Management Review Quarterly
https://doi.org/10.1007/s11301-021-00239-4

Addressing the privacy paradox on the organizational level: review and future directions

Mauro Luis Gotsch[1] · **Marcus Schögel**[1]

Received: 17 March 2021 / Accepted: 1 September 2021
© The Author(s) 2021

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

JEL Classification 3660 · 3920

✉ Mauro Luis Gotsch
mauro.gotsch@unisg.ch

Marcus Schögel
marcus.schoegel@unisg.ch

[1] Institute of Marketing, University of St. Gallen, Dufourstrasse 40a, 9000 St. Gallen, Switzerland

Published online: 13 September 2021

1 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 and 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 and 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 and de Jong 2017, p. 1051). Martin and 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.

2 Theory

Greenaway and 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 and de Jong 2017; Feng and Xie 2019; Kokolakis 2017). The sectoral level is focused on policies and regulations intended to protect privacy (e.g. Citron 2009; Mcneely and Hahm 2014; Richards 2008; Whitman 2004). Greenaway and 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 and 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 and Murphy 2017; Palmatier and Martin 2019, p. 58; Sarathy and Robertson 2003; Wang et al. 1998): To tackle the increasing privacy vulnerability of consumers, privacy processes and outcomes should be increasingly studied on the organisational level.

2.1 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. 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 and Crossler 2011, p. 1029) while "advocating for a holistic way of thinking about organisational use of consumer data" (Martin and 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 and 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.

2.2 The privacy paradox

Six years ago, Dienlin and 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 and 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 and 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 and 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 and Hartzog 2019, p. 1492). As long as the "irrational" side of individual privacy decisions (Gambino et al. 2016; Sundar and Kim 2019; Sundar et al. 2013) and the structural hurdles to informed consent (Mourey and Waldman 2020; Reidenberg et al. 2014; Richards and 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 and Crossler 2011, p. 1027; Martin and 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.

2.3 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 and 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 (Bauer and Lasinger 2014; Bauer and 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 et al. 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 and Hart 2006; Hui et al. 2007; Morlok 2016), damage control for data breaches (Malhotra and Malhotra 2011) and even firm performance (Martin et al. 2017).

However, since no cohesive overarching framework of how to address the privacy paradox on an organisational level exists (Palmatier and 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" (Martin and Murphy 2017, p. 152).

3 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, sociopsychology, ethics and law and used both qualitative and quantitative research

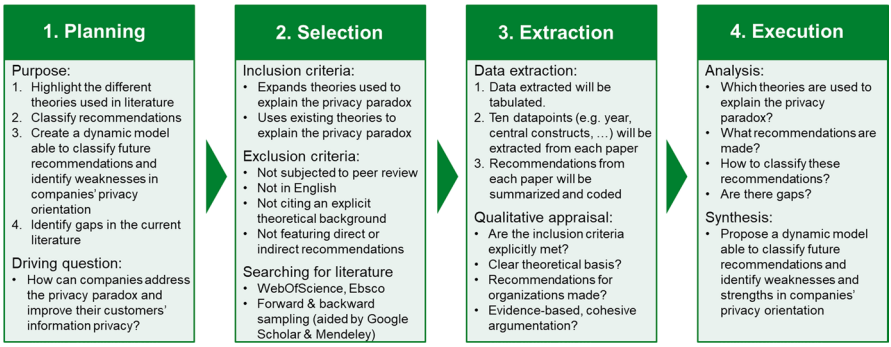


Fig. 1 Guide to the four phases of a literature review (based on Okoli 2015, p. 885)

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.

3.1 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 and Charters (2007, p. 54) was drafted. Due to the comparatively small team size involved in this review, no further training steps were taken.

3.2 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 WebofScience 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 and 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 and Block (2021, p. 3) to clearly express the effect of the exclusion criteria used.

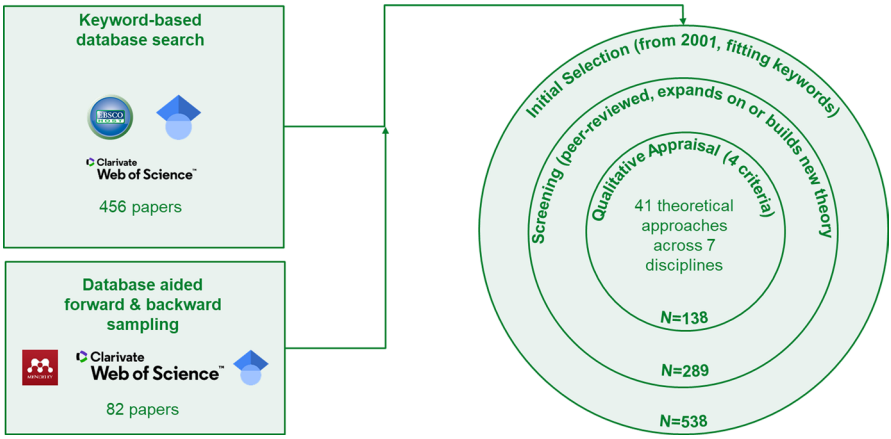


Fig. 2 Literature selection process

3.3 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 and 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.

3.4 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).

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.

4 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 and McAdam 2004, p. 258) along a temporal axis while allowing for recursive behaviour (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).

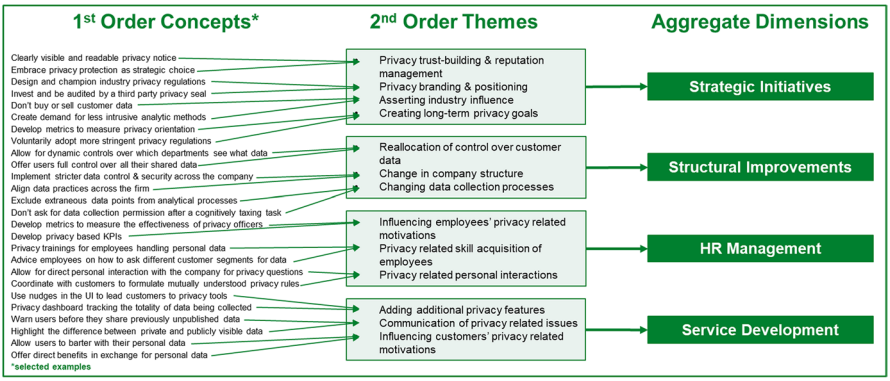


Fig. 3 Data structure of the literature review (based on Gioia et al. 2013, p. 21)

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 and 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 and 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.

4.1 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 and Li (2010).

4.1.1 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 and 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 and 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 and 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.

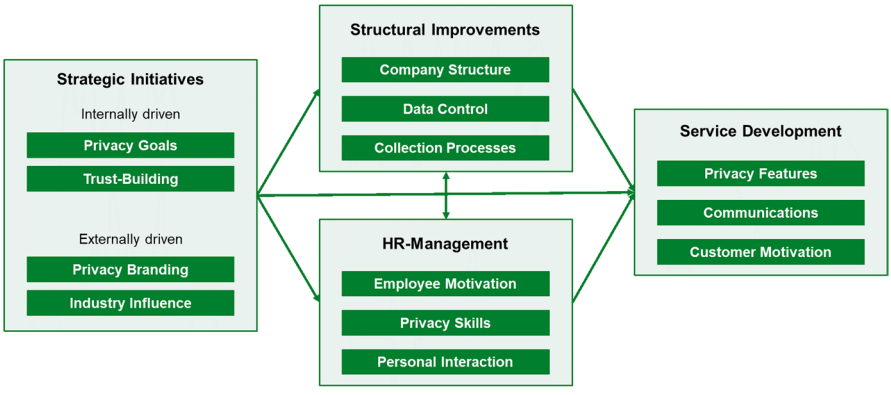


Fig. 4 Relationship between the aggregate dimensions

4.1.2 Trust-building

Trust is one of the central variables affecting the success of privacy measures (Wirtz and Lwin 2009), customer support of big data technologies (Bauer and Strauss 2016; Michler et al 2020) and the negative consequences of privacy turbulences for firms (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 and 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 and 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.

4.1.3 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 and 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

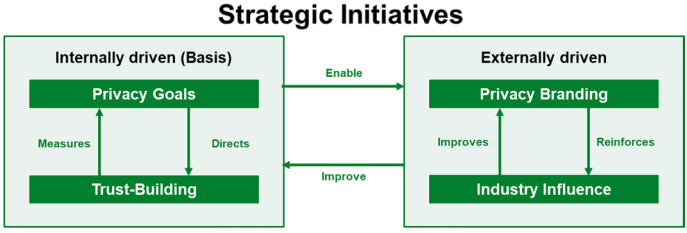


Fig. 5 Connections between strategic initiative codes

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 and 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.

4.1.4 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 and Gonja 2011) to distancing the company from industry actors with questionable privacy practices (Casadesus-Masanell and 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 (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 and Montecchi 2020) or creating an industry-wide demand for privacy friendly data collection processes (Martin 2020).

4.2 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).

4.2.1 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 and 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 et al. (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.

4.2.2 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

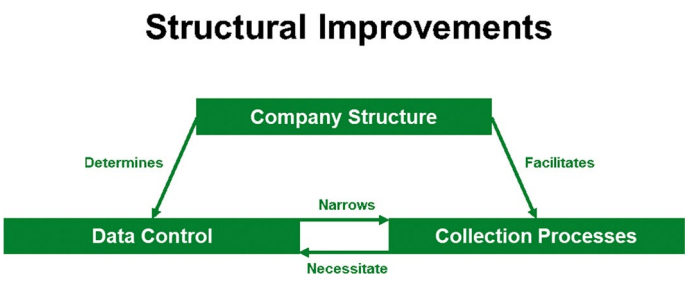


Fig. 6 Connections between structural improvement codes

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" (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 leverage their personal data more effectively. 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 and 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.

4.2.3 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 and 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 (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 and 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.

4.3 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 and 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 and 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).

4.3.1 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 and Maas (2018) who advise to co-create the value produced by sharing data

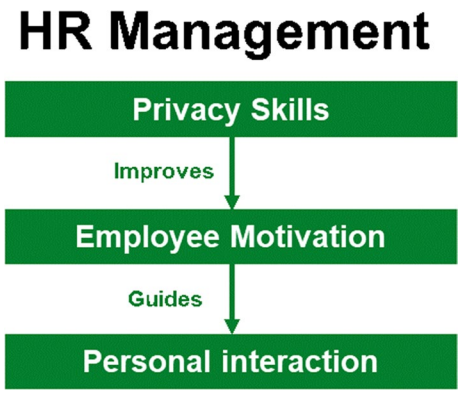


Fig. 7 Connections between HR management codes

by accommodating customers throughout the customer journey present an interesting avenue for further research.

4.3.2 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.

4.3.3 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 (Pötzsch 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 and Krajecki 2016, p. 179; Pötzsch 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.

4.4 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 and 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.

4.4.1 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 and Metzger 2016; Dinev et al. 2009), it also means allowing for audience management of this data (De Wolf and 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 and 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 (Bauer and Lasinger 2014; Bauer and 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).

4.4.2 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 and 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.

4.4.3 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 and 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 (Fig. 8).

4.5 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

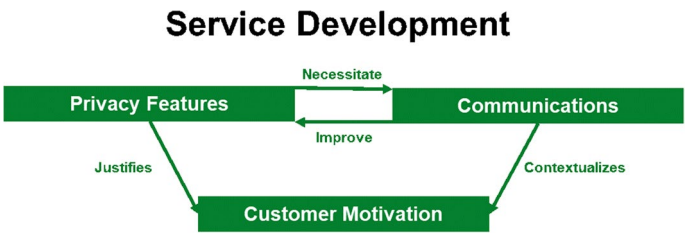


Fig. 8 Connections between service development codes

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 and Montecchi 2020; Waters and 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 and Verhoef 2016, p. 89).

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 (Fig. 10).

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 and 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

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

Fig. 9 Categorisation of theories (adapted from Barth and de Jong 2017, p. 1043)

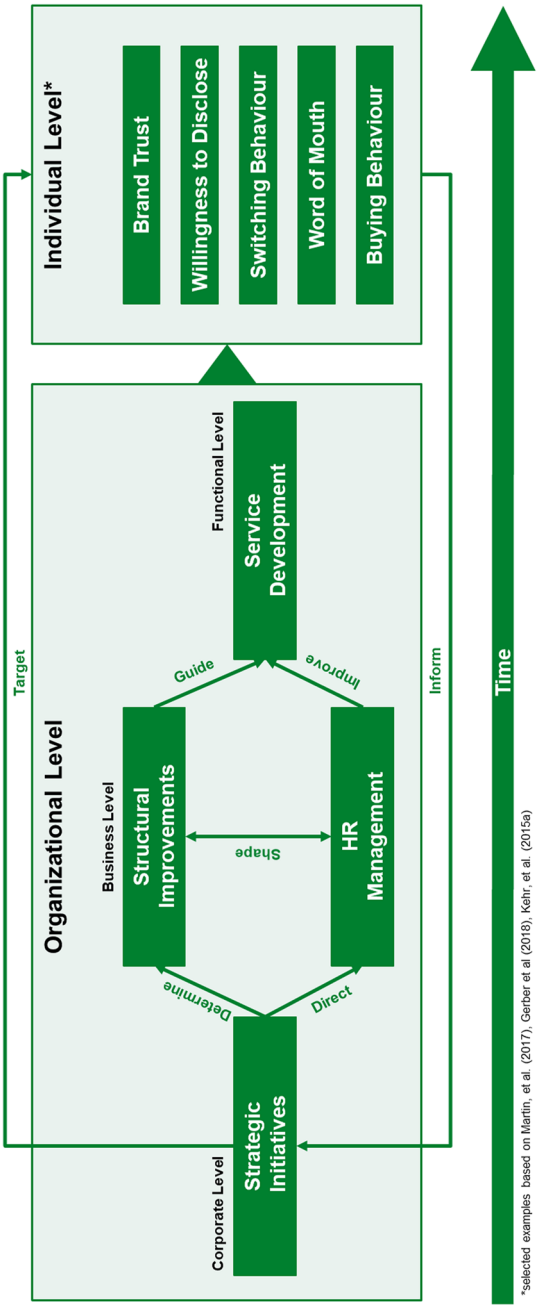


Fig. 10 Dynamic model for addressing the privacy paradox as a firm

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.

5 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 and 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.

5.1 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.

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" (Wang and 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 (Martin et al. 2017; Wirtz and 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" (Wang and 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.

5.2 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 and 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 and 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 marketeers to define guidelines on how and when organisations should protect their customers' privacy (Nowak and 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 and 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 and 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.

5.3 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?

6 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 confidentially 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 and 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 inter-coder reliability (for details on the codes and processes used see the supplemental materials).

7 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 and 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 and Nissenbaum 2014; Cate and 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 (Martin and 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 and 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".

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s11301-021-00239-4.

Author contributions Mauro Gotsch created the initial study conception and design. Material preparation, data collection and analysis were performed by Mauro Gotsch and Marcus Schögel. The first draft of the manuscript was written by Mauro Gotsch and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open Access funding provided by Universität St.Gallen. Research fully financed by the Institute of Marketing, University of St. Gallen.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declared that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings to EC'04, New York, pp 1–9

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. In: Science, vol 347(6221). American Association for the Advancement of Science, pp 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. J Econ Lit 54(2):442–492. https://doi.org/10.1257/jel.54.2.442

Acquisti A, Komanduri S, Analytics C, Leon PG, De Mexico B, Schaub F, Wang Y, Wilson S, Cranor LF, Sadeh N, Wang Y, Adjerid I, Balebako R, Brandimarte L, Cranor LF, 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 Comput Surv 50(3):1–41. https://doi.org/10.1145/3054926

Ahluwalia R (2008) How far can a brand stretch? Understanding the role of self-construal. J Mark Res 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: Arkin RM (ed) Most underappreciated: 50 prominent social psychologists describe their most unloved work. Oxford Scholarship Online, Oxford, pp 583–605. https://doi.org/10.1093/acprof:osobl/9780199778188.003.0029

Ajzen I, Fishbein M (1970) The prediction of behavior from attitudinal and normative variables. J Exp Soc Psychol 6(4):466–487. 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. Psychol Bull 87(5):888–918. 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. In: Proceedings of the 22nd Americas conference on information systems, pp 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. In: Twenty-fourth Americas conference on information systems, pp 1–10

Anhalt-Depies C, Stenglein JL, Zuckerberg B, Townsend PM, Rissman AR (2019) Tradeoffs and tools for data quality, privacy, transparency, and trust in citizen science. Biol Cons 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. Manag Sci 49(4):571–582. https://doi.org/10.1287/mnsc.49.4.571.14424

Auxier BYB, 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, pp 1–63

Bandara W, Furtmueller E, Gorbacheva E, Miskon S, Beekhuyzen J (2015) Achieving rigor in literature reviews: insights from qualitative data analysis and tool-support. Commun Assoc Inf Syst 34:154–204

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. Elsevier B.V., pp 562–567. https://doi.org/10.1016/j.procs.2017.11.074

Bansal G, Zahedi FM, Gefen D (2016) Do context and personality matter? Trust and privacy concerns in disclosing private information online. Inform Manag 53(1):1–21. https://doi.org/10.1016/j.im.2015.08.001

Barnes SB (2006) A privacy paradox: social networking in the United States. First Monday. 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. Commun ACM 57(11):31–33. https://doi.org/10.1145/2668897

Barth S, de Jong MDT (2017) The Privacy paradox-investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. Telematics Inform 34:1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth S, de Jong MDT, Junger M, Hartel PH, Roppelt JC (2019) Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics Inform 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. J Commun 67(1):26–53. https://doi.org/10.1111/jcom.12276

Bauer C, Lasinger P (2014) Adaptation strategies to increase advertisement effectiveness in digital media. Manag Rev Quart 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. Manag Rev Quart 66:159–194. https://doi.org/10.1007/s11301-015-0118-z

Bauer A, Reiner G, Schamschule R (2000) Organizational and quality systems development: an analysis via a dynamic simulation model. Total Qual Manag 11(4–6):410–416. https://doi.org/10.1080/09544120050007715

Becker B, Gerhart B (1996) The impact of human resource management on organizational performance: progress and prospects. Acad Manag J 39(4):779–801. https://doi.org/10.2307/256712

Beke FT, Eggers F, Verhoef PC (2018) Consumer informational privacy: current knowledge and research directions. In: Foundations and trends in marketing, vol 11(1). https://doi.org/10.1561/1700000057

Bélanger F, Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. In: MIS quarterly: management information systems, vol 35(4). University of Minnesota, pp 1017–1041. https://doi.org/10.2307/41409971

Bickelmann J (2021) Sag mir, wo du schreibst. Der Tagesspiegel 18

Boerman SC, Kruikemeier S, Zuiderveen Borgesius FJ (2018) Exploring motivations for online privacy protection behavior: insights from panel data. Commun Res 00:1–25. 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(3). https://doi.org/10.2307/25750690

Casadesus-Masanell R, Hervas-Drane A (2015) Competing with privacy. Manag Sci 61(1):229–246. https://doi.org/10.1287/mnsc.2014.2023

Cate FH, Mayer-Schönberger V (2013) Notice and consent in a world of Big Data. Int Data Privacy Law 3(2):67–73

Chen H, Beaudoin CE, Hong T (2017) Securing online privacy: an empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Comput Hum Behav 70:291–302. https://doi.org/10.1016/j.chb.2017.01.003

Child JT, Pearson JC, Petronio S (2009) Blogging, communication, and privacy management: development of the blogging privacy management measure. J Am Soc Inform Sci Technol 60(10):2079–2094. https://doi.org/10.1002/asi.21122

Child JT, Haridakis PM, 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. Comput Hum Behav 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. Comput Hum Behav 81:42–51. https://doi.org/10.1016/j.chb.2017.12.001

Citron DK (2009) Cyber civil rights. Boston Univ Law Rev 89(1):61–126

Clemons EK, 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 Inform 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. J Bus Ind Market. 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. Eur J Soc Psychol 45(3):285–297. https://doi.org/10.1002/ejsp.2038

Dienlin T, Metzger MJ (2016) An extended privacy calculus model for SNSs: analyzing self-disclosure and self-withdrawal in a representative U.S. Sample. J Comput Med Commun 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. Inf Syst Res 17(1):61–80. https://doi.org/10.1287/isre.1060.0080

Dinev T, Xu H, Smith HJ (2009) Information privacy values, beliefs and attitudes: an empirical analysis of web 2.0 privacy. In: Proceedings of the 42nd annual Hawaii international conference on system sciences, HICSS, pp 1–10. https://doi.org/10.1109/HICSS.2009.255

Dinev T, Xu H, Smith JH, Hart P (2012) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur J Inf Syst 22:295–316. https://doi.org/10.1057/ejis.2012.23

Dinev T, Mcconnell AR, Smith HJ (2015) Informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Inf Syst Res 26(4):639–655. https://doi.org/10.1287/isre.2015.0600

Eastlick MA, Lotz SL, Warrington P (2006) Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment. J Bus Res 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 MS, Miyazaki AD, Sprott DE (2010) Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. J Serv Mark 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. J Interact Advert 19(1):43–57. https://doi.org/10.1080/15252019.2018.1521317

Forrester JW (1968) Industrial dynamics—after the first decade. Manag Sci 14(7):398–415. https://doi.org/10.1287/mnsc.14.7.398

Freudiger J, Rane S, Brito AE, Uzun E (2014) Privacy preserving data quality assessment for high-fidelity data sharing. In: WISCS '14: proceedings of the 2014 ACM workshop on information sharing & collaborative security, pp 21–29. https://doi.org/10.1145/2663876.2663885

Gambino A, Kim J, Sundar SS, Ge J, Rosson MB (2016) User disbelief in privacy paradox: heuristics that determine disclosure. In: Conference on human factors in computing systems-proceedings, pp 2837–2843. https://doi.org/10.1145/2851581.2892413

Gioia DA, Corley KG, Hamilton AL (2013) Seeking qualitative rigor in inductive research: notes on the Gioia methodology. Organ Res Methods 16(1):15–31. https://doi.org/10.1177/1094428112452151

Gold AH, Malhotra A, Segars AH (2001) Knowledge management: an organizational capabilities perspective. J Manag Inf Syst 18(1):185–214. https://doi.org/10.1080/07421222.2001.11045669

Greenaway KE, Chan YE (2005) Theoretical explanations for firms' information privacy behaviors. J Assoc Inform Syst 6(6):171–198. https://doi.org/10.17705/1jais.00068

Gunther RE (2009) Peter Drucker-the grandfather of marketing: an interview with Dr. Philip Kotler. J Acad Mark Sci 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. Electron Commer Res Appl 16:55–65. https://doi.org/10.1016/j.elerap.2015.11.001

Hallam C, Zanella G (2017) Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput Hum Behav 68:217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hann I-H, Hui K-L, Lee S-YT, Png IPL (2007) Overcoming online information privacy concerns: an information-processing theory approach. J Manag Inf Syst 24(2):13–42. https://doi.org/10.2753/MIS0742-1222240202

Hermalin BE, Katz ML (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 DJ, Schwartz D, St. John DC, Picone-Decaro E, Jenkins RA, Carey JW (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 HY, Bashir M (2020) seeking privacy makes me feel bad?: An exploratory study examining emotional impact on use of privacy-enhancing features. In: Advances in intelligent systems and computing, 1129 AISC, pp 600–617. https://doi.org/10.1007/978-3-030-39445-5_44

Hui K, Teo HH, Lee S-YT (2007) The value of privacy assurance: an exploratory field experiment. MIS Q 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 Inf Technol 17:89–101. https://doi.org/10.1007/s10676-015-9363-z

James TL, Nottingham Q, Collignon SE, Warkentin M, Ziegelmayer JL (2015) The interpersonal privacy identity (IPI): development of a privacy as control model. Inf Technol Manag 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. J Manag Inf Syst 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. Inf Syst J 25(6):607–635. https://doi.org/10.1111/isj.12062

Keith MJ, Babb JS, Lowry PB (2014) A longitudinal study of information privacy on mobile devices. In: Proceedings of the annual Hawaii international conference on system sciences, pp 3149–3158. https://doi.org/10.1109/HICSS.2014.391

Kim T, Barasz K, John LK (2019) Why am i seeing this ad? The effect of ad transparency on ad effectiveness. J Consum Res 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, pp 1–65

Kitkowska A, Wästlund E, Martucci LA, Warner M, Shulman Y (2020) Enhancing privacy through the visual design of privacy notices: exploring the interplay of curiosity, control and affect. In: Sixteenth symposium on usable privacy and security, pp 437–456

Kokolakis S (2017) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput Secur 64:122–134. 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. Manag Rev Quart 2021:1–6. https://doi.org/10.1007/S11301-021-00228-7

Lanier CD, Saini A (2008) Understanding consumer privacy: a review and future directions. Acad Mark Sci Rev 12(1):1–48

Lemon KN, Verhoef PC (2016) Understanding customer experience throughout the customer journey. J Mark 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. J Manuf Technol Manag 15(3):254–266. https://doi.org/10.1108/17410380410523489

Li H, Yu L, He W (2019) The Impact of GDPR on Global Technology Development. J Glob Inf Technol Manage 22(1):1–6. https://doi.org/10.1080/1097198X.2019.1569186

Malhotra A, Malhotra CK (2011) Evaluating customer information breaches as service failures: an event study approach. J Serv Res 14(1):44–59. https://doi.org/10.1177/1094670510383409

Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355. https://doi.org/10.1287/isre.1040.0032

Mao Y (2018) Intercoder reliability techniques: holsti method. In: Allen M (ed) The SAGE encyclopedia of communication research methods, 1st edn. SAGE Publications, pp 741–743. https://doi.org/10.4135/9781483381411

Martin K (2020) Breaking the privacy paradox: the value of privacy and associated duty of firms. Bus Ethics Q 30(1):65–96. https://doi.org/10.1017/beq.2019.24

Martin KD, Murphy PE (2017) The role of data privacy in marketing. J Acad Mark Sci 45(2):135–155. https://doi.org/10.1007/s11747-016-0495-4

Martin KD, Borah A, Palmatier RW (2017) Data privacy: effects on customer and firm performance. J Mark 81(1):36–58. https://doi.org/10.1509/jm.15.0497

Matz SC, Appel RE, Kosinski M (2020) Privacy in the age of psychological targeting. Curr Opin Psychol 31(2):116–121. https://doi.org/10.1016/j.copsyc.2019.08.010

Mcneely CL, Hahm J (2014) The big (data) bang: policy, prospects, and challenges. Rev Policy Res 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. Manag Rev Quart 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. IEEE Sympos Secur Privacy 2017:19–38. 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. J 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. In: PACIS, pp 75–92. http://aisel.aisnet.org/pacis2016/75
Mothersbaugh DL, Foxx Ii WK, Beatty SE, Wang S (2012) Disclosure antecedents in an online service context: the role of sensitivity of information background disclosure and disclosure antecedents. J Serv Res 15(1):76–98. https://doi.org/10.1177/1094670511424924
Mourey JA, Waldman AE (2020) Past the privacy paradox: the importance of privacy changes as a function of control and complexity. J Assoc Consum Res 5(2):1–38. 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 PA, Horne DR (2007) Privacy attitudes and privacy-related behavior. Psychol Mark 24(10):829–847. https://doi.org/10.1002/mar.20186
Nowak GJ, Phelps J (1995) Direct marketing and the use of individual-level consumer information: determining how and when "privacy" matters. Direct Market 9(3):46–60. https://doi.org/10.1002/(SICI)1522-7138(199723)11:43.0.CO;2-F
Oetzel MC, Gonja T (2011) The online privacy paradox: a social representations perspective. In: Conference on human factors in computing systems - proceedings, pp 2107–2112. https://doi.org/10.1145/1979742.1979887
Okoli C (2015) A guide to conducting a standalone systematic literature review. Commun Assoc Inf Syst 37(43):879–910
Ozdemir ZD, Smith HJ, Benamati JH (2017) Antecedents and outcomes of information privacy concerns in a peer context: an exploratory study. Eur J Inf Syst 6:642–660. https://doi.org/10.1057/s41303-017-0056-z
Palmatier RW, Martin KD (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. J Interact Mark 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. ACM, pp 363–372
Prince C (2018) Do consumers want to control their personal data? Empirical evidence. Int J Hum Comput Stud 110(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. Pers Ubiquit Comput 12(7):527–542. https://doi.org/10.1007/s00779-008-0200-9
Reidenberg JR, Russell CN, Callen AJ, Qasir S, Norton T (2014) Privacy harms and the effectiveness of the notice and choice framework. J Law Policy Inform Soc 11(2):485–524
Richards NM (2008) Intellectual privacy. Texas Law Rev 87(2):387–445
Richards NM, Hartzog W (2019) The pathologies of digital consent. In: Washington University Law Review, pp 1461–1503. https://papers.ssrn.com/abstract=3370433
Rodriguez S (2021) Facebook strikes back against Apple privacy change, prompts users to accept tracking to get 'better ads experience.' In: CNBC. https://www.cnbc.com/2021/02/01/facebook-strikes-back-against-apple-ios-14-idfa-privacy-change.html
Sanchez-Rola I, Dell'amico M, Kotzias P, Eurecom DB, Bilge L, Vervier P-A, Santos I, Balzarotti D (2019) Can i opt out yet? GDPR and the global illusion of cookie control. In: AsiaCCS, vol 12, pp 340–351. https://doi.org/10.1145/3321705.3329806
Sarathy R, Robertson CJ (2003) Strategic and ethical considerations in managing digital privacy. J Bus Ethics 46:2
Schade M, Piehler R, Warwitz C, Burmann C (2018) Increasing consumers' intention to use location-based advertising. J Prod Brand Manag 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 Comput 14(1):34–43. https://doi.org/10.1109/MPRV.2015.5

Seo J, Kim K, Park M, Park M, Lee K (2018) An Analysis of Economic Impact on IoT Industry under GDPR. Mob Inf Syst 1–6. https://doi.org/10.1155/2018/6792028

Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Q 20(2):167–196

Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Q 35(4):989–1015

Solove DJ (2013) Privacy self-management and the consent dilemma. Harv Law Rev 126:1880–1903

Solove DJ (2021) The myth of the privacy paradox. George Washington Law Rev 89(1):1–51

Son BJ-Y, Kim SS (2008) Internet user's information privacy-protective responses: a taxonomy and nomological model. MIS Q 32(3):503–529

Steiner PH, Maas P (2018) When customers are willing to disclose information in the insurance industry: a multi-group analysis comparing ten countries. Int J Bank Market 36(6):1015–1033. https://doi.org/10.1108/IJBM-12-2016-0183

Sun S (2008) Organizational culture and its themes. Int J Bus Manag 137–141

Sundar S, Kim J (2019) Machine heuristic: when we trust computers more than humans with our personal information. In: Conference on human factors in computing systems-proceedings, pp 1–9. https://doi.org/10.1145/3290605.3300768

Sundar SS, Kang H, Zhang B, Go E, Wu M (2013) Unlocking the privacy paradox: do cognitive heuristics hold the key? In: Conference on human factors in computing systems-proceedings, pp 811–816. https://doi.org/10.1145/2468356.2468501

Sundar SS, Kim J, Rosson MB, Molina MD (2020) Online privacy heuristics that predict information disclosure. In: Conference on human factors in computing systems-proceedings, pp 1–12. https://doi.org/10.1145/3313831.3376854

Taneja A, Vitrano J, Gengo NJ (2014) Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: an empirical investigation. Comput Hum Behav 38:159–173. https://doi.org/10.1016/j.chb.2014.05.027

Tang Z, Hu Y, Smith MD (2008) Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor. J Manag Inf Syst 24(4):153–173. https://doi.org/10.2753/MIS0742-1222240406

Teece DJ, Pisano G, Shuen A (1997) Dynamic capabilities and strategic management. Strateg Manag J 18(7):509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3c509::AID-SMJ882%3e3.0.CO;2-Z

Teixeira GA, da Silva MM, Pereira R (2020) The critical success factors of GDPR implementation : a systematic literature review. Digit Policy Regul Govern 21(4):402–418. https://doi.org/10.1108/DPRG-01-2019-0007

Teng PK, Heng BLJ, Wong Abdullah SIN (2019) Distinctive comparison of consumers' mobile payment adoption between China and Malaysia. Asia Proc Soc Sci 2(3):57–61. https://doi.org/10.31580/apss.v2i3.258

Vergara-Laurens IJ, Jaimes LG, Labrador MA (2017) Privacy-preserving mechanisms for crowdsensing: survey and research challenges. IEEE Internet Things J 4(4):855–869. https://doi.org/10.1109/JIOT.2016.2594205

Völckner F, Sattler H (2006) Drivers of brand extension success. J Mark 70(2):18–34. https://doi.org/10.1509/jmkg.70.2.18

Waldman AE (2020) Cognitive biases, dark patterns, and the "privacy paradox." Curr Opin Psychol 31(2):105–109. https://doi.org/10.1016/j.copsyc.2019.08.025

Wang Y, Lo H-P (2003) Customer-focused performance and the dynamic model for competence building and leveraging A resource-based view. J Manag Dev. https://doi.org/10.1108/02621710310478486

Wang H, Lee MKO, Wang C (1998) Consumer privacy concerns about internet marketing. Commun ACM 41(3):63–70. https://doi.org/10.1145/272287.272299

Waters S, Ackerman J (2011) Exploring privacy management on facebook: motivations and perceived consequences of voluntary disclosure. J Comput-Mediat Commun 17(1):101–115. https://doi.org/10.1111/j.1083-6101.2011.01559.x

Westin AF (2003) Social and political dimensions of privacy. J Soc Issues 59(2):431–453. https://doi.org/10.1111/1540-4560.00072

Whitman JQ (2004) The two western cultures of privacy: dignity versus liberty. Yale Law J 113:6
Wilkie WL, Moore ES (2011) Expanding our understanding of marketing in society. J Acad Mark Sci 40:53–73. https://doi.org/10.1007/s11747-011-0277-y
Williams M, Nurse JRC, Creese S (2016) The perfect storm: the privacy paradox and the Internet-of-things. In: Proceedings-2016 11th international conference on availability, reliability and security, ARES 2016, pp 644–652. https://doi.org/10.1109/ARES.2016.25
Wirtz J, Lwin MO (2009) Regulatory focus theory, trust, and privacy concern. J Serv Res 12(2):190–207. https://doi.org/10.1177/1094670509335772
Wright PM, McMahan GC (1992) Theoretical perspectives for strategic human resource management. J Manag 18(2):295–320. https://doi.org/10.1177/014920639201800205
Wu KW, Huang SY, Yen DC, Popova I (2012) The effect of online privacy policy on consumer privacy concern and trust. Comput Hum Behav 28(3):889–897. https://doi.org/10.1016/j.chb.2011.12.008
Xu H, Luo X, Carroll JM, Rosson MB (2011) The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decision Support Syst 51(1):42–52. https://doi.org/10.1016/j.dss.2010.11.017
Yun H, Lee G, Kim DJ (2019) A chronological review of empirical research on personal information privacy concerns: an analysis of contexts and research constructs. Inform Manag 56(4):570–601. https://doi.org/10.1016/j.im.2018.10.001
Zhou KZ, Li CB (2010) How strategic orientations influence the building of dynamic capability in emerging economies. J Bus Res 63(3):224–231. https://doi.org/10.1016/j.jbusres.2009.03.003
Zhu H, Ou CXJ, van den Heuvel WJAM, Liu H (2017) Privacy calculus and its utility for personalization services in e-commerce: an analysis of consumer decision-making. Inform Manag 54(4):427–437. https://doi.org/10.1016/j.im.2016.10.001

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.