org/10.1177/1094670509335772>
- Wright, P. M., & McMahan, G. C. (1992). Theoretical Perspectives for Strategic Human Resource Management. *Journal of Management*, 18(2), 295–320. <https://doi.org/10.1177/014920639201800205>
- 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>

- Xu, H., Luo, X. (Robert), Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52. <https://doi.org/10.1016/j.dss.2010.11.017>
- Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information and Management*, 56(4), 570–601. <https://doi.org/10.1016/j.im.2018.10.001>
- Zhou, K. Z., & Li, C. B. (2010). How strategic orientations influence the building of dynamic capability in emerging economies. *Journal of Business Research*, 63(3), 224–231. <https://doi.org/10.1016/j.jbusres.2009.03.003>
- Zhu, H., Ou, C. X. J., van den Heuvel, W. J. A. M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, 54(4), 427–437. <https://doi.org/10.1016/j.im.2016.10.001>

6. Article

Gotsch, M. & Schögel, M. (n.d.). Organisational Privacy Orientation – Scale Development and Validation. *Journal of Business Research*, under review.

Organisational Privacy Orientation - Scale Development and Validation

Mauro Luis Gotsch, MA HSG

mauro.gotsch@unisg.ch / ORCID: 0000-0002-5319-2347

Institute of Marketing, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

Prof. Dr. Marcus Schögel

marcus.schoegel@unisg.ch

Institute of Marketing and Customer Insight, University of St. Gallen

Dufourstrasse 40a

9000 St. Gallen

Switzerland

CRedit author statement:

Mauro Gotsch: Methodology, Conceptualisation, Formal Analysis, Investigation, Writing – Original Draft, Visualisation, Data Curation, Writing – Review & Editing, Validation

Marcus Schögel: Supervision, Validation, Resources, Project Administration, Funding Acquisition

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 operationalised all the organisational facets which could categorise a firm's marketing strategy as privacy oriented. Hence, this paper reports a series of five studies and develops a self-assessment scale meant to holistically measure organisational privacy orientation. The proposed construct consists of four dimensions: strategic privacy orientation, structural privacy orientation, customer centric privacy orientation and tactical privacy orientation. The resulting scale shows internal consistency, reliability as well as construct and nomological validity. The results are used to provide a basis for future research and a guide for managers to analyse or further develop their organisational privacy strategy.

Keywords: *Privacy strategy, information privacy, marketing strategy, scale development*

Declarations of interest: none

PsycInfo Classification Codes: 3660, 3920

Acknowledgements

The authors would like to thank Dr. Nico Ebert, Dr. Iris Schmutz, Dr. Marcel Cahenzli, Dr. Martin Berger, Dr. Martin Schumacher, Dr. Severin Lienhard, Dr. Peter Fischer, Susanna Renner and Alexander Tombach for their constructive suggestions on previous drafts of this article. Additionally, the authors would like to thank the Verein Unternehmerischer Datenschutz (VuD) and the International Association of Privacy Professionals (IAPP) for participating and contributing to the quantitative study. Finally, I would like to thank Valdrin Bekaj, Manon Champagne, David Morand and Fabian Schaefer, who aided us in the collection and transcription of parts of the qualitative interview data.

Introduction

Even though consumers bear “the entirety of downsides” (Rapp et al., 2009, p. 59) of commercial data sharing, they often do not perceive the benefits of providing their data to companies (Cisco, 2019; KPMG, 2021; Salesforce, 2019) or are manipulated into giving consent to share their data (Lupiáñez-Villanueva et al., 2022; Nouwens et al., 2020; Waldman, 2020). Consequently, marketing strategies often fail to address both privacy regulations and consumers’ growing demand for more data privacy (Quach et al., 2022). Although past privacy research has revealed “deep insights” into consumers’ privacy concerns, privacy technologies, structural forces, and legal compliance, “this focus has limited our view of privacy too much to individual silos” (K. D. Martin & Murphy, 2017, p. 153). Hence, this paper addresses the need for a more holistic analysis of organisational privacy practices through the definition of an organisational privacy orientation construct (OPO) to capture the relevant dimensions that operationalise the idea of a privacy-oriented organisation. In doing so, we hope to provide a unifying framework upon which organisational privacy initiatives benefitting consumers and companies alike can be built.

The need for a deeper understanding of OPO is driven both by technological and societal developments. The protection of consumers’ privacy in digital spaces as a fundamental human right has only recently been comprehensibly codified in several modern legislations; most notably the general data protection regulation of the EU (GDPR), the California Consumer Privacy Act (CCPA) and the Personal Information Protection Law of the People’s Republic of China (PIPL). Yet, the push for organisations to protect their customers’ digital privacy is as old as the internet (see e.g., Wang et al., 1998). Sarathy & Robertson (2003, p. 124) postulated 20 years ago, that “firms will need to pay continuous attention to privacy issues if consumer goodwill and successful marketing are to be achieved”. Firms that can instil trust in their customers through superior data privacy may increase their customers’ satisfaction (Dehghanpouri et al., 2020; K. Martin, 2018) and willingness to share data (Dinev & Hart, 2006) while decreasing the negative outcomes of data leaks on a firm’s performance (A. Malhotra & Malhotra, 2011; K. D. Martin et al., 2017). Additionally, with the growing support for the “environmental, social and governance risk” (ESG) scores among investors, any firm looking for capital “would be well advised” to improve their organisational privacy orientation (Bloemendal, 2022, p. 47).

Prior research has provided a rich foundation to define privacy-oriented customer interactions (Acquisti et al., 2017, 2020; Bandara et al., 2017; Barth & de Jong, 2017; Brough & Martin, 2021; Gerber et al., 2018; Kitkowska, Shulman, et al., 2020; Kokolakis, 2017; Yun et al., 2019), privacy oriented organisational measures (Beke et al., 2018; Bélanger & Crossler, 2011; Gotsch & Schögel, 2021; Lanier & Saini, 2008; K. D. Martin & Murphy, 2017; Smith et al., 2011) as well as privacy-oriented policies (Acquisti et al., 2016; Solove, 2013, 2021; Williams et al., 2016). While these studies offer the theoretical and conceptual insights necessary to define the dimensions of privacy orientation, they have limitations. Recommendations on how firms can holistically

“deliver consistent, transparent privacy protection to their customers while achieving other important organisational objectives” are still lacking (Greenaway et al., 2015, p. 601). While studies like Gotsch & Schögel (2021) provide a theoretical framework which combines the strategic, structural, human resource and service dimensions of organisational privacy, a rigorous operationalisation of the construct has yet to be developed.

To contribute to this extant literature stream, this study builds upon the frameworks proposed by Greenaway et al. (2015), Wirtz et al. (2022) and Gotsch & Schögel (2021) to create a self-assessment scale for organisational privacy orientation. The paper provides clear definitions for all the dimensions which make up OPO and conceptualises and operationalises their domains. It empirically tests both the theoretical antecedents and possible outcomes of a privacy-oriented company. The findings extend prior empirical studies by supporting a relationship between corporate social responsibility and OPO as well as OPO and marketing performance. More generally, the scale offers both researchers and managers a holistic view on the dimensions which make up OPO. In doing so, it provides them with a reliable and valid measurement for the level of privacy orientation of any given company. The findings open opportunities for research into the importance of privacy orientation on company success and customer perception.

Theoretical Basis

Historically, informational privacy or data privacy has been researched on three levels (Greenaway & Chan, 2005, p. 172): the personal, organisational and the sectoral level. Of the three, the organisational level has often only been studied in its relation to the other two (Bélanger & Crossler, 2011, p. 1028; Gotsch & Schögel, 2021, p. 3). This gap is surprising, considering organisational informational privacy, defined as the claim to “appropriate flows” (Parker, 1974, p. 281) of personal information within an organisational context (K. D. Martin & Murphy, 2017, p. 136; Nissenbaum, 2010, p. 4), has been in the forefront of discussions on almost any technical innovation of the past twenty years. Be it social media (Jozani et al., 2020), voice assistants (Vimalkumar et al., 2021), the internet of things (Sicari et al., 2015), or artificial intelligence (Puntoni et al., 2020) – all these technologies and business models connected to them run on the capture of surplus behavioural data from their users (Zuboff, 2020). Hence, any firm processing customer data contributes to their “customers’ vulnerability escalation” regarding informational privacy (Palmatier & Martin, 2019, p. 88).

First discussions of OPO have therefore mostly concentrated on the potentially hazardous consequences organisational data processing could have on consumers (see e.g., Baruh & Cemalcilar, 2014; Li, 2011). Regrettably, very few managerially oriented studies have tried to address informational privacy as its own strategic direction to be included into current marketing practices (Gotsch & Schögel, 2021; Greenaway et al., 2015; K. D. Martin & Murphy, 2017). This also seems to be true for most firms, who often view privacy as a compliance issue or cost factor to

be avoided (Ebert & Widmer, 2018; Linden et al., 2020; Lupiáñez-Villanueva et al., 2022; Nouwens et al., 2020; Pelteret & Ophoff, 2016) rather than an integral part of their marketing function.

As a consequence, we have a detailed understanding on how firms neglecting risks to their customers' privacy can lead to a loss of revenue (Baruh et al., 2017; Chellappa & Sin, 2005; Johnson et al., 2020; Pavlou et al., 2007; Tsai et al., 2011), higher exposure to litigation (Solove, 2013; Son & Kim, 2008) or loss of access to high-quality data (Awad & Krishnan, 2006; Dinev & Hart, 2006; Jiang et al., 2013; K. Martin, 2018; Son & Kim, 2008). Additionally, past studies have suggested, that a reactive, compliance-oriented approach is insufficient in sustainably avoiding these risks (Acquisti et al., 2016; Solove, 2013).

At the same time, comparatively little attention has been paid to the potential upsides of a privacy-oriented strategies (Bleier et al., 2020; Gotsch & Schögel, 2021; K. D. Martin & Murphy, 2017). The effects of individual measures might hint at OPO increasing customer trust and satisfaction (Dehghanpouri et al., 2020; Eastlick et al., 2006; Wu et al., 2012), willingness to share data (Dinev & Hart, 2006; Hui et al., 2007; Morlok, 2016) or firm performance (K. D. Martin et al., 2017). However, these studies lack comparability, since none of them rely on a common conceptualisation of privacy orientation; A problem most privacy research has in common (Smith et al., 2011, p. 997). As such, the goal of this paper is to conceptualise OPO and provide a reliable measurement, so that both potential up- and downsides of a strategic focus on privacy can be tested and compared in future studies.

Conceptualisation of organisational privacy orientation

Previous research on OPO has defined it as “the extent to which a firm delivers consistent, transparent privacy protection to its customers while achieving other important organisational objectives” (Greenaway et al., 2015, p. 580). The definition implies an inherent tension between a firm's demand for customer data to fulfil their objectives and their customers' demand for privacy – an observation which has often been repeated in other studies (Gerlach et al., 2019; Pelteret & Ophoff, 2016). Therefore, OPO is often also eluded to in constructs with a similar trade-off between “short-term profit or market share goals (...) and a culture that fosters the well-being of multiple stakeholder groups” (Allen & Peloza, 2015, p. 636), e.g., as part of corporate social responsibility (Allen & Peloza, 2015; Pollach, 2011), corporate digital responsibility (Lobschat et al., 2021; Wirtz et al., 2022) or environmental, social and governance reporting (ESG) (Bloemendal, 2022).

Analog to those constructs or other “orientation” measurements such as “market orientation” (Alberto Fernandes Sampaio et al., 2018; Kohli et al., 1993) or “green marketing orientation” (Papadas et al., 2017), OPO is usually portrayed as a multi-dimensional construct. Greenaway,

et al. (2015, p. 587) 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 (2005) and the categorisation of the role of privacy in marketing by Martin & Murphy (2017), “privacy orientation” must address consumer antecedents, structural forces, and societal demands. The model of Gotsch & Schögel (2021, p. 12) builds upon these ideas of privacy orientation and proposes a companywide process influenced top down from a strategic level. Table 1 provides an overview of these related constructs and details on how their findings are integrated within this study.

Construct	Definition	Organisational Privacy Orientation (OPO)
Company Information Privacy Orientation (CIPO) (Greenaway et al., 2015)	The extent to which a firm delivers consistent, transparent privacy protection to its customers while achieving other important organisational objectives.	The dimensions of control and justice are reflected in the strategic dimension of OPO, especially in the notion of using privacy as a positioning tool. At the same time, its more tactical implications are reflected within the short-term tactical aspects of OPO.
Corporate Digital Responsibility (CDR) (Lobschat et al., 2021; Wirtz et al., 2022)	The set of shared values and norms guiding an organization’s operations with respect to four main processes related to digital technology and data.	The central conceit of CDR to consider cultural and structural processes as central driver of privacy-oriented behaviour as well as their effects on stakeholders and an ecosystem at large are reflected in the 4-dimensional structure of privacy orientation.
Privacy as Strategy (K. D. Martin et al., 2017; K. D. Martin & Murphy, 2017)	Firms using their consumer information protection approaches as competitive differentiation.	To evaluate the level of privacy offered by any organization, a holistic view blending consumer, organizational, ethical, and legal concerns is necessary – which is why OPO is conceived as a multi-dimensional and reflective construct.
Activity-oriented Customer Centricity (ACC) (Hassler, 2021; Riedmann-Streitz, 2018)	Thinking and acting consistently from the perspective of people based on a forward-looking human-centred attitude and brand vision regarding data-driven marketing activities.	Using strategic marketing as the unifying lens to guide disparate organizational privacy activities.
Digital Trust (Wortmann et al., 2022)	Digital trust in an industry or company is induced across three actionable domains: (1) digital trust strategy, (2) digital trust operating model, (3) digital trust foundation.	The strategic and top-down nature of this digital trust model is also reflected in the strategic dimension of OPO driving its structural, human resource and tactical aspects.
Information security policy compliance culture (Amankwa et al., 2018)	The attitudes, assumptions, beliefs, values, and knowledge that employees use to interact with the organization’s information security systems and procedures at any point in time.	ISPPC provides possible antecedents and relevant constructs for the structural dimensions of OPO.
(Personal) Privacy Orientation (Baruh & Cemalcilar, 2014)	Personal privacy orientation consists of (1) the belief of “privacy as a right” (2) “other-contingent privacy” (3) “concern about own informational privacy” and (4) “concern about privacy of others”.	The four dimensions of personal privacy orientation are incorporated in both the strategic and cultural aspects of OPO as important values to be anchored within employees.

Classification of organisational privacy processes (Gotsch & Schögel, 2021)	Firms can align their privacy practices with customers' expectations across four inter-connected managerial processes: (1) strategic initiatives, (2) structural improvements, (3) human resource management, and (4) service development.	Both the dimensionality and the idea of OPO as an iterative process were taking as a basis in this study to conceptualize the construct.
---	--	--

Table 6-1 Constructs related to organisational privacy orientation.

Synthesizing the results from table 1 and adopting the cultural view suggested by Lobschat et al. (2021) & Greenaway, et al. (2015), this study conceptualises the OPO construct as a reflective construct across four dimensions: strategic privacy orientation, structural privacy orientation, human resource privacy orientation, and tactical privacy orientation. This approach lends itself as a basis for the development of a measurement scale, as it consists of four dimensions, which address both external and internal, short, and long-term activities contributing to privacy orientation.

In the following chapters, each dimension and relevant their sub-dimensions as well as previous research related to them is discussed in more detail.

Strategic Organisational Privacy Orientation

Strategic OPO refers to all actions by general management which “have material effects on the survival and success” (Teece et al., 1997, p. 528) of long-term organisational privacy initiatives. Specifically, the customer data strategy guiding data processing (Greenaway et al., 2015), privacy collaborations with other industry actors (Gotsch & Schögel, 2021; K. D. Martin et al., 2017; Wortmann et al., 2022), positioning within an industry (Gotsch & Schögel, 2021; K. D. Martin & Murphy, 2017) and trust building within one's customer base (Lobschat et al., 2021) all determine strategic OPO.

Martin & Murphy (2017, p. 153) introduced the term “privacy as strategy” into marketing literature and postulated to successfully differentiate a firm from another using privacy practices, it would need to (1) involve its customers in the process, (2) align data processing activities across all aspects of the firm, (3) commit to these changes in the long-term and (4) foster trust in the customer base towards the company. While these recommendations give an impression on how to improve customers' privacy, they do not provide the necessary information to delineate several distinct customer data strategies. Greenaway, at al. (2015) had previously described existing privacy strategies based on who has control over customer data (customer vs. firm vs. third parties) and how said customer data is used within a given business model (exploitation vs. customer centricity). Both ideas were later elaborated upon by Quach, et al. (2022), defining firm-level data strategies as being either sharing-focused (i.e., allowing other industry partners to utilise a firm's collected data) or on monetisation-focused

(i.e., a firm using all data for its own benefits), while still being beholden to privacy laws and demands by customers.

Customer data strategies are formulated within a specific industry context – meaning they are also dependent on how well a firm’s given strategy is supported by its partners. Both new privacy regulations (Peukert et al., 2022) and larger privacy violations (K. D. Martin et al., 2017) have wide-spread spill over effects on a firm’s data strategy. This is largely due to the interconnectedness of most data ecosystems and the prevalence of second party data in marketing (Schneider et al., 2017). As such, past studies have concluded that privacy concerns should also be addressed by an industry at large (Casadesus-Masanell & Hervas-Drane, 2015; Oetzel & Gonja, 2011; Pavlou et al., 2007). To this end, industry-level initiatives like NIST or GAIA-X also serve to improve OPO.

All these strategic efforts pay into improving customers’ trust in data processing and support for data-driven business models (Bauer & Strauss, 2016; Wirtz & Lwin, 2009) or new technologies (Michler et al., 2020). Trust and fairness, fostered by long-term goals which are publicly communicated and internally upheld are essential for OPO (Gotsch & Schögel, 2021; Greenaway et al., 2015; K. Martin, 2018; Wirtz & Lwin, 2009).

Structural Organisational Privacy Orientation

The structural aspects of OPO refer to the rules, architecture and company structure features which are influenced by OPO. This refers 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). It therefore refers to all the forces which guide and inform commercial processing of data, but not to the people working within these structures.

Organisational changes (departmental or company-wide) to foster OPO are most often named when discussing the role the chief privacy officer (CPO) should play in the overall organisational structure (Bamberger & Mulligan, 2010; Solove, 2013) or when talking about inter-departmental data transmission (Hermalin & Katz, 2006). While recommendations about a more customer-centric organisational structure helping to align privacy processes with the needs of customers are sometimes mentioned (Child et al., 2012; Hassler, 2021), they so far have not been substantiated within a quantitative research project. However, it would stand to reason that organisational structures allowing for easier supervision by a data privacy or data governance team would improve OPO (see e.g., Tahaei et al., 2021).

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 organisation, is usually closely influenced by its organisational structure. As such, recommendations to empower consumers by including them into said structure

and providing them with “control over their private data flow” (Prince, 2018, p. 30) are often repeated in privacy research papers (Bleier et al., 2020; N. K. Malhotra et al., 2004; Nissenbaum, 2010; Ozdemir et al., 2017; Raento & Oulasvirta, 2008). How such a system should look like from the technical side is a rich and ongoing stream of research (see e.g., Domingo-Ferrer et al., 2019; Hassan et al., 2020). However, studies on the management side of data privacy architecture – i.e., how it develops and is enforced – are few and far between.

The same knowledge gap is found in managerial approaches to privacy preserving data processing in general. Studies concerned with improving the safety and privacy of data collection processes have been published throughout the last decade (Freudiger et al., 2014; Mohassel & Zhang, 2017; Ribeiro-Navarrete et al., 2021; Rodiya et al., 2013; Vergara-Laurens et al., 2017). Additionally, a wealth of information exists on how to reduce biases and information asymmetry at the point of collection (Alashoor & Baskerville, 2015; Barth et al., 2019; Sundar et al., 2020). Yet, there are only a few studies on how these insights should be incorporated within an organisational context – e.g., recommending fitting time periods for privacy preserving collection (Williams et al., 2016) or restricting collection only to specific data points (Choi et al., 2018).

Finally, the most clearly defined structural force is the overall privacy risk management, which plays a central role in the OPO. Mainly, the idea of enforcing privacy principles through regular privacy audits (Makri & Lambrinoudakis, 2015), insuring against high privacy risks (Cheng et al., 2021) and measuring whether these efforts manifest in higher perceived privacy (Chang et al., 2018). Many of these insights have already been codified into law (GDPR Art. 39, Art. 47, Art. 58) or are requirements of cybersecurity and privacy frameworks (e.g., NIST, ISO, etc.).

Human Resource Organisational Privacy Orientation

Human resource OPO involves building and anchoring the skills, resources, and positions necessary for a privacy-oriented company culture. Such efforts include hiring a diverse team of privacy professionals (Bamberger & Mulligan, 2010; Kayworth et al., 2005; Muscatella, 2020) and fostering employee privacy awareness (Bulgurcu et al., 2017) through regular trainings and early investment in privacy support infrastructure (Schögel & Gotsch, 2021; Solove, 2013).

While privacy research has stressed the importance of an organisational privacy culture for years (Bélanger & Crossler, 2011; Greenaway et al., 2015; Power & Trope, 2007), “there are still few examples and little guidance on how to build privacy culture in organisations” through facilitators such as chief privacy officers or privacy champions (Tahaei et al., 2021, p. 1). Comparing the expected growth in analytical capability and access to customer data even in small enterprises (Bianchini & Michalkova, 2019; Coleman et al., 2016; Sen et al., 2016) with the personnel necessary to successfully navigate modern privacy regulations (see e.g., Peukert et al.,

2022; Teixeira et al., 2020) it becomes clear, how important building a privacy aware human resource pool has become.

At the same time, providing customers with the opportunity to speak to a company representative on regards to its privacy policy, while personnel-intensive, helps in reducing privacy concerns while increasing the perceived procedural fairness (Gotsch & Schögel, 2021, p. 18; Morey & Krajecki, 2016, p. 179; Pötzsch et al., 2010). The importance of this “customer centric” approach to communicating data privacy is often stressed in marketing guides (Hassler, 2021; Palmatier & Martin, 2019) or in commercial blogs (Brodherson et al., 2021; Sarnot, 2020) but has so far only partially been addressed in scientific literature. Still, it would stand to reason, that giving employees tasked with handling customer data and customers alike the opportunity to talk to a privacy champion would have beneficial effects on customer trust and responsible data processing.

As such it is unfortunate, how comparatively little is known about benchmarking or guiding privacy efforts through key performance indicators or similar measures. While benchmarking systems for privacy policies have been proposed (Tesfay et al., 2018), it is still unclear how such tools are or could be used to guide employees needing to comply with them (Z. S. Li et al., 2022).

Tactical Organisational Privacy Orientation

Tactical OPO concerns all short-term actions which aid in providing customers with more transparency and control over their personal data flows within a given organisation. As it is mostly concerned with product or service-related features (de Wolf & Pierson, 2014; Dienlin & Metzger, 2016; Dinev et al., 2009, 2012), or the effective communication of said features (Baruh et al., 2017; Boerman et al., 2018; Hann et al., 2007; Huang & Bashir, 2020), it is probably the most well-researched of the four dimensions. However, other tactics, such as providing compensation for sharing data (Chen et al., 2017; Hann et al., 2007), highlighting the social value of using privacy controls (Morlok, 2016) or nudging costumers within user interfaces to incentivise the use of privacy controls (Acquisti et al., 2017; Kitkowska, Wästlund, et al., 2020) have also been suggested as potential improvements.

The idea of ensuring transparency and control in the design of products and services has been repeated often and across different studies (Beke et al., 2018; Bélanger & Crossler, 2011; K. Martin, 2018; K. D. Martin & Murphy, 2017). Most existing recommendations should be covered by the privacy by design principle, enshrined in regulations such as the GDPR (Art 47 GDPR). Yet, considering how many companies struggle with providing their customers transparency and control over their data flows (Ibdah et al., 2021; Milne et al., 2006; Palmatier & Martin, 2019) or even design their touchpoints to nudge customers into sharing more data (Lupiañez-Villanueva et al., 2022; Nouwens et al., 2020; Waldman, 2020) it is clear that tactical

OPO is just the most visible part of a bigger strategy (Gotsch & Schögel, 2021; Shastri et al., 2019).

Scale development methodology

For the development of a reliable scale, we followed the recommended process laid out by Mackenzie, et al. (2011, p. 297). The design of the individual studies was based on the scale development processes by Walsh & Beatty (2007, p. 131), adapted for strategic management scales by Papadas, et al. (2017, p. 239). Table 2 provides the overview across all 5 five studies – including a qualitative study, item generation, a survey amongst privacy experts as well as two quantitative studies to finalise the scale. Appendix 1 chronicles the conceptualisation of OPO and the definitions of its dimensions and Appendix 3 provides the full initial list of the items created as well as its iterations.

Stages of Scale Development Process	Details
Study 1: Domain specification and dimensions	- Literature review - 36 in-depth interviews, 5 privacy laws and guidelines - The first study confirms the four dimensions comprising the construct “organisational privacy orientation” and provides detailed insights about the strategic, structural, human resource and tactical actions an organization could use to improve their privacy orientation.
Study 2: Sharpening definitions, item generation and expert review	- Qualitative study - 6 management researchers and 4 PhD candidates judge the definitions for the 15 subdimensions and the items for conciseness and validity - Generation of 67 items based on 4 dimensions - 12 items are reworded, 2 are eliminated. Two constructs as well as their subdimension definition are merged. - 65 items are retained for the next step
Study 3: Clarification and rating items by practitioners	- Survey to 41 data privacy professionals - The importance of all 65 items to their dimensions is rated with a scale from 1 to 5 as well as with qualitative feedback. - 51 items are retained for the next step
Study 4: Scale purification and item refinement; initial reliability assessment, factor loadings, dimensionality, item refinement and reduction	- Survey to 353 manager-level executives or business owners from the EU, CH & UK - Exploratory factor analysis - 32 items meet the criteria and are retained for the next and final step
Study 5: Finalization of the scale; reliability and dimensionality, convergent validity, discriminant validity, Nomological validity	- Cross-sectional survey with 387 firms in the EU, CH & UK - Repetition of the exploratory factor analysis, 22 items retained - Confirmatory factor analysis, 4 items deleted - 18 items meet the criteria and are retained for validity tests - Validation of the scale using AMOS - Establishment of nomological validity

Table 6-2 Scale development process

Study I – Domain specification and dimensions

According to Mackenzie, et al. (2011, p. 299), the first step in construct conceptualisation is to undertake a thorough review of the extant literature on organisational privacy literature and “conduct preliminary research using an inductive approach with subject matter experts or practitioners”. To this end, we undertook 36 in-depth interviews with experts and individuals in relevant positions in European companies. Specifically, we talked to 19 data privacy officers, 10 CEO/CMOs of smaller firms with data protection responsibilities as well as 5 data privacy consultants and 2 data privacy auditors. Additionally, we followed the recommendations of several of these interviewees and included the data privacy and security criteria catalogues of the GDPR, the ISO-IEC 27000, GAIA-X, digital trust label, and the NIST Privacy Framework in our documentation. To ensure the relevance of the sample, we made sure to only include experts from B2C companies or companies with direct access to customer data. The composition of the individuals was chosen to ensure familiarity with high privacy standards; We included 11 experts from the (online) retail sector, 9 from the IT/Telecommunication sector, 5 from the banking/fintech sector, 5 data strategy consultants, 3 from the mobility/automotive sector, 2 privacy auditors/trainers and 2 from medical start-ups. Appendix 2 provides an overview to each interview.

The interviews were recorded to ensure a verbatim transcription. Each expert was interviewed based on a previously provided interview guide (Assarroudi et al., 2018, p. 8). Interviews started with open-ended questions with the aim to define “organisational privacy orientation” (e.g., which characteristics do you associate with organisational privacy orientation? What distinguishes an organisation 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?). With all questions, it was made clear that the organisation as a whole is the intended unit of analysis (Graneheim & Lundman, 2004, p. 107).

Their insights were analysed using directed content analysis (Assarroudi et al., 2018; Hsieh & Shannon, 2005) based on the CIPO construct by Greenaway, et al. (2015), Corporate Digital Responsibility (Lobschat et al., 2021) and the classification of organisational privacy processes by Gotsch & Schögel (2021). All models were integrated and served as the main categorisation matrix which was expanded using the emerging new categories through the inductive approach of coding all documents (Assarroudi et al., 2018, p. 9). As a result, the definitions we first identified in the literature review of the theoretically derived 4 main dimensions were slightly adjusted, and additional sub-dimensions formed (see Appendix 1). 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 two additional interviews and the inclu-

sion of recommended criteria catalogues (NIST Privacy Framework; GAIA-X, digital trust label, GDPR implementation guidelines and the ISO-IEC 27000) any further data collection was stopped.

Based on this data, organisational privacy orientation was defined as the extent to which an organisation engages in strategic, structural, human-resource and tactical processes and activities which aim at developing, delivering, and maintaining products and/or services which ensure consistent and transparent privacy protection to its customers. The listing of the main 4 dimensions as well as their definitions can be seen in table 3, the model also including all their sub-dimensions can be found in Appendix 1.

Important to note is that each of the dimensions is “viewed as a manifestation of the focal construct” OPO, which “exists separately at a deeper and more embedded level than its sub-dimensions” (Mackenzie et al., 2011, p. 301). Meaning, we understand OPO as a uni-dimensional construct that is measured across four reflective indicators (Coltman et al., 2008). Therefore, high OPO is understood as giving rise to the strategic, structural, human resource and tactical OPO, which are in turn measurable by observable indicators (Diamantopoulos & Siguaaw, 2006).

Dimensions	Definition
Strategic organizational privacy orientation	The extent to which a firm integrates consistent, transparent privacy protection to its customers in their strategic marketing decisions.
Structural organizational privacy orientation	The extent to which a firm’s established rules, norms or structures guide privacy preserving behaviour.
Human resource organizational privacy orientation	The level of knowledge and assimilation of corporate privacy preserving values by all internal stakeholders.
Tactical organizational privacy orientation	The extent to which privacy preserving values are embodied in tactical marketing decisions.

Table 6-3 Organisational privacy orientation dimensions

Study 2 – Sharpening definitions & item generation

Before any items were generated, the construct’s sub-dimensions, their relationship and their definitions were presented to 6 management researchers as well as 4 doctoral researchers unaffiliated with the study. They were provided with an overview of the study’s progress so far and then confronted with the name of all sub-dimensions as well as their definitions. After each definition they were asked to rate the perceived usefulness (taken from Bosmans, 2006) of the definition, suggest adjustments to the definitions and/or add specific comments regarding the sub-dimensions. Additionally, the reflective nature of OPO is once again considered against a formative conceptualisation. Since both the literature and the results from study 1

suggest a cultural and structural understanding of OPO versus a more behavioural concept which is shaped by a reallocation of resources, a reflective model was favoured (Coltman et al., 2008). The resulting 15 sub dimensions and their definitions build the basis for the formulation of the items.

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 sub-dimension were written by one researcher and reviewed by the other. Care was taken to translate the theoretical dimensions into broader, more comprehensive statements, while adding variations and tangential items to add the necessary redundancy suggested by a reflective approach (Anna Clark et al., 1995, p. 311; Coltman et al., 2008, p. 1252). This process yielded an initial set of 67 items.

These items were then presented to another 5 unaffiliated researchers for a basic pre-test on the items’ clarity, content validity, and face validity (Hardesty & Bearden, 2004). They were instructed with the research team present, and all concerns and notes were recorded. After this process, 12 items were reworded to be more concise, and 2 items were deleted because they were deemed misleading. The resulting 65 items were used as the basis for the next study.

Study 3 – Assessing item validity

Following the steps laid out by Mackenzie, et al. (2011, p. 297) the remaining 64 items were included into a survey to be submitted to expert review. With the aid of the Swiss association for organisational data privacy (“Verein Unternehmerischer Datenschutz”, VUD) and the International Association of Privacy Professionals (IAPP) the items were evaluated by 41 data protection officers from Switzerland and the European Union. 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 (Papadas et al., 2017, p. 240). Additionally, each participant was asked to comment on the items’ face validity and content validity (Assarroudi et al., 2018; Hardesty & Bearden, 2004) 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 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.

The resultant 51 items were presented one last time to a group of 4 marketing doctoral researchers who were tasked with assigning the items to the four OPO dimensions and asked to evaluate their clarity and conciseness. The set of 51 items was then translated into German, once again presented to 3 doctoral researchers for an evaluation of clarity and then retained for the next step in the scale development process.

Study 4 – Scale purification and item refinement

All 51 items were scaled to a 7-point Likert scale (1= strongly disagree to 7= strongly agree) to “provide more varieties of options which in turn increase the probability of meeting the objective reality of people” (Joshi et al., 2015, p. 398) while still allowing participants to easily and quickly gauge their preferred answer (Dawes, 2008). For pilot testing, a “convenience sample” of 16 employees with management experience was recruited over a survey exchange platform (Netemayer et al., 2003, p. 116). Since the testing revealed no difficulties in understanding, the survey was sent out in German and English. To guarantee sample representativeness, the survey was distributed through a closed pool of 1584 managers and the official mailing list of the Swiss Marketing Association containing 3121 marketing professionals. The mailing with reminders yielded 426 completed surveys. These were further screened to exclude answers from people who failed the attention checks or whose professional profile did not include any managerial responsibilities or managerial experience. Table 4 provides a basic overview of the study’s participants.

The resulting 353 answers were used in an exploratory factor analysis (EFA) using direct oblimin rotation for constructs with multiple dimensions (Brown, 2009), to reduce the number of viable items and test the underlying dimensions of the OPO construct (Watkins, 2018). The parallel analysis methodology (Glorfeld, 1995) was used to select the number of factors to retain and to “avoid proliferation of superfluous constructs and weak theories” (Patil et al., 2008, p. 170).

The resulting four factors were mostly consistent with theory. It was found that most theorised aspects of human resource OPO either loaded only on the structural construct or showed factor loadings below 0.5. However, since all the customer interaction related aspects of HR OPO loaded on a single vector, it was decided to retain it as a new dimension called customer centric OPO (CC OPO). All 4 factors explained 57.3% of variance, above the adequate level of validity average to be accepted (Mackenzie et al., 2011, p. 314; Merenda, 2019, p. 160; Peterson, 2000, p. 261). Additionally, to avoid issues of cross loadings, factor loadings ranging between 0.60 and 0.90, and corrected item-to-total correlations of 0.50 and above, 19 items were removed from the scale.

The resulting factors were tested for reliability using Cronbach’s Alpha (Coltman et al., 2008, p. 1252). All values were found to be satisfactory (Strategic OPO = .928, Structural OPO = .932, CC OPO = .886, Tactical OPO = .728), with the first three suggesting fitting redundancy in the items due the high alpha value while the tactical OPO meeting the recommended threshold of 0.7%, suggesting some items might need to be reworded to be more precise (Taber, 2018). A final set of 32 items was used as the basis for the final step of the scale development process.

Categories		% (n = 353)
Professional Experience in current position	1-5 years	43.6%
	>5 years	56.4%
Job post	Upper management	12.5%
	Middle management	39.7%
	Junior management	19.3%
	Employee with management responsibilities	28.6%
Market	B2C	31.2%
	B2B	24.4%
	B2B&B2C	44.4%
Country	Switzerland, UK, Liechtenstein	51.4%
	EU	48.6%

Table 6-4 Study 4 – sample characteristics

Study 5 – Finalisation and validation of the scale

To finalise the scale, the EFA was followed up by a second, large quantitative study to confirm the developed scale's dimensionality, reliability, and validity (Coltman et al., 2008; Mackenzie et al., 2011).

The questionnaire was rewritten to feature only the 32 OPO items and included a marketing and financial performance scale (Fraj et al., 2011), a measurement of competition intensity (Homburg et al., 2012), an information security policy compliance culture scale (Amankwa et al., 2018), and a general corporate social responsibility scale (Turker, 2009) to assess the validity of the OPO scale. All scales and their wording used in this study can be found in Appendix 4.

A sample of managers from publicly traded customer facing companies from the EU, UK, Switzerland, and Liechtenstein was recruited through the research platform prolific.co. All participants were filtered with the platforms' filter options according to the above stated inclusion criteria and paid for filling out the questionnaire. 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 (see GDPR Art. 13, Möhle, 2021).

The recruiting process yielded 418 participants. These were filtered to exclude any participants who failed attentions checks. 387 answers were chosen as a basis for the final study. Table 5 details the characteristics of the sample used.

Categories		% (n = 387)
Professional Experience in current position	1-5 years	60.7%
	>5 years	39.3%
Job post	Upper management	3.9%
	Middle management	25.1%
	Junior management	23.0%
	Employee with management responsibilities	55.5%
Market	B2C	42.9%
	B2B&B2C	57.1%
Country	Switzerland, UK, Liechtenstein	74.9%
	EU	24.1%
Industry	Accounting	1.0%
	Administration & Office Support	2.3%
	Advertising, Arts & Media	1.0%
	Banking & Financial Services	11.9%
	Customer Service	2.3%
	Construction & Architecture	1.5%
	Consulting	0.5%
	Training & Education	7.0%
	Engineering	3.9%
	Government & Defence	5.4%
	Healthcare & Medical	12.1%
	Hospitality & Tourism	4.9%
	Human Resources & Recruiting	0.3%
	IT & Communication	9.0%
	Insurance	2.1%
	Manufacturing & Logistics	7.5%
	Marketing	0.5%
	Resources & Energy	1.3%
	Real-Estate & Property	1.3%
	Retail & FMCG	15.0%
	Sales	1.6%
	Science & Technology	2.3%
	Trades & Services	1.3%

Table 6-5 Study 5 - sample characteristics

Reliability assessment and dimensionality

Prior to the confirmatory factor analysis, the exploratory factor analysis with direct oblimin rotation from study 4 was repeated the same way (Papadas et al., 2017). The results again confirmed the construct's dimensionality, showing the same four-factor structure and explaining 65.8% of total variance. To remove superfluous items, all cross-loading items and items with a factor loading outside the 0.6 to 0.9 range were removed. After deleting 10 items, all others loaded onto their single predicted factor, suggesting no further elimination of items is necessary. Cronbach's Alpha was calculated for each factor to assess reliability, with Strategic

OPO = .868, Structural OPO = .917, CC OPO = .904 and Tactical OPO = .805. Each individual item within each of the dimensions showed an average item to total correlation of .708 and all exceeded .568 – demonstrating satisfactory levels of internal consistency (Taber, 2018). As such, 22 items were retained for the next step.

Convergent and discriminant validity

All items of the scale were loaded to their respective dimensions in a confirmatory factor analysis. All indicators loaded significantly on their theoretical dimensions. To improve model fit, the standardised residual covariances were observed and 4 items with more than 2 instances of standardised residual covariance of >2.0 were removed from the model (Maydeu-Olivares & Shi, 2017). The resulting measurement model with 18 items provided a good fit to the data ($\chi^2 = 383.407$; $df = 129$; $p < 0.001$; $CFI = 0.94$; $TLI = .93$; $RMSEA = 0.07$; $\frac{PCMIN}{DEF} = 2.97$; $SRMR = 0.05$) and was chosen for the final configuration of the scale.

Table 6 shows the final list of the 18 retained items within their respective dimensions. Their respective ranges, factor loadings, means and standard deviations are listed as well.

Factor Item ("At my company...")	Range	Mean	SD	Load
<i>Strategic organizational marketing orientation (alpha =0.837)</i>				
1. top management explicitly names data privacy as an important part of our company's strategy.	1-7	5.35	1.64	0.85
2. top management emphasizes that the protection of costumers' data privacy is the responsibility of each employee.	1-7	5.66	1.54	0.85
3. the protection of the data privacy of customers is named within our mission statement.	1-7	4.79	1.83	0.70
<i>Structural organizational marketing orientation (alpha =0.913)</i>				
1. we have created a separate department specializing in data privacy issues.	1-7	4.61	2.07	0.64
2. we have clear guidelines on how to react to a detected personal data breach.	1-7	5.33	1.83	0.80
3. all accesses to our customer data are logged and recorded.	1-7	5.20	1.81	0.79
4. we regularly conduct internal privacy risk assessments with a clearly defined scope.	1-7	4.83	1.84	0.87
5. we conduct an external privacy audit at least once every year.	1-7	4.84	1.86	0.71
6. our company has a system in place that ensures that improper or frequent accesses to customer data are immediately noticed.	1-7	4.89	1.77	0.84
7. we organize presentations for our employees to inform them about our data privacy regulations.	1-7	4.85	1.96	0.70
8. we have access to an online archive or training platform, where our employees can learn about our privacy regulations.	1-7	5.26	1.90	0.69
<i>Customer centric organizational marketing orientation (alpha =0.920)</i>				
1. our customers understand, what data we collect from them.	1-7	5.11	1.61	0.89
2. our customers understand, why we collect data from them.	1-7	5.21	1.53	0.91
3. our data processing activities are transparent to our customers.	1-7	5.09	1.63	0.88
<i>Tactical organizational marketing orientation (alpha =0.805)</i>				
1. we only collect enough data from customers to fulfil their order(s).	1-7	5.25	1.61	0.66

2.	our customers can test our products and services without sharing a lot of personal data.	1-7	4.25	1.93	0.66
3.	we do not collect customer data unless the customer receives a clear benefit in return.	1-7	4.18	1.85	0.71
4.	we make efforts to use as little personal data for our products and services as possible.	1-7	4.59	1.74	0.85

Table 6-6 Study 5 scale items with descriptive statistics and factor loadings

Convergent validity was tested by additionally looking at inter-item correlations of each dimension. All of them exceeded a value of 0.5, suggesting convergent validity. Additionally, average variance extracted (AVE) was calculated for each construct exceeded the recommended level of 0.5 (dos Santos & Cirillo, 2021). 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 (Voorhees et al., 2016, p. 124). An overview is provided in Table 7.

Construct	AVE	Squared correlations			
		1	2	3	4
1. Strat.OPO	0.64				
2. Struc.OPO	0.59	0.49			
3. CC OPO	0.79	0.26	0.34		
4. Tact.OPO	0.52	0.09	0.18	0.27	
5. CSR	0.68	0.20	0.32	0.22	0.27
6. Competition	0.75	0.01	0.05	0.01	0.04
7. SOC	0.53	0.48	0.70	0.36	0.20
8. Lead	0.75	0.38	0.51	0.31	0.18
9. MP	0.54	0.12	0.18	0.16	0.12

Table 6-7 Study 5 - Discriminant validity tests

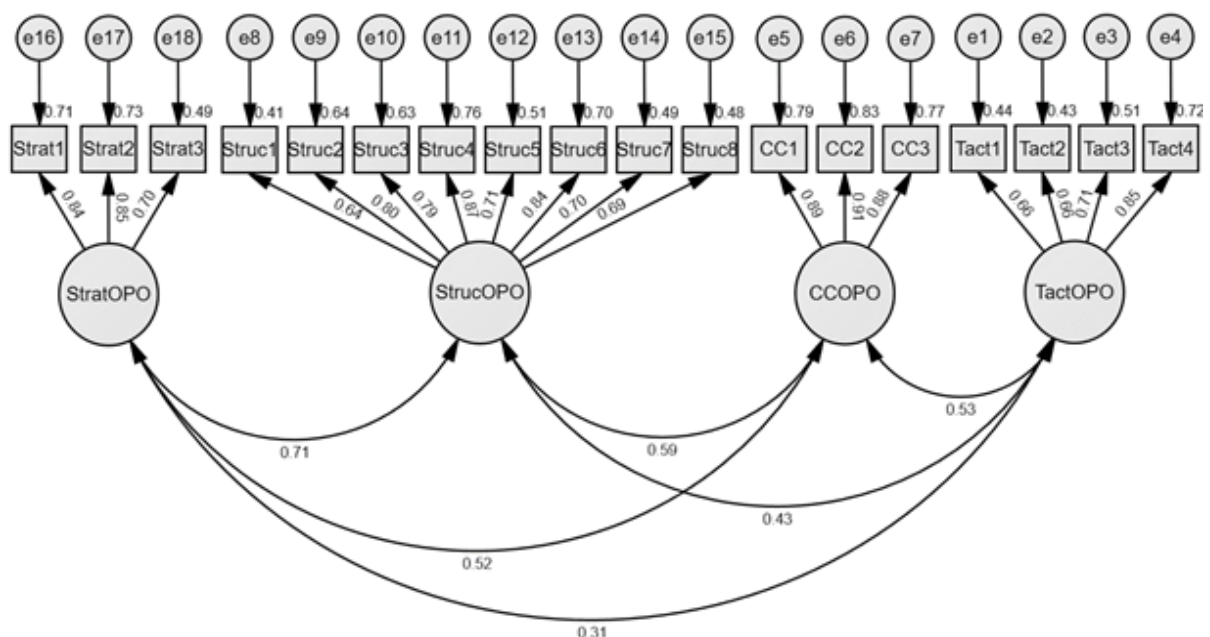


Figure 6-1 Study 5, CFA model and results for the OPO scale. Note: all coefficient values are standardised and appear next to the associated path (all values sig. at a $p < 0.001$ level).

Nomological validity

To test whether OPO exhibits not just predictive but also nomological validity, a system of antecedents and consequences for the construct was formulated, pre-registered on Wharton's "as predicted" service and tested in the final sample (Hagger et al., 2017, p. 3). This study relied on structural equation modelling to investigate three antecedents of OPO, and two potential consequences identified in study 1. Each was operationalised with a previously established scale, using a measurement of competition intensity (Homburg et al., 2012), an information security policy compliance culture scale (Amankwa et al., 2018) and a general corporate social responsibility scale (Turker, 2009) used for antecedents as well as a marketing and financial performance scale (Fraj et al., 2011) for the consequences. Appendix 4 details the used items as well their alpha and mean values. Using SPSS AMOS, a structural model was estimated and demonstrated a good fit for the data ($\chi^2 = 2358.993$; $df = 1053$; $p < 0.001$; $CFI = 0.91$; $TLI = .90$; $RMSEA = 0.06$; $\frac{PCMIN}{DEF} = 2.24$; $SRMR = 0.06$). An overview to the model in fig. 2 can be found in table 8 which illustrates the correlations among all the OPO dimensions and variables as well as the paths of the nomological validity test.

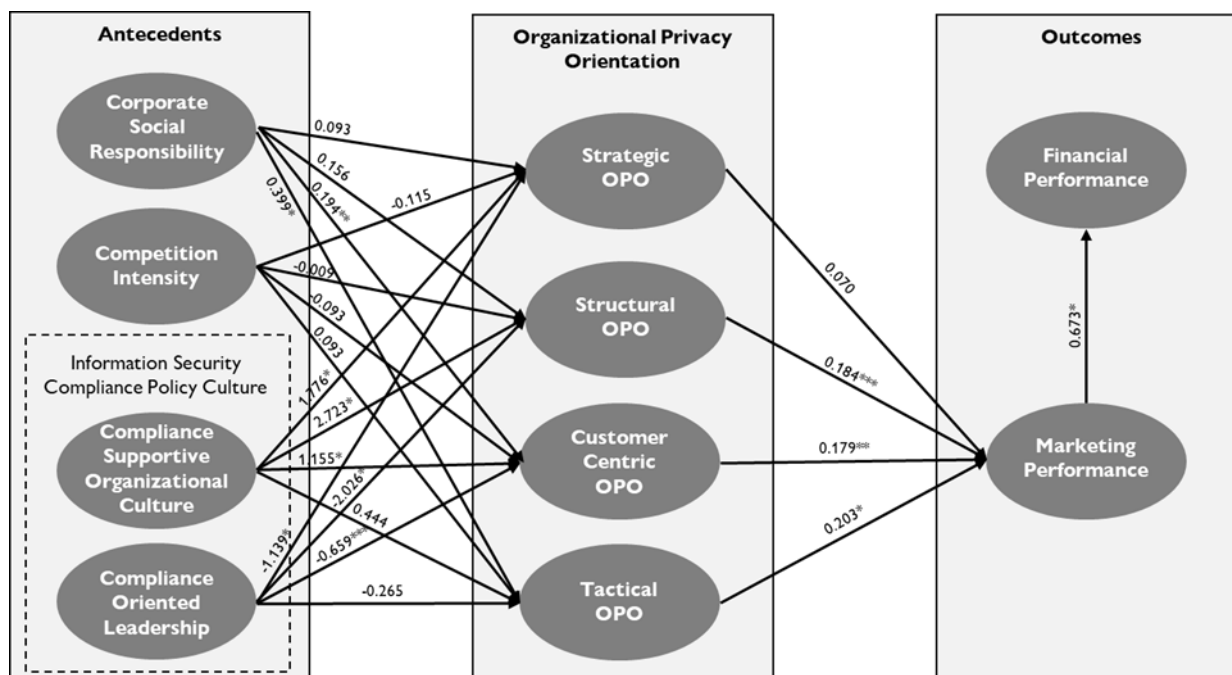


Figure 6-2 Study 5, test of the nomological validity of the scale. Note: all path coefficients are standardised estimates. *** $p < 0.05$ / ** $p < 0.01$ / * $p < 0.001$

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., 2022), it was included as an antecedent. It was found that it drives the tactical and customer centric OPO dimensions ($\beta = .399$, $p < 0.001$; $\beta = .194$, $p <$

0.01). However, CSR did not significantly affect the strategic and structural OPO dimensions ($\beta = .0093, p = 0.246$; $\beta = .156, p = 0.120$). Since both the strategic and structural OPO dimensions are focused on how data is used and its processing enforced within a company, it would make sense that the more general stakeholder benefit focus of CSR would only drive the downstream benefits of OPO. Since both CSR and tactical and CC OPO are focused on procedural justice within a company, its influence is bound to be felt the strongest there (Greenaway et al., 2015).

To predict the strategic and structural aspect of OPO two variables associated with information security policy compliance culture were included – namely a compliance supportive organisational culture (SOC) and an information security policy compliance leadership (LEAD) (Amankwa et al., 2018). The model supports this prediction, with SOC being a potential driver to strategic OPO ($\beta = 1.176, p < 0.001$), structural OPO ($\beta = 2.723, p < 0.001$), and CC OPO ($\beta = 1.155, p < 0.001$), but not tactical OPO ($\beta = 0.444, p = 0.091$). Yet, an overly strict security policy compliance leadership was found to significantly reduce strategic OPO ($\beta = -1.139, p < 0.001$), structural OPO ($\beta = -2.026, p < 0.001$) and CC OPO ($\beta = -0.659, p < 0.05$), but not tactical OPO ($\beta = -0.265, p = 0.311$). This finding suggests that a purely compliance orientated leadership is inconducive to a more holistic understanding of organisational privacy which does not only involve top-down edicts but also a corresponding culture and support network of employees. This argumentation is in line with the research of Alholgail & Mirza (2014) that also suggests that employees and users should be closely involved in data security and privacy decision making to instil a sense of ownership. Additionally, it corroborates long-standing recommendations in privacy literature to switch from a “reactive” compliance orientation to a more “proactive” privacy culture (Gotsch, 2022; Hull, 2015, p. 99; Lanier & Saini, 2008, p. 28).

The final antecedent, competition intensity (COMP), was included because it has been hypothesised to play an “important role” in shaping how well firms could compete with a privacy positioning (Casadesus-Masanell & Hervas-Drane, 2015, p. 242) and because – like with CSR – would impede the long-term innovation and learning cycle necessary for anchoring privacy learning processes within a firm (Vilanova et al., 2009). However, COMP showed no significant effect on OPO, neither on the strategic ($\beta = -0.115, p = 0.084$), structural ($\beta = -0.009, p = 0.910$), CC ($\beta = -0.093, p = 0.096$) nor tactical ($\beta = 0.093, p = 0.085$) dimensions. Potentially, the small effect size and significance was caused by the variable being measured with a self-assessment scale, which might not fully correlate with the actual competition intensity in the market. However, since the theoretical basis for the effect is strong and almost fell within an acceptable significance level, it would be worth to revisit competition intensity as a potential antecedent to OPO in a future study.

Finally, our interviews as well as previous studies (K. D. Martin et al., 2017) suggest, that an increased OPO could lead to higher levels of marketing performance (MP) by more closely aligning customers’ privacy expectations with the data processing of a given firm (Gotsch &

Schögel, 2021). This in turn would ideally translate into higher financial performance (FP). At this point it must be acknowledged that both MP and FP are measured subjectively within this study. Meaning they provide adequate data to establish a positive link in the context of nomological validity but are not to be understood as a causal relationship. Within this context, all customer facing measures of OPO, meaning the structural ($\beta = 0.184, p < 0.05$), CC ($\beta = 0.179, p < 0.01$) and tactical ($\beta = 0.203, p < 0.001$) aspects of OPO have a positive effect on MP, which in turn is a significant driver for FP ($\beta = 0.673, p < 0.001$). On the other hand, the effect of strategic OPO on MP is non-significant ($\beta = 0.070, p = 0.387$), which may result from its focus providing results which are only experienced over years rather than individual encounters. However, since strategic OPO is responsible for the alignment of the other OPO dimensions, it could be positively linked with other important organisational measurements such as organisational identification or employee satisfaction (Park & Back, 2020).

Path	β (standardized)	S.E.	p
CSR → Strat. OPO	+0.093	0.072	0.246
CSR → Struc. OPO	+0.156	0.086	0.120
CSR → CC OPO	+0.194	0.063	0.004
CSR → Tact. OPO	+0.399	0.048	<0.001
COMP → Strat. OPO	-0.115	0.057	0.091
COMP → Struc. OPO	-0.009	0.069	0.910
COMP → CC OPO	-0.093	0.050	0.084
COMP → Tact. OPO	+0.093	0.035	0.096
SOC → Strat. OPO	+1.776	0.367	<0.001
SOC → Struc. OPO	+2.723	0.652	<0.001
SOC → CC OPO	+1.155	0.312	<0.001
SOC → Tact. OPO	+0.444	0.218	0.091
LEAD → Strat. OPO	-1.139	0.338	<0.001
LEAD → Struc. OPO	-2.026	0.587	<0.001
LEAD → CC OPO	-0.659	0.289	0.016
LEAD → Tact. OPO	-0.265	0.202	0.311
Strat. OPO → MP	+0.070	0.055	0.387
Struc. OPO → MP	+0.184	0.064	0.042
CC OPO → MP	+0.179	0.043	0.007
Tact. OPO → MP	+0.203	0.056	<0.001
MP → FP	+0.673	0.068	<0.001

Table 6-8 Study 5, statistics for the paths of the nomological validity test

In total, the test showed that OPO can be supported in a nomological network featuring related antecedents and consequences. Hence, it sheds first light on the patterns and relations which drive and are driven by the construct (Hagger et al., 2017).

Discussion

The digitalisation of most aspects of our lives will most likely continue for years to come. For each stakeholder to profit from the data streams captured from customers and directed towards companies, the latter need to build their awareness and competences for data privacy and security. However, to evaluate which strategies positively contribute to OPO, marketers need a uniform conceptualisation of the construct and know how to measure it. Hence, the contribution of this paper is threefold: 1) in a 5-step scale development process, we created the first holistic measurement for privacy orientation on an organisational level; 2) building on previous research and our own studies, we conceptualise OPO as a four-dimensional construct; 3) by testing the nomological validity of the construct, we provide first insights in the previously only hypothesised benefits of a more holistic focus on organisational privacy. All these results provide a series of theoretical and managerial implications, which are discussed below.

Theoretical implications

The central theoretical contribution of this study is to unite previous research streams on the role of privacy on an organisational level (K. D. Martin & Murphy, 2017) to conceptualise and operationalise a model of organisational privacy orientation and construct a comprehensive and tested framework to set a basis for future privacy research. In total, our results provide three main theoretical implications.

First, our results categorise the insights of earlier studies into organisational privacy (e.g., Gotsch & Schögel, 2021; Greenaway et al., 2015; Lobschat et al., 2021) by updating and confirming the dimensionality of the construct. So far, previous literature has focused on the strategic (Brodherson et al., 2021; Hassler, 2021; K. D. Martin et al., 2017; K. D. Martin & Murphy, 2017) and tactical aspects (Acquisti et al., 2020; Adjerid et al., 2018; Lanier & Saini, 2008) of organisational privacy. Yet, our interviews as well as the scale itself demonstrate, that the structural forces shaping OPO as well as the people working within these structures are paramount in securing data privacy within organisations. This holistic understanding of OPO allows both managers and consumers to distinguish between companies with a long-term investment in their privacy and companies using only superficial transparency and control at the touchpoint level to nudge customers into giving consent to share their data (see also Lupiáñez-Villanueva et al., 2022).

Second, the five studies provide researchers with a solid conceptualisation of OPO, which offers a holistic view on privacy from a businesses' perspective. Both the qualitative insights from study 1-3 as well as the quantitative insights from study 4 and 5 based on relevant samples confirm the feasibility of the construct as well as its reliability and validity. As such, it

may prove a useful foundation for future privacy research in an organisational context and allow for the comparability of said studies.

Third, the fifth study gives support to the hypothesised positive effects of OPO on marketing and firm performance. While forthcoming privacy practices have been linked to firm performance in the past (K. D. Martin et al., 2017), it was usually framed from the perspective of crisis avoidance, rather than an asset in and of itself. Our results find that structural, CC and tactical OPO may be drivers of marketing performance in general. Additionally, by looking at compliance culture and CSR as antecedents, we provide a more nuanced understanding of how OPO is distinct but related to both constructs. The correlations between the four OPO dimensions also support the hypothesis that privacy orientation is guided by the strategic dimension and from there shows its effects on the other, more short-term oriented dimensions. Consequently, the results highlight the value of looking at OPO holistically to understand why some organisations enjoy the trust of their customers regarding data privacy and some do not, despite similar tactical OPO choices (see e.g., de Langhe & Puntoni, 2021).

Managerial implications

This study provides useful insights to (marketing-) managers looking to align their data processing activities more closely with the privacy expectations of their customers. Firstly, by understanding OPO as a four-dimensional construct across various levels of organisational hierarchy, the analysis of potential weaknesses becomes clearer. As an example, if all previous privacy efforts went into easily understandable privacy features on the touchpoint level without investing equivalently into structural OPO, customers' privacy vulnerability is still increased due to potential mishandling of data by employees. Similarly, if an effective data governance team has been assembled but it has neither the support from top management nor is known by the employees processing customer data, their efforts are likely to be wasted. As such, companies might use the OPO construct as a template to devise data privacy strategies, starting at the strategic level down to HR and structural measures, which in turn manifest in effective day-to-day tactical decisions.

Secondly, from the relationship between each of the dimensions, implications on building a privacy-oriented organisation can be drawn. Seeing how privacy orientation is likely determined top-down, both through strategic direction and a corresponding company culture, it presents a logical starting point for a discussion on OPO. If the business model stands in conflict with privacy preserving values (e.g., by relying exclusively on the capture of behavioural surplus data), it can be presumed that no amount of investment in research and development or privacy controls on the touchpoint level will increase OPO. However, it is not enough for an organisation to orientate itself only around legal compliance, as study 5 showed that a purely compliance driven leadership is likely to reduce the potential benefits which could be gained from OPO. As a contrast, a compliance supportive organisational culture and a focus

on CSR in general are likely to create the kind of organisational culture and human resource pool which allows for the processing of customer data while still fulfilling their customers' privacy needs. From there, a truly unique and future proof human resource pool can be built.

Finally, the nomological validity test provides first indices that organisations able to increase their privacy orientation might do so to the benefits of their marketing and financial performance. On the one hand, by creating a respectful data processing culture, which understands privacy as a collective endeavour and a vital part of the customer experience, rather than a limitation of it. On the other hand, growing the strategic, structural, HR and tactical competences for a privacy-oriented organisations may result in a unique and hard to imitate set of organisational capabilities with applications in other fields of marketing (e.g., innovation marketing, data analytics, customer retention, etc.).

Limitations and directions for further research

The results of this study are to be understood within the following limitations. First, while study 1 was based on several extensive systematic literature reviews and interviews with a balanced mix of industry professionals, they are by no means representative for any specific industry or market. As such, a narrower investigation of industry-specific organisational privacy practices might capture a deeper understanding of individual privacy practices. Applying the OPO 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 OPO 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, in study 3 we focused our sample on privacy 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 OPO. Consequently, we suggest future studies focus on evaluating OPO from the perspective of different stakeholders to draw comparative results and to further expand our understanding of OPO.

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 organisations in a business to consumer (B2C) market. However, we suspect that the benefits of privacy orientation might also increase the digital trust in organisations looking to participate

in a larger data ecosystem (Wortmann et al., 2022). Future studies might therefore use the OPO construct to explore its benefits and downsides in a business-to-business context.

Finally, the results of our last study 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. By using a longitudinal study design or using market data in combination with the OPO scale, additional insights into its effects are sure to be gained.

Conclusion

This paper conceptualises organisational privacy orientation (OPO) as an organisation-wide effort to provide consistent, transparent privacy protection while allowing for data processing to better satisfy customers' needs. Consumers grow increasingly savvy with regards to their personal data and about how their information is used for marketing. As such, firms looking to respect this growing need have a corresponding obligation to understand how privacy is guaranteed and protected within an organisational setting.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, 30(4), 736–758. <https://doi.org/10.1002/jcpy.1191>
- 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 Reference Format. *ACM Computing Surveys*, 50(3), 1–41. <https://doi.org/10.1145/3054926>
- Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly: Management Information Systems*, 42(2), 465–488. <https://doi.org/10.25300/MISQ/2018/14316>
- Alashoor, T., & Baskerville, R. (2015). The Privacy Paradox: The Role of Cognitive Absorption in the Social Networking Activity. *Proceedings of the 22nd Americas Conference on Information Systems*, 1–20.
- Alberto Fernandes Sampaio, C., Manuel Hernández-Mogollón, J., & Gouveia Rodrigues, R. (2018). Market Orientation and Hotel Industry: Developing a Measurement Model. *International Conference on Innovation, Engineering and Entrepreneurship*, 1058–1065.
- Alhogail, A., & Mirza, D. A. (2014). A Framework for Information Security Culture Change. *Journal of Theoretical and Applied Information Technology*, 20(2). www.jatit.org
- 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>
- Anna Clark, L., Watson, D., & Clark, A. (1995). Constructing Validity: Basic Issues in Objective Scale Development. *Psychological Assessment*, 7(3), 309–319.
- 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>
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly: Management Information Systems*, 30(1), 13–28. <https://doi.org/10.2307/25148715>
- 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
- Bandara, R., Fernando, M., & Akter, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. In C. / P. / CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies (Ed.), *Procedia Computer Science* (Vol. 121, pp. 562–567). Elsevier B.V. <https://doi.org/10.1016/j.procs.2017.11.074>
- Barth, S., & de Jong, M. D. T. (2017). The Privacy Paradox - Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior - A Systematic Literature Review. *Telematics and Informatics*, 34, 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55–69. <https://doi.org/10.1016/j.tele.2019.03.003>

- Baruh, L., & Cemalcilar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences*, 70, 165–170. <https://doi.org/10.1016/J.PAID.2014.06.042>
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Bauer, C., & Strauss, C. (2016). Location-based advertising on mobile devices A literature review and analysis. *Management Review Quarterly*, 66, 159–194. <https://doi.org/10.1007/s11301-015-0118-z>
- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. In *Foundations and Trends in Marketing* (Vol. 11, Issue 1). <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.IJR-ESMAR.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>
- Bosmans, A. (2006). Scents and Sensibility: When Do (In)Congruent Ambient Scents Influence Product Evaluations? *Journal of Marketing*, 70, 32–43. <http://www.marketingpower.com/jmblog>.
- Brodherson, M., Broitman, A., Chero, J., & Robinson, K. (2021). Marketing in a privacy-first world. *McKinsey and Company Blog*. <https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/a-customer-centric-approach-to-marketing-in-a-privacy-first-world>
- Brough, A. R., & Martin, K. D. (2021). Consumer Privacy During (and After) the COVID-19 Pandemic. *Journal of Public Policy and Marketing*, 40(1), 108–110. <https://doi.org/10.1177/0743915620929999>
- Brown, J. D. (2009). Choosing the Right Type of Rotation in PCA and EFA. *JALT Testing & Evaluation SIG Newsletter*, 13(3), 1–6. <https://hosted.jalt.org/test/PDF/Brown31.pdf>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2017). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. In *MIS Quarterly* (Vol. 34, Issue 3). <https://doi.org/10.2307/25750690>
- Casadesus-Masanell, R., & Hervás-Drane, A. (2015). Competing with privacy. *Management Science*, 61(1), 229–246. <https://doi.org/10.1287/mnsc.2014.2023>
- Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 35(3), 445–459. <https://doi.org/10.1016/J.GIQ.2018.04.002>
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management* 2005 6:2, 6(2), 181–202. <https://doi.org/10.1007/S10799-005-5879-Y>
- 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>
- Cheng, Y., Mei, S., Zhong, W., & Gao, X. (2021). Managing consumer privacy risk: The effects of privacy breach insurance. *Electronic Commerce Research*, 1–35. <https://doi.org/10.1007/S10660-021-09492-X/FIGURES/4>
- 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>
- Cisco. (2019). *Consumer Privacy Survey - The growing imperative of getting data privacy right*. <https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf>
- Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorell, X., & Reis, M. S. (2016). How Can SMEs Benefit from Big Data? Challenges and a Path Forward. *Quality and Reliability Engineering International*, 32(6), 2151–2164. <https://doi.org/10.1002/qre.2008>
- Coltman, T., Devinney, T. M., Midgley, D. F., & Venaik, S. (2008). Formative versus reflective measurement models: Two applications of formative measurement. *Journal of Business Research*, 61(12), 1250–1262. <https://doi.org/10.1016/J.JBUSRES.2008.01.013>
- Dawes, J. (2008). Do data characteristics change according to the number of scale points used? *International Journal of Market Research*, 50(1), 61–77. <https://www.researchgate.net/publication/312458209>
- de Langhe, B., & Puntoni, S. (2021, February 2). Facebook's Misleading Campaign Against Apple's Privacy Policy. *Harvard Business Review*. <https://hbr-org.cdn.ampproject.org/c/s/hbr.org/amp/2021/02/facebooks-misleading-campaign-against-apples-privacy-policy>
- de Wolf, R., & Pierson, J. (2014). Who's my audience again? Understanding audience management strategies for designing privacy management technologies. *Telematics and Informatics*, 31(4), 607–616. <https://doi.org/10.1016/j.tele.2013.11.004>
- Dehghanpouri, H., Soltani, Z., & Rostamzadeh, R. (2020). The impact of trust, privacy and quality of service on the success of E-CRM: the mediating role of customer satisfaction. *Journal of Business & Industrial Marketing*, 1–17. <https://doi.org/10.1108/JBIM-07-2019-0325>
- Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, 17(4), 263–282. <https://doi.org/10.1111/j.1467-8551.2006.00500.x>
- 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., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Dinev, T., Xu, H., & Smith, H. J. (2009). Information privacy values, beliefs and attitudes: An empirical analysis of web 2.0 privacy. *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*, 1–10. <https://doi.org/10.1109/HICSS.2009.255>
- 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>
- Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Computer Communications*, 140–141, 38–60. <https://doi.org/10.1016/J.COMCOM.2019.04.011>
- dos Santos, P. M., & Cirillo, M. Â. (2021). Construction of the average variance extracted index for construct validation in structural equation models with adaptive regressions. *Communications in Statistics: Simulation and Computation*. <https://doi.org/10.1080/03610918.2021.1888122>
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. <https://doi.org/10.1016/j.jbusres.2006.02.006>
- Ebert, N., & Widmer, M. (2018). *Datenschutz in Schweizer Unternehmen 2018*. ZHAW Zürcher Hochschule für Angewandte Wissenschaften. <https://doi.org/10.21256/ZHAW-4001>
- 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>

- Freudiger, J., Rane, S., Brito, A. E., & Uzun, E. (2014). Privacy Preserving Data Quality Assessment for High-Fidelity Data Sharing. *WISCS '14: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 21–29. <https://doi.org/10.1145/2663876.2663885>
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, 77, 226–261. <https://doi.org/10.1016/j.cose.2018.04.002>
- 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>
- Glorfeld, L. W. (1995). An Improvement on Horn's Parallel Analysis Methodology for Selecting the Correct Number of Factors to Retain. *Educational and Psychological Measurement*, 55(3), 377–393. <https://doi.org/https://doi.org/10.1177/0013164495055003002>
- Gotsch, M. L. (2022). Customer Centricity & Datenschutz - Die Geschichte eines Missverständnisses. *Marketing Review St. Gallen*, 2022(2), 12–19. <https://www.alexandria.unisg.ch/265774/>
- 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>
- Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, 24(2), 105–112. <https://doi.org/10.1016/j.nedt.2003.10.001>
- Greenaway, K. E., & Chan, Y. E. (2005). Theoretical Explanations for Firms' Information Privacy Behaviors. *Journal of the Association for Information Systems*, 6(6), 171–198. <https://doi.org/10.17705/1jais.00068>
- 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>
- Hagger, M. S., Gucciardi, D. F., & Chatzisarantis, N. L. D. (2017). On nomological validity and auxiliary assumptions: The importance of simultaneously testing effects in social cognitive theories applied to health behavior and some guidelines. *Frontiers in Psychology*, 8(11), 1–14. <https://doi.org/10.3389/FPSYG.2017.01933/FULL>
- 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>
- Hardesty, D. M., & Bearden, W. O. (2004). The use of expert judges in scale development. Implications for improving face validity of measures of unobservable constructs. *Journal of Business Research*, 57(2), 98–107. [https://doi.org/10.1016/S0148-2963\(01\)00295-8](https://doi.org/10.1016/S0148-2963(01)00295-8)
- Hassan, M. U., Rehmani, M. H., & Chen, J. (2020). Differential Privacy Techniques for Cyber Physical Systems: A Survey. In *IEEE Communications Surveys and Tutorials* (Vol. 22, Issue 1, pp. 746–789). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/COMST.2019.2944748>
- Hassler, M. (2021). *Von Data-Driven zu People-Based Marketing* (1st ed.). mitp.
- 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>
- 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>
- Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- 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
- Hui, K., Teo, H. H., & Lee, S.-Y. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31(1), 19–33.

- Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17, 89–101. <https://doi.org/10.1007/s10676-015-9363-z>
- 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>
- Ibdah, D., Lachtar, N., Raparathi, S. M., & Bacha, A. (2021). Why Should i Read the Privacy Policy, i Just Need the Service’: A Study on Attitudes and Perceptions Toward Privacy Policies. *IEEE Access*, 9, 166465–166487. <https://doi.org/10.1109/ACCESS.2021.3130086>
- 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>
- Johnson, G. A., Shriver, S. K., & Du, S. (2020). Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry? *Marketing Science*, 39(1), 33–51. <https://doi.org/10.1287/mksc.2019.1198>
- Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, BJASt(4), 397–403. <https://doi.org/10.9734/BJAST/2015/14975>
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107, 1–15. <https://doi.org/10.1016/j.chb.2020.106260>
- Kayworth, T., Brocato, L., Whitten, D., Kayworth, T. ;, Brocato, L. ;, Kayworth, T., Brocato, L., & Whitten, D. (2005). What is a Chief Privacy Officer? An Analysis Based on Mintzberg’s Taxonomy of Managerial Roles. *Communications of the Association for Information Systems*, 16(6), 110–126. <https://doi.org/10.17705/1CAIS.01606>
- Kitkowska, A., Shulman, Y., Martucci, L. A., & Wästlund, E. (2020). Psychological Effects and Their Role in Online Privacy Interactions: A Review. *IEEE Access*, 8, 21236–21260. <https://doi.org/10.1109/ACCESS.2020.2969562>
- 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.
- Kohli, A. K., Jaworski, B. J., & Kumar, A. (1993). MARKOR: A Measure of Market Orientation. *Journal of Marketing Research*, 30(4), 467. <https://doi.org/10.2307/3172691>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, 64(November), 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- KPMG. (2021). *Corporate Data Responsibility - Bridging the consumer trust gap*.
- Lanier, C. D., & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12(1), 1–48.
- Li, Y. (2011). Privacy Concerns: Literature Review and an Integrative Framework . *Communications of the Association for Information Systems*, 28(28), 453–496. <https://doi.org/10.17705/1CAIS.02828>
- 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, 106868. <https://doi.org/10.1016/j.infsof.2022.106868>
- Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, 1, 47–64. <https://doi.org/10.2478/popets-2020-0004>
- Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, 122, 875–888. <https://doi.org/10.1016/j.jbusres.2019.10.006>
- Lupiañez-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*.
- 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/10.2307/23044045>
- Makri, E. L., & Lambrinoudakis, C. (2015). Privacy principles: Towards a common privacy audit methodology. *International Conference on Trust and Privacy in Digital Business*, 9264, 219–234. https://doi.org/10.1007/978-3-319-22906-5_17/FIGURES/2
- Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 14(1), 44–59. <https://doi.org/10.1177/1094670510383409>

- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>
- Martin, K. (2018). 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., & 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>
- Maydeu-Olivares, A., & Shi, D. (2017). Effect sizes of model misfit in structural equation models: Standardized residual covariances and residual correlations. *Methodology*, 13, 23–30. <https://doi.org/10.1027/1614-2241/A000129>
- Merenda, P. F. (2019). Measurement and Evaluation in Counseling and Development A Guide to the Proper Use of Factor Analysis in the Conduct and Reporting of Research: Pitfalls to Avoid. *Measurement and Evaluation in Counseling and Development*, 30(3), 156–164. <https://doi.org/10.1080/07481756.1997.12068936>
- Michler, O., Decker, R., & Stummer, C. (2020). To trust or not to trust smart consumer products: a literature review of trust-building factors. *Management Review Quarterly*, 70, 391–420. <https://doi.org/10.1007/s11301-019-00171-8>
- Milne, G. R., Culnan, M. J., & Greene, H. (2006). A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy*, 25(2), 238–249.
- Mohassel, P., & Zhang, Y. (2017). SecureML: A System for Scalable Privacy-Preserving Machine Learning. 2017 *IEEE Symposium on Security and Privacy*, 19–38. <https://doi.org/10.1109/SP.2017.12>
- Möhle, J.-P. (2021). Totalrevision des Schweizer Datenschutzgesetzes – Ende gut, alles gut? *Datenschutz Und Datensicherheit - DuD 2021* 45:9, 45(9), 598–602. <https://doi.org/10.1007/S11623-021-1498-Y>
- Morey, T., & Krajecki, K. (2016). Personalisation, data and trust: The role of brand in a data-driven, personalised, experience economy. *Journal of Brand Strategy*, 5(2), 178–185.
- Morlok, T. (2016). Sharing is (not) caring - The role of external privacy in users' information disclosure behaviors on social network sites. *PACIS*, 75–92. <http://aisel.aisnet.org/pacis2016/75>
- Muscatella, D. la. (2020). Data protection officer: Tasks and responsibilities of a key role for the innovation of the relationship between data and data subjects & rights. *Data Protection & Privacy*, 3(4), 403–417.
- Netemayer, W., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications*. Sage.
- Nissenbaum, H. (2010). Privacy in Context Technology, Policy, and the Integrity of Social Life. In *Privacy in Context*. Stanford University Press.
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Association for Computing Machinery (Ed.), *CHI* (pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376321>
- Oetzel, M. C., & Gonja, T. (2011). The online privacy paradox: A social representations perspective. *Conference on Human Factors in Computing Systems - Proceedings*, 2107–2112. <https://doi.org/10.1145/1979742.1979887>
- Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, 6, 642–660. <https://doi.org/10.1057/s41303-017-0056-z>
- Palmatier, R. W., & Martin, K. D. (2019). *The Intelligent Marketer's Guide to Data Privacy*. palgrave macmillan.
- Papadas, K. K., Avlonitis, G. J., & Carrigan, M. (2017). Green marketing orientation: Conceptualization, scale development and validation. *Journal of Business Research*, 80, 236–246. <https://doi.org/10.1016/J.JBUSRES.2017.05.024>
- Park, S. H., & Back, K. J. (2020). Modified scales for organizational identification and organizational disidentification for the foodservice industry. *International Journal of Hospitality Management*, 91, 102667. <https://doi.org/10.1016/J.IJHM.2020.102667>
- Parker, R. B. (1974). A Definition of Privacy. *Rutgers Law Review*, 27(2), 275–297. <https://heinonline.org/HOL/Page?handle=hein.journals/rutlr27&id=283&div=23&collection=journals>

- Patil, V. H., Singh, S. N., Mishra, S., & Todd Donavan, D. (2008). Efficient theory development and factor retention criteria: Abandon the 'eigenvalue greater than one' criterion. *Journal of Business Research*, 61(2), 162–170. <https://doi.org/10.1016/J.JBUSRES.2007.05.008>
- Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *Source: MIS Quarterly*, 31(1), 105–136.
- 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.informing-science.org/Publications/3573>
- Peterson, R. A. (2000). A Meta-Analysis of Variance Accounted for and Factor Loadings in Exploratory Factor Analysis. *Marketing Letters*, 11(3), 261–275.
- Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory Spillovers and Data Governance: Evidence from the GDPR. *Marketing Science*, 41(4). <https://doi.org/10.1287/mksc.2021.1339>
- 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>
- Pötzsch, S., Wolkerstorfer, P., & Graf, C. (2010). Privacy-Awareness Information for Web Forums: Results from an Empirical Study. In ACM (Ed.), *NordiCHI* (pp. 363–372). ACM.
- Power, M., & Trope, R. L. (2007). Developing a Culture of Privacy - A Case Study. *IEEE Security & Privacy*, 58–60. www.ssha.org
- Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human Computer Studies*, 110(March 2016), 21–32. <https://doi.org/10.1016/j.ijhcs.2017.10.003>
- Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2020). Consumers and Artificial Intelligence: An Experiential Perspective: <https://doi.org/10.1177/0022242920953847>, 85(1), 131–151.
- 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>
- Raento, M., & Oulasvirta, A. (2008). Designing for privacy and self-presentation in social awareness. *Personal and Ubiquitous Computing*, 12(7), 527–542. <https://doi.org/10.1007/s00779-008-0200-9>
- Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). Advertising and Consumer Privacy: Old Practices and New Challenges. *Journal of Advertising*, 38(4), 51–61. <https://doi.org/10.2753/JOA0091-3367380404>
- Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change*, 167, 120681. <https://doi.org/10.1016/J.TECHFORE.2021.120681>
- Riedmann-Streitz, C. (2018). Redefining the Customer Centricity Approach in the Digital Age. *International Conference of Design, User Experience, and Usability*, 10918 LNCS, 203–222. https://doi.org/10.1007/978-3-319-91797-9_15
- Rodiya, K., Paul Singh, A., & Parihar Asst, D. (2013). A Review of Privacy Preserving Data Publishing Technique. *International Journal of Emerging Research in Management & Technology*, 2, 2278–9359.
- Salesforce. (2019). *State of the connected customer*.
- Sarathy, R., & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics* 2003 46:2, 46(2), 111–126. <https://doi.org/10.1023/A:1025001627419>
- Sarnot, P. (2020). Building a culture of privacy: Be customer-centric . *IAPP*. <https://iapp.org/news/a/building-a-culture-of-privacy-be-customer-centric/>
- Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, 34(3), 593–603. <https://doi.org/10.1016/J.IJR-ESMAR.2017.02.003>
- Schögel, M., & Gotsch, M. L. (2021). Intelligente Automatisierung im Marketing. *Wirtschaftsinformatik & Management* 2021 13:4, 13(4), 256–265. <https://doi.org/10.1365/S35764-021-00352-9>
- Sen, D., Ozturk, M., & Vayvay, O. (2016). An Overview of Big Data for Growth in SMEs. *Procedia - Social and Behavioral Sciences*, 235, 159–167. <https://doi.org/10.1016/J.SBSPRO.2016.11.011>

- 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.
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/J.COMNET.2014.11.008>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989–1015.
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126, 1880–1903.
- Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review*, 89(1), 1–51.
- Son, B. J.-Y., & Kim, S. S. (2008). Internet User's Information Privacy-Protective Responses: A Taxonomy and Nomological Model. *MIS Quarterly*, 32(3), 503–529.
- Sundar, S. S., Kim, J., Rosson, M. B., & Molina, M. D. (2020). Online Privacy Heuristics that Predict Information Disclosure. *Conference on Human Factors in Computing Systems - Proceedings*, 1–12. <https://doi.org/10.1145/3313831.3376854>
- Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, 1273–1296. <https://doi.org/10.1007/s11165-016-9602-2>
- Tahaei, M., Frik, A., & Vaniea, K. (2021). Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges; Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15. <https://doi.org/10.1145/3411764>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Teixeira, G. A., da Silva, M. M., & Pereira, R. (2020). The Critical Success Factors of GDPR Implementation : a Systematic Literature Review. *Digital Policy, Regulation and Governance*, 21(4), 402–418. <https://doi.org/https://dx.doi.org/10.1108/DPRG-01-2019-0007>
- Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018). I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR. *WWW ' 18 Companion*, 163–166. <https://doi.org/10.1145/3184558.3186969>
- Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254–268. <https://doi.org/10.1287/isre.1090.0260>
- 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>
- Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2017). Privacy-Preserving Mechanisms for Crowdsensing: Survey and Research Challenges. In *IEEE Internet of Things Journal* (Vol. 4, Issue 4, pp. 855–869). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/JIOT.2016.2594205>
- Vilanova, M., Lozano, J. M., & Arenas, D. (2009). Exploring the Nature of the Relationship Between CSR and Competitiveness. *Journal of Business Ethics*, 87, 57–69. <https://doi.org/10.1007/s10551-008-9812-2>
- Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, 120, 106763. <https://doi.org/10.1016/J.CHB.2021.106763>
- Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: an analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science*, 44(1), 119–134. <https://doi.org/10.1007/s11747-015-0455-4>
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the “privacy paradox.” *Current Opinion in Psychology*, 31(2), 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- Walsh, G., & Beatty, S. E. (2007). Customer-based corporate reputation of a service firm: Scale development and validation. *Journal of the Academy of Marketing Science*, 35(1), 127–143. <https://doi.org/10.1007/S11747-007-0015-7/TABLES/7>
- 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>

- Watkins, M. W. (2018). Exploratory Factor Analysis: A Guide to Best Practice: *Journal of Black Psychology*, 44(3), 219–246. <https://doi.org/10.1177/0095798418771807>
- Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-things. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 644–652. <https://doi.org/10.1109/ARES.2016.25>
- Wirtz, J., Kunz, W., Hartley, N., Tarbit, J., & Kunz, W. H. (2022). 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/
- Wirtz, J., & Lwin, M. O. (2009). Regulatory Focus Theory, Trust, and Privacy Concern. *Journal of Service Research*, 12(2), 190–207. <https://doi.org/10.1177/1094670509335772>
- 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>
- Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information and Management*, 56(4), 570–601. <https://doi.org/10.1016/j.im.2018.10.001>
- Zuboff, S. (2020). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Reprint). PublicAffairs.

Managerial Implications

Taken together, the 6 articles presented within this dissertation lay the groundwork for future organisational privacy research and demonstrate, that data privacy and data-driven marketing need not be contradictory. In short, the key take-aways from a managerial perspective are:

- **Article 1:** The GDPR is not a compliance problem for marketers, but a chance to integrate and understand data privacy as part of the customer experience of any data-intensive product or service.
- **Article 2:** The transparency and control over commercial data processing demanded under the GDPR increases trust and improves trust recovery after data leaks. If evaluated separately, high transparency has a greater impact on trust when compared to high control.
- **Article 3:** Marketers' play a central role in defining the privacy orientation of their company. However, to do so, they need a level of privacy literacy as basis and the possibility to act upon that knowledge.
- **Article 4:** The focus on customer centricity has been and is often used inconsistently as a justification for the excess collection of customer data. Customer centric data processing is categorised by a high degree of purpose limitation and needs to be built in co-creation with the customer.
- **Article 5:** Organisational privacy orientation is determined top-down from the strategic level, translated into corresponding organisational structures that facilitate a unique human resource pool which enacts privacy policies on the tactical level. Improving or building organisational privacy is an iterative process, where information from the tactical level is used as a basis to adjust strategic direction.
- **Article 6:** Organisational privacy orientation is a measurable construct, which is aided by a generally high focus on corporate social responsibility and is harmed by a strict focus on compliance. Privacy orientation, in turn, was found to increase the marketing and financial performance of a given firm.

In total, the results make the case for managers in general and marketers specifically to work to align their organisation's data processing activities with the privacy needs of their customers (Gotsch, 2020, 2022). In doing so, they may increase their organisation's resilience against data breaches, increase customers' trust in the brand and create a future-ready human resource pool. This final chapter explains how customer-centric data management practices can be translated from the strategic level to individual customer journeys, employees and finally touchpoints. The goal: a culture of organisational privacy orientation in line with customers' needs and modern data protection laws.

What is the Idea behind Organisational Privacy Orientation?

While there is no doubt that the digitalisation of our daily lives has given rise to several beneficial and innovative business models, the data processing underlying them has often not kept up with the demands of modern data privacy legislation. This is demonstrated by the illegibility of most privacy policies (Slepchuk & Milne, 2020) and the widespread use of nudging techniques on digital platforms used to coax customers into giving consent (Lupiáñez-Villanueva et al., 2022).

Organisational privacy orientation (OPO) as a construct stands for data processing in accordance with digital privacy as a human right. As such, it is defined as the degree to which “a firm delivers consistent and transparent privacy protection to its customers” (Greenaway et al., 2015, p. 580) through strategic, structural, human resource and tactical measures (Gotsch & Schögel, n.d.). However, coming from a managerial point of view, OPO aims to achieve this goal while still reaping the benefits from modern data processing.

First studies within and outside this dissertation attest to the value of the strategic resources to be gained while pursuing OPO:

- **Positioning Benefits:** Using privacy as a differentiation tactic has mostly been discussed within two paradigms: The first is providing privacy as a core service, as it is the case with data intermediaries (e.g., VPN services). While these models are assumed to allow “customers to purchase a certain degree of privacy (...), the overall amount of privacy and privacy-based customer utility will continue to erode” (Rust et al., 2002, p. 455). The second is closer to the subject of this dissertation: competing with privacy as a strategic focus in a disclosure heavy market. The study of Casadesus-Masanell & Hervás-Drane (2015, p. 240) suggests, that offering customers a privacy-oriented alternative to existing market actors can yield a profit, if the consumers’ general willingness to pay is high.

However, positioning is not only communicated to potential customers, but to other industry actors as well. Since customer data is often used in a larger ecosystem of data controllers and processors, OPO increasingly becomes a barrier to entry for new actors wishing to participate. The example of Facebook demonstrates this well: In 2018, it was revealed that Facebook had given away personally identifiable data of over 87 Million users to Cambridge Analytica through its open API, without seeking their consent (Isaak & Hanna, 2018). The consequences were not only felt by Facebook itself: apart from starting an industry-wide dialogue on privacy (Isaak & Hanna, 2018), it resulted in a lowered general trust in social media by consumers (Maineri & Reeskens, 2019) and even calls for political action to split up the Silicon Valley tech firms to curb their influence on society (Cadwalladr, 2019). Such industry-wide spill-over effects are to be expected and have been observed in other contexts, such as product recalls (Borah & Tellis, 2016). Hence, industry actors would do well to position themselves as privacy-

oriented and protect themselves from potential negative spill-over effects (Martin et al., 2017b). At the same time, they signal to the rest of their industry, that they can be trusted as part of a larger data ecosystem (Wortmann et al., 2022).

- **Branding Benefits:** In 2015, following the privacy and surveillance debate started by the Snowden revelations, Apple released the iPhone 6s with a controversial encryption feature. Apple claimed that this feature supposedly prevented both Apple and the government to access customer data without consent (Mcgee et al., 2017). Shortly after, this claim was tested in the arena of public opinion, as the FBI reached out to Apple for help with unlocking iPhones connected to a terror attack in San Bernardino. The company refused, with Apple CEO Tim Cook making the following statement: “The way that we simply see this is, if this (...) can be used to force us to do something that would make millions of people vulnerable, then you can begin to ask yourself: If that can happen, what else can happen? In the next Senate you might say: Well, maybe it should be a surveillance OS. Maybe law enforcement would like the ability to turn on the camera on your Mac” (Grossman, 2016). While Apple has emphasised privacy as a selling point before, especially to distance themselves from its Silicon Valley rivals, it was this event which cemented privacy as “one of Apple’s core values” (Apple, 2020) – with one of the iPhone’s current central branding claims being “Privacy – that’s iPhone” (Chen, 2020; Fazzini, 2019).

Apple might be the most visible example of using privacy both as branding instrument and selling point – but studies looking at “internet companies” have been emphasizing privacy as a central selling point for well over a decade (Bart et al., 2005; Tang et al., 2008; Y. Wang & Hajli, 2014). The idea is that branding a product as privacy-oriented plays to the highly related concept of trust. Milne & Boza (1999) even suggested, that improving trust through a privacy focus is a more effective strategy for improving disclosure behaviour than reducing privacy concerns. Other industries, which rely heavily on trust, such as the newspaper industry, have also recently discovered the branding potential in emphasizing privacy measures such as foregoing programmatic ads (see e.g., Flaig, 2020). It has also been shown that customers of online market-places were willing to pay up to a 5% price premium to buy from a seller with stricter privacy policies (Tsai et al., 2011).

Morey & Krajecki (2016, p. 184) support these findings, saying that trust-building without focusing on information privacy will be a major challenge, concluding: “Personal data and consumer trust are the building blocks of the personalised experience economy. They must be earned by firms, and willingly given by consumers. It is the new face of brand building, and very much the domain of marketers.”

- **Human Resource Benefits:** The position of the Chief Data Officer (CDO) has grown in importance even before the GDPR was ratified and made it a mandatory post. Lee et al. (2014, p. 1) define this “new breed of executive” as overseeing “collaboration direction, data space & structure and value impact” (deciding how and what data is processed for which reason). Often either suggested as an accompanying role or merged

in the same role is the Chief Privacy Officer (CPO). Both positions have the potential to shape and enforce a firm's privacy strategy – which is why adequate training and hiring for the right leadership style is an effective tool to successfully use a privacy-oriented strategy (Kayworth et al., 2005, p. 121).

During the first wave of internet-focused privacy research, Sipior & Ward (2002) made the following recommendation to protecting companies from privacy related lawsuits: “In order to effectively coordinate proactive and reactive organisation-wide action to potential consequences, we recommend expanding the role of the existing CPO”. Additionally, it was recommended to train employees on the privacy policy of the company to ensure the future protection of the firm even as “the reliance on the Internet continues to grow”. (p. 77)

Looking at the recommendation from a resource-based view (see e.g., Gassmann et al., 2016), this point has only become more relevant. Similarly, to how early investment into acquiring high skilled labour to build big data architecture has resulted in higher growth and returns (Tambe, 2014), so will investing in the talent which knows how to facilitate OPO (see e.g., Adams & Bennett, 2018).

Building these capabilities (early) will convey two benefits. First, OPO is likely to improve the data architecture of a firm overall, as seamless data streams and central storage (instead of data silos) easier to analyse (J. Kim et al., 2016). Additionally, a central data storage can more adhere to current data privacy laws (Gupta et al., 2018), e.g., by allowing customers to check their shared data across the entire company instead of just single touchpoints. Second, there already exists a wealth of research on privacy preserving big data applications, which will require considerable talent to effectively utilise for marketing purposes (Freudiger et al., 2014; Gupta et al., 2018; Zheng et al., 2018). OPO drives both ends – as Anhalt-Depies et al. (2019, p. 7) put it “It is possible to provide high-quality, spatially explicit data (...) while protecting sensitive information in ways that provide protections to privacy and resources. However, doing this well requires significant investment in (understanding) technological solutions, data policies, and transparency efforts.”

- **Data Quality Benefits:** Prior to the ratification of the GDPR, a lot of industry-facing articles predicted this new law to “dramatically affect the way data is collected” (Downes, 2018), ending a lot of big data processing and monetisation tactics which had been in use prior. The idea that big data business models are incompatible with modern privacy regulations is intuitively correct, but only partially true. Looking at it from an economics perspective, the widespread availability of personal data would lead to a lowering of the informational value of individual data points (D’Acquisto et al., 2015). Part of this deterioration of data quality can already be observed, because if customers are faced with a situation where risk and reward of sharing data are intertwined, they will start protecting themselves by falsifying data instead of opting out of using said service all together (Jiang et al., 2013; Martin et al., 2017b).

Hence, it has long been argued, that in order to secure high-quality data, it is necessary for “privacy building trust in big data” (D’Acquisto et al., 2015, p. 18). While there are many factors which more effectively drive customers to share their data (e.g., offering an immediate benefit) (Kehr et al., 2015), perceived privacy or ownership of data does so as well (Dinev et al., 2012; Hui et al., 2007; Morlok, 2016; Z. Wang & Yu, 2015), with the added benefit of mitigating potential negative effects down the road (Martin et al., 2017b). Additionally, it has been suggested, that increased privacy not just increases the amount of data willingly disclosed, but also the quality of said data (Z. Wang & Yu, 2015).

Finally, all these benefits also pay into increasing customers’ overall experience when interacting with a company. Currently, the binary consent offered on many data collecting touchpoints (e.g., cookie banners) are both ineffective and a hinderance in the overall customer experience. By closer specifying the purpose of data processing and by learning which parts of the data processing might potentially be unconscionable for customers, consent request can both be deployed more precisely and offer more meaningful information to the customer (Gotsch & Schögel, n.d.).

These benefits can be realised by incorporating OPO across its four dimensions:

- **Strategy level:** Customer-centric data processing - i.e., ensuring all data processing is bound to a purpose which directly benefits the customer sharing said data.
- **Structural level:** Consent-based marketing - i.e., guaranteeing the effectiveness of data processing while upholding the organisation’s privacy principles.
- **Personnel level:** Promoting a data privacy culture - i.e., providing the necessary resources and incentives for save and privacy-oriented data processing.
- **Tactical level:** Frictionless satisfaction of needs - i.e., guaranteeing the efficiency of data processing on the touchpoint level.

As the implementation of GDPR guidelines have shown, such a process of alignment can be long and arduous for any firm (Teixeira et al., 2020). However, for companies looking to expand their digital capabilities or introducing a new digital business venture, OPO is a useful positioning tool. While it is difficult to provide general guidelines on how OPO can be increased, the following chapters provide an overview for managers how the OPO of their place of work could be assessed or developed.

Strategic OPO

Strategic OPO is defined as “the extent to which a firm integrates consistent, transparent privacy protection to its customers in their strategic marketing decisions” (Gotsch & Schögel, n.d.). Strategic guidance is necessary for the development of any corporate resource, as this is

the best way to create "hard-to-imitate internal and external competencies" (Teece et al., 1997, p. 515). OPO is no exception: it needs an externally communicated and internally lived vision that serves as a foundation for all other OPO efforts (Gotsch & Schögel, 2021, p. 12). Internally, this means that data privacy is not simply defined as a compliance problem but is directly addressed like other strategic goals. In branding terms privacy is to be understood as a core value and a part of the customer experience. How this is realised might look differently between industries – e.g., depending on the type of product being sold (Gotsch & Schögel, 2022, p. 6):

- **Fast moving consumer goods:** For low-involvement products with a high degree of substitution (e.g., food or beverages), the decision and purchase phase are usually short or even spontaneously. Accordingly, privacy-oriented data processing strategies should focus on finding the necessary data to eliminate frictions in the purchasing process and facilitate the upsell.
- **Consumer goods:** Low-involvement products with a low degree of substitution (e.g., drugs) have a longer consideration phase. Hence, it is important that collected data is used to improve both the product itself and the care at the individual touchpoints (e.g., better consultation or more intuitive product design).
- **Loyalty goods:** Products with a high degree of substitution and high involvement (e.g., consumer electronics) are characterised by a long decision phase. Since further purchases depend on high customer loyalty, data processing should not only contribute to the improvement of the customer journey, but also to the continuous improvement of products in question.
- **Evaluation goods:** The lower the degree of substitution for a high-involvement product (e.g., financial services), the longer and more important the pre-purchase phase becomes. Data processing should therefore help customers in their research, evaluation and consideration steps.

Strategic OPO requires understanding what data the organisation needs in any of the examples mentioned above while also learning at which steps and for which data customers feel the most vulnerable if data is disclosed.

At the same time, an OPO positioning entails being wary of industry actors with a different trajectory and distancing itself from them. In the short term, this means auditing suppliers or other actors in the same data ecosystem with dubious data privacy practices. A prominent example would be Apple's battle against Facebook over more transparent data collection on iOS devices (Rodriguez, 2021). In the long term, OPO can only be used for a sustainable differentiation, if the company is committed to better privacy standards in its markets, either through the voluntary adoption of recognised privacy standards or the pro-active establishment of new standards. As an example: two years ago, the Swiss companies Migros, Swisscom, SBB and Credit Suisse proved that this is possible with comparatively simple means with their

"Privacy Icons"-initiative. This established a uniform visual language to inform customers more efficiently about data requests for services (Hotz & Glatthaar, 2020).

Relevant indicators for the self-assessment of strategic OPO:

- Our top management explicitly names data privacy as an important part of our company's strategy.
- Our top management emphasises that the protection of costumers' data privacy is the responsibility of each employee.
- The protection of the data privacy of our customers is named within our mission statement.

Structural OPO

Structural OPO is "the extent to which a firm's established rules, norms or structures guide privacy preserving behaviour" (Gotsch & Schögel, n.d.). From the customer's point-of-view, strategic OPO mainly influences how they view the company, but it contributes little to how fair they evaluate the exchange of data for benefits to be (Greenaway et al., 2015). From a privacy perspective, informed consideration of data sharing is only possible for customers in a rather narrow "zone of effectiveness" (Reidenberg et al., 2014, p. 517). Specifically, requests to share data should only be presented to customers if the following conditions are met (Richards & Hartzog, 2019, p. 517):

1. **Infrequent:** Not every interaction over every touchpoint needs to be recorded. As such, requests for consent should only pop-up in the customer journey where they are needed.
2. **Comprehensible:** The benefits (and potential risks) of disclosure should be immediately obvious to the customer. This is the case if the benefits are directly tied to the disclosure of data and the risks are presented in the order of severity rather than hidden behind a privacy policy.
3. **Serious:** Customers need to be in a situation where they can take requests seriously – i.e., not while being distracted or nudged to a predetermined conclusion.
4. **Protected:** Any data shared by customers is stored in line with current cyber security standards and internal access is limited to as few employees as possible.

These are the goals of Structural OPO: to ensure through rules, regulations, data architecture and audits, that these conditions are met for all data processing activities (Lu et al., 2014).

Relevant indicators for the self-assessment of structural OPO:

- We have created a separate department specializing in data privacy issues.

- We have clear guidelines on how to react to a detected personal data breach.
- All accesses to our customer data are logged and recorded.
- We regularly conduct internal privacy risk assessments with a clearly defined scope.
- We conduct an external privacy audit at least once every year.
- Our company has a system in place that ensures that improper or frequent accesses to customer data are immediately noticed.
- We organise presentations for our employees to inform them about our data privacy regulations.
- We have access to an online archive or training platform, where our employees can learn about our privacy regulations.

Human Resource OPO

HR OPO is defined as “the level of knowledge and assimilation of corporate privacy preserving values by all internal stakeholders” (Gotsch & Schögel, n.d.). The acquisition and promotion of skills in the human resource pool contributes directly to the implementation of a company's operational and strategic goals. The exact mix of skills required will depend on the strategic objectives, but the tendency should be for the internal demand for analysts and IT staff to increase as more data sources are tapped. Additionally, all employees need to be regularly trained on how the company's privacy strategy affects their daily tasks.

Soft skills should not be neglected in this context either, especially in companies with intensive customer contact (e.g., financial services). After all, communicating the customer's benefit regarding the processing of their data is an important part of the customer experience. It is up to employees to create little moments of trust throughout the customer journey, which ensure that the consent to share data is genuine. (Gotsch & Schögel, 2022)

If these capabilities are available in the company, they must in turn be anchored in the company's incentive structure through a transparent data architecture and guiding key figures. As the final step in the process of embedding data privacy skills in a company's workforce, face-to-face interactions serve as an important source of learning for employees, helping to align a company's data protection with the needs of its customers. (Schögel & Gotsch, 2021, p. 18). Hence, the effects of human resource OPO are felt by customers, if they understand the value being generated through the company's data processing as explained by its employees.

Relevant indicators for the self-assessment of human resource OPO:

- Our customers understand, what data we collect from them.
- Our customers understand, why we collect data from them.
- Our data processing activities are transparent to our customers.

Tactical OPO

Tactical OPO is defined as “the extent to which privacy preserving values are embodied in tactical marketing decisions” (Gotsch & Schögel, n.d.). One of the main focuses of marketing related privacy research has been improving the data gathering processes themselves. Martin & Murphy suggested (2017) to give the customers both more control and transparent information over requested data flows. The importance of creating processes with both transparency and control in mind “has been established” (Beke et al., 2018, p. 8) and partially incorporated into e.g., the GDPR. Especially being able to provide transparency over data processing contributes to brand trust (Gotsch, 2021). Apart from that, there exist multiple privacy enhancing analytics methods which can be employed instead of relying on more data intensive methods (D’Acquisto et al., 2015; Freudiger et al., 2014; J. Kim et al., 2016).

Of course, just relying on anonymisation techniques alone is not enough. From the experience of many companies with the implementation of the GDPR principles, we know that one of the biggest hurdles is the lack of a clear privacy strategy and the lack of translation to the operational level (Linden et al., 2020; Teixeira et al., 2020; Zaeem & Barber, 2020). This is also the reason why the stream of complaints about non-compliant processing in Europe has not yet stopped four years after its ratification (Lupiáñez-Villanueva et al., 2022).

On the other hand, companies that have already taken steps to comply with the GDPR have a wide range of instruments at their disposal that make data processing even more transparent and easier to monitor for their customers. The most frequently mentioned privacy practices at a touchpoint level are transparent communication (i.e., not written like a legal text), simple data management (i.e., GDPR-compliant) and refraining from manipulative nudges. Best practices for individual aspects of data privacy are to be found among big tech companies. From Apple’s app tracking transparency to Google’s privacy check, to Facebook’s step-by-step tour of privacy features, there are plenty of ideas for most companies on how to make their own touchpoints more privacy-oriented. (Gotsch & Schögel, 2022)

Relevant indicators for the self-assessment of tactical OPO:

- We only collect enough data from customers to fulfil their order(s).
- Our customers can test our products and services without sharing a lot of personal data.
- We do not collect customer data unless the customer receives a clear benefit in return.
- We make efforts to use as little personal data for our products and services as possible.

Conclusion

In the last twenty years, a lot has been invested in the digitalisation of processes and business models across all industries. For many companies, data privacy has been and is just another hurdle that requires a lot of investment and resource acquisition to overcome. With the global data ecosystem growing by the day, time is right to challenge this view. The recommendations in this dissertation are not out of reach for most companies - but they require a conscious and timely commitment from marketing management to understand their customers' privacy as an integral part of customer engagement.

This does not mean that companies should forego data processing or that every SME must keep up with Apple's security standards. The degree of one's privacy orientation will always depend on the extent to which customer data is processed to deliver customer value. However, the goal for every company should be to be able to conduct an open dialogue with its customers about data processing - without making them uncomfortable or being deliberately obtuse. A high organisational privacy orientation is only reached if customers are able to fully reap the benefits of their willingly shared data.

Currently, customers are still coming to terms with the exponential logic of data driven business ventures and are therefore at a disadvantage, when it comes to avoiding or regulating firms looking to exploit this power imbalance. However, children of younger generations, who grow up with smartphones in their hands today, will have experienced three decades of privacy discussions and scandals by the time they are able to vote with their wallet. At the same time, privacy cannot be expected to go out of fashion, as it is a deliberate and basic human desire and therefore a human right. As such, brands and companies able to instil privacy orientation as a core value in the minds of young generations today, will be the only ones able to build the sustainable data ecosystems of tomorrow.

References

- Adams, M., & Bennett, S. (2018). Corporate governance in the digital economy : The critical importance of information governance. *Governance Directions*, 40(10), 631–640.
- Anhalt-Depies, C., Stenglein, J. L., Zuckerberg, B., Townsend, P. M., & Rissman, A. R. (2019). Tradeoffs and tools for data quality, privacy, transparency, and trust in citizen science. *Biological Conservation*, 238, 1–7. <https://doi.org/10.1016/j.biocon.2019.108195>
- Apple. (2020). *Privacy*. Apple. <https://www.apple.com/privacy/>
- Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *Journal of Marketing*, 69, 133–152. www.spglobal.com
- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. In *Foundations and Trends in Marketing* (Vol. 11, Issue 1). <https://doi.org/10.1561/17000000057>
- Borah, A., & Tellis, G. J. (2016). Halo (Spillover) Effects in Social Media: Do Product Recalls of One Brand Hurt or Help Rival Brands? *Journal of Marketing Research*, LIII, 143–160. <https://doi.org/10.1509/jmr.13.0009>
- Cadwalladr, C. (2019, March 19). Cambridge Analytica a year on: ‘a lesson in institutional failure’ | UK news | The Guardian. *The Guardian*. <https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie>
- 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, B. X. (2020, June 23). *Apple Announces New Privacy Features - The New York Times*. The New York Times. <https://www.nytimes.com/2020/06/23/technology/apple-announces-new-privacy-features.html>
- D’Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y.-A. de, & Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. In A. Bourka & P. Drogkaris (Eds.), *Enisa* (Issue December). European Union Agency for Network and Information Security. <https://doi.org/10.2824/641480>
- 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>
- Downes, L. (2018). GDPR and the End of the Internet’s Grand Bargain. *Harvard Business Review*. <https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain>
- Fazzini, K. (2019). *Apple’s big bet on privacy has risks*. CNBC. <https://www.cnbc.com/2019/01/10/apple-privacy-big-bet-risks.html>
- Flaig, M. (2020). New York Times macht Schluss mit Programmatic Ads . *W&V*. https://www.wuv.de/m Medien/new_york_times_macht_schluss_mit_programmatic_ads?utm_source=newsletter-redaktion&utm_campaign=mailing&utm_medium=teaser
- Freudiger, J., Rane, S., Brito, A. E., & Uzun, E. (2014). Privacy Preserving Data Quality Assessment for High-Fidelity Data Sharing. *WISCS ’14: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 21–29. <https://doi.org/10.1145/2663876.2663885>
- Gassmann, O., Frankenberger, K., & Sauer, R. (2016). Exploring the Field of Business Model Innovation. In *Exploring the Field of Business Model Innovation*. <https://doi.org/10.1007/978-3-319-41144-6>
- Gotsch, M. L. (2020). Was hat das Marketing nach 2 Jahren DSGVO gelernt? *Swiss Marketing Review*, 6, 4–9.
- Gotsch, M. L. (2021). The individual and joint effects of data usage control & transparency on customers’ privacy responses. *AMA Summer Academic Conference Poster Submission*, 1–7.
- Gotsch, M. L. (2022). Customer Centricity & Datenschutz - Die Geschichte eines Missverständnisses. *Marketing Review St. Gallen*, 2022(2), 12–19. <https://www.alexandria.unisg.ch/265774/>
- Gotsch, M. L., & Schögel, M. (n.d.). Organizational Privacy Orientation - Scale Development and Validation. *Currently under Review at the Journal of Business Research*, 1–35.
- 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>
- Gotsch, M. L., & Schögel, M. (2022). Privacy as Strategy - Ein Framework für das kundenzentrierte Datenmanagement. *GfM Forschungsreihe*, 2(1), 1–15. <https://www.alexandria.unisg.ch/265983/>
- 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>
- Grossman, L. (2016, March 17). *Apple CEO Tim Cook: Inside His Fight With the FBI* | Time. Time Magazine. <https://time.com/4262480/tim-cook-apple-fbi-2/>
- Gupta, M., Patwa, F., & Sandhu, R. (2018). An Attribute-Based Access Control Model for Secure Big Data Processing in Hadoop Ecosystem. *Publication:ABAC’18: Proceedings of the Third ACM Workshop on Attribute-Based Access Control*, 12(18), 13–24. <https://doi.org/10.1145/3180457.3180463>

- Hotz, J., & Glatthaar, M. (2020, November 30). Verkehrsschilder für den Datenschutz – Privacy Icons. *Privacy Icons*. <https://privacy-icons.ch/verkehrsschilder-fuer-den-datenschutz/>
- Hui, K., Teo, H. H., & Lee, S.-Y. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31(1), 19–33.
- Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56–59. <https://doi.org/10.1109/MC.2018.3191268>
- 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>
- Kayworth, T., Brocato, L., Whitten, D., Kayworth, T. ;, Brocato, L. ;, Kayworth, T., Brocato, L., & Whitten, D. (2005). What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles. *Communications of the Association for Information Systems*, 16(6), 110–126. <https://doi.org/10.17705/1CAIS.01606>
- 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>
- Kim, J., Ha, H., Chun, B. G., Yoon, S., & Cha, S. K. (2016). Collaborative analytics for data silos. *2016 IEEE 32nd International Conference on Data Engineering, ICDE 2016*, 743–754. <https://doi.org/10.1109/ICDE.2016.7498286>
- Lee, Y., Madnick, S., Maguire, J. N., Wang, R., Wang, F., & Zhang, H. (2014). A Cubic Framework for the Chief Data Officer: Succeeding in a World of Big Data. *MIS Quarterly Executive*, 13(1), 1–13.
- Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, 1, 47–64. <https://doi.org/10.2478/popets-2020-0004>
- Lu, R., Zhu, H., Liu, X., Liu, J., & Shao, J. (2014). Toward efficient and privacy-preserving computing in big data era. *IEEE Network*, 28(4), 46–50. <https://doi.org/10.1109/MNET.2014.6863131>
- 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*.
- Maineri, A. M., & Reeskens, T. (2019). IN ZUCK WE TRUST? A Quasi-Natural Experiment to Study Trust in Social Media. *114th Annual Meeting of the American Sociological Association*, 1–33.
- 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., & 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>
- Mcgee, H., Hsieh, N., & Mcara, S. (2017). Apple: Privacy vs . Safety (A). *Harvard Business School*, November, 1–34. <https://store.hbr.org/product/apple-privacy-vs-safety-a/316069?sku=316069-PDF-ENG>
- Milne, G. R., & Boza, M. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 13(1), 5–24. [https://doi.org/10.1002/\(SICI\)1520-6653\(199924\)13:1<5::AID-DIR2>3.0.CO;2-9](https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9)
- Morey, T., & Krajecki, K. (2016). Personalisation, data and trust: The role of brand in a data-driven, personalised, experience economy. *Journal of Brand Strategy*, 5(2), 178–185.
- Morlok, T. (2016). Sharing is (not) caring - The role of external privacy in users' information disclosure behaviors on social network sites. *PACIS*, 75–92. <http://aisel.aisnet.org/pacis2016/75>
- Reidenberg, J. R., Russell, C. N., Callen, A. J., Qasir, S., & Norton, T. (2014). Privacy Harms and the Effectiveness of the Notice and Choice Framework. *Journal of Law and Policy for the Information Society*, 11(2), 485–524.
- Richards, N. M., & Hartzog, W. (2019). The Pathologies of Digital Consent. *Washington University Law Review*, 1461–1503. <https://papers.ssrn.com/abstract=3370433>
- Rodriguez, S. (2021, February 1). Facebook strikes back against Apple privacy change, prompts users to accept tracking to get 'better ads experience.' *CNBC*. <https://www.cnn.com/2021/02/01/facebook-strikes-back-against-apple-ios-14-idfa-privacy-change.html>
- Rust, R. T., Kannan, P. K., & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30(4), 455–464. <https://doi.org/10.1177/009207002236917>
- Schögel, M., & Gotsch, M. L. (2021). Intelligente Automatisierung im Marketing. *Wirtschaftsinformatik & Management* 2021 13:4, 13(4), 256–265. <https://doi.org/10.1365/S35764-021-00352-9>
- Sipior, J. C., & Ward, B. T. (2002). A strategic response to the broad spectrum of internet abuse. *Information Systems Management*, 19(4), 71–79. <https://doi.org/10.1201/1078/43202.19.4.20020901/38837.9>
- Slepchuk, A. N., & Milne, G. R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, 31, 89–93. <https://doi.org/10.1016/j.copsyc.2019.08.007>
- Tambe, P. (2014). Big Data Investment, Skills, and Firm Value. *Management Science*, 60(6), 1452–1469. <https://doi.org/10.1287/mnsc.2014.1899>

- Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems*, 24(4), 153–173. <https://doi.org/10.2753/MIS0742-1222240406>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Teixeira, G. A., da Silva, M. M., & Pereira, R. (2020). The Critical Success Factors of GDPR Implementation : a Systematic Literature Review. *Digital Policy, Regulation and Governance*, 21(4), 402–418. <https://doi.org/https://dx.doi.org/10.1108/DPRG-01-2019-0007>
- Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254–268. <https://doi.org/10.1287/isre.1090.0260>
- Wang, Y., & Hajli, N. (2014). Co-Creation in Branding through Social Commerce: The Role of Social Support, Relationship Quality and Privacy Concerns. *Twentieth Americas Conference on Information Systems*, 1–16. <https://www.researchgate.net/publication/263425985>
- Wang, Z., & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Computer Law and Security Review*, 31(6), 782–792. <https://doi.org/10.1016/j.clsr.2015.08.006>
- 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>
- Zaeem, R. N., & Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies. *ACM Transactions on Management Information Systems (TMIS)*, 12(1). <https://doi.org/10.1145/3389685>
- Zheng, X., Mukkamala, R. R., Vatrappu, R., & Ordieres-Mere, J. (2018). Blockchain-based personal health data sharing system using cloud storage. *2018 IEEE 20th International Conference on E-Health Networking, Applications and Services, Healthcom 2018*, 1–6. <https://doi.org/10.1109/HealthCom.2018.8531125>

—

Appendix

Declaration about the Co-Authorship

This statement specifies the contribution from Matthias Friesenecker & Marcus Schögel for the listed articles. The co-authors listed agree to the use of the contributions to the cumulative thesis by Mauro Gotsch at the University of St.Gallen.

Name of Article	Authors	Publication Medium	Status of Publication *	Contribution from Mauro Gotsch	Signature Co-author / s
Knowing is Half the Battle – The Effect of SME Marketers' Privacy Literacy on Privacy Orientation	Friesenecker, Matthias; Gotsch, Mauro; Schögel, Marcus	Journal Article: Marketing Review St. Gallen	accepted	Methodology, Writing – Review & Editing, Validation, Supervision, Formal analysis	M. Gotsch M. Schögel
Addressing the Privacy Paradox on the Organizational Level – Review and Future Directions	Gotsch, Mauro; Schögel, Marcus	Journal Article: Management Review Quarterly	accepted	Methodology, Conceptualization, Formal Analysis, Investigation, Writing – Original Draft, Visualization, Data Curation, Writing – Review & Editing, Validation	M. Schögel
Organizational Privacy Orientation - Scale Development and Validation	Gotsch, Mauro; Schögel, Marcus	Journal Article: Journal of Business Research	submitted	Conceptualization, Methodology, Formal analysis, Investigation, Writing – Original Draft, Writing – Review & Editing, Visualization.	M. Schögel

* Submitted / in revision / accepted

Place and date: St. Gallen, 08.11.2022

Signature of PhD student: 

Curriculum Vitae

Mauro L. Gotsch

Scientific Project Manager & Seminar Manager – University of St. Gallen

mauro.gotsch@unisg.ch | [linkedin.com/in/mauro-gotsch/](https://www.linkedin.com/in/mauro-gotsch/)

Gallusstrasse 6, 9000 St. Gallen, Schweiz

Personal Details

Date of Birth	19.02.1992
Hometown	Samnaun, CH
Martial Status	Unmarried

Professional Experience

10.2018 – today St. Gallen, Switzerland	Institute for Marketing and Customer Insight at the University of St.Gallen Scientific project manager and seminar manager • Management of the CAS for Strategic Purchasing Management • Organisation and supervision of various seminars and study trips in the institute's executive education • Organisation and supervision of courses in the master's programme at the University of St. Gallen • Implementation and supervision of quantitative and qualitative research projects
07.2016 – 11.2018 Zurich, Switzerland	ENAIP Schweiz, NPO for the professional integration of migrants Online marketing & course planning • Strategic development of the teaching programme and competition monitoring in the Zurich and Central Switzerland markets • Planning, co-design and coordination of various marketing campaigns (online and offline) • Support, development, SEO and SEA for the four websites of ENAIP and its partners • Community management of all social media channels (FB, Youtube, Instagram, etc.) • Translation work German, English, Italian
09.2016 – 11.2018 Zurich, Switzerland	Liceo Vermigli, Italian private school in Zurich Head of online marketing • Support, development and SEO for the Liceo Vermigli website.

- Supervision of all social media channels (FB, Youtube, Instagram, etc.)
 - Conception, co-design and coordination of various trade fair appearances (e.g., Berufsmesse Zurich)
 - Translation work German, English, Italian
- 06.2015 – 09.2015
Zurich,
Switzerland
- Zense GmbH, Boutique-Consulting for Storytelling and Visualisation**
Marketing intern
- Conception and contribution to the successful launch of the spin-off project "SightSite", writing of foundation dossiers, co-design of the company's image
 - Preparation of project presentations, as well as editing and proof-reading of storyboards and scripts
 - Customer correspondence, material acquisition
- 09.2014 – 05.2016
St. Gallen,
Switzerland
- The Two Minutes University, Visualisation of Academic Works**
Marketing Consultation
- Developing the business model, writing and presenting to investors, fund acquisition
 - Co-designing the corporate identity, planning the branding strategy for market entry
 - Creation of online content, promotional and instructional videos
 - Conception as well as distribution of promotional items

Teaching Experience

- 07.2019 – today
- Introduction to scientific research and writing**
University of St. Gallen
- Part of Module 1 in the CAS for Strategic Purchasing Management
 - 12-24 managers from the DACH region
 - Correction of three transfer papers per participant per semester
- 08.2020 – today
- Data privacy in strategic marketing management**
Gesellschaft für Marketing (GfM), Institute for Marketing and Customer Insight
- Various presentations on the strategic importance of data privacy for marketing management
 - 10-50 executives from the DACH region
- 08.2018 – 11.2022
- Supervision of Bachelor and Master theses**
University of St. Gallen
- Supervision of 49 students during their final theses
 - Definition of research questions, restriction of research area
 - Advice on quantitative and qualitative methodology

Education

01.2018 – today	Doctoral Programme in Business Administration (PMA) Focus: Strategic Data Privacy Marketing University of St. Gallen (HSG) Supervisor: Prof. Dr. Marcus Schögel
09.2020 – 03.2022	Training programme for university didactics (CAS) University of St. Gallen (HSG) Thesis: „Vereinbarkeit der Forschungs- und Praxisorientierung in der universitären Erwachsenenbildung“
03.2017 – 05.2017	Google Trainings (Advanced): Analytics, Tag Manager, Search Advertising, Youtube Advertising, Mobile First – Drive Engagement Google Seminars, Zurich
09.2014 – 02.2017	Master of Arts in Marketing, Service- and Communication Management University of St. Gallen (HSG) Master's Thesis: „Eine experimentelle Untersuchung der Wirkung von Gamification auf die Zufriedenheit im Kaufprozess und die Kaufwahrscheinlichkeit“ Grade 5.75 of 6
09.2011 – 09.2014	Bachelor of Arts in Management Science (BWL) University of St. Gallen (HSG) Bachelor's Thesis: „Schülerorientierte Online-Kommunikation - Funktion, Potenzial und Nutzung am Beispiel des Gymnasiums Kloster Disentis“ - Grade 5.25 of 6
08.2005 – 05.2011	Gymnasiale Maturität with Latinum Bündner Kantonsschule, Chur Matura Thesis: „In alt-vertrauten Gassen. Kriminalroman.“ Grade 6 von 6

Languages

German	Native Tongue
Englisch	Business fluent, C2, Cambridge Certificate of Advanced English Grade A (2011), Business Higher University of St. Gallen, Grade 5.5 von 6
Italian	B2 – C1 (CEFR)

Software & IT

MS - Office	Word, Excel, Powerpoint, Outlook, OneNote, OneDrive, Teams, Dynamics
Adobe CC	Photoshop, Illustrator, After Effects, Premiere, Animate, InDesign, Acrobat
Google	Adwords, Analytics, Tag-Manager, Search Console, MyBusiness, Youtube
Webdesign	Wordpress, Drupal, Gravity Forms, Ninja Forms, Woocommerce, HTML, CSS, Javascript Grundlagen, Screaming Frog SEO Spider
Scientific Software	IBM SPSS Statistics, AMOS, R Studio, Orange, Questback EFS Survey, Atlas.ti, Mendeley, Prolific.co, GiMP
Others	Dragonframe Stop Motion Animation, AVS Audio Editor, Zoom, OLS

Voluntary Work

01.2014 – today Across Switzerland	Quickphix, Association for Swiss TTRPG Enthusiasts Association president • Support and maintenance of the website • Organisation of club events (online & offline) • Writing, illustrating and marketing of club publications • Translation work German, English
06.2019 – today St. Gallen, Switzerland	Restessbar St. Gallen Volunteer • Collecting food from St. Gallen supermarkets and restaurants to prevent food waste
08.2018 – today International	Marketing Review St. Gallen, AMA Summer Conference Reviewer • Reading and evaluating scientific journal articles
11.2020 – 02.2022 St. Gallen, Switzerland	Marketing Review St. Gallen Content coordination • Acquisition of articles, writing to researchers, conducting interviews

Statutory Declaration

Hereby I declare

- that I wrote this dissertation without any illicit assistance and without using any other aids than stated and that this dissertation was neither presented in equal nor in similar form at any other university;
- that I cited all references that were used respecting current academic rules.

Place and date of issue:

Signature: