

Bues, Mirja; Pixa, Laura

Article

When, Why and How Consumers Seek to Protect their Privacy

Marketing Review St.Gallen

Provided in Cooperation with:

Universität St. Gallen, Institut für Marketing und Customer Insight

Suggested Citation: Bues, Mirja; Pixa, Laura (2016) : When, Why and How Consumers Seek to Protect their Privacy, Marketing Review St.Gallen, ISSN 1865-7516, Thexis Verlag, St.Gallen, Vol. 33, Iss. 2, pp. 62-69

This Version is available at:

<https://hdl.handle.net/10419/275847>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

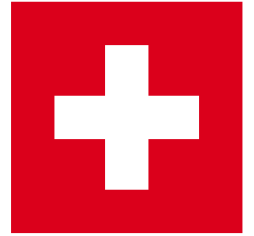
Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Marketing Review St. Gallen



2 | 2016 **SCHWERPUNKT** Interview mit Roman Melcher, dm-drogerie markt • Kundendaten revolutionieren die Wirtschaft
• Algorithmen revolutionieren das Marketing • Attribution im Online-Marketing • Brand Equity Valuation Through Big
Data Intelligence • Social Media und CRM Systeme in der Assekuranz • A Marketing Research Tool for Conducting Web
Experiments • Consumer Privacy Concerns & Big Data • Farming 4.0: Chancen und Herausforderungen
SPEKTRUM Negative Preise – ein neues Phänomen • Interview mit Dr. Hiesinger, thyssenkrupp AG
www.marketing-review.ch



Big Data & Data Intelligence



When, Why and How Consumers Seek to Protect their Privacy

Big data have not only offered marketers new possibilities, but have also multiplied threats to consumer privacy. Consumers face uncertainty and risk when disclosing personal information, which leads to growing privacy concerns and protective responses. This article seeks to identify the determinants of such protective behaviors.

M. Sc. Mirja Bues, Laura Pixa

Novel technologies have significantly increased the quality and quantity of the data to which companies have access, and provide companies with new possibilities to offer a customized marketing mix. Today, companies can use dynamic pricing (Taylor 2004), customized price promotion (Zhang/Krishnamurthi 2004), and customized direct marketing tools (Ansari/Mela 2003) to target their customers individually. However, the same technological advances that have made the internet a potent marketing tool have also multiplied the threats to consumer privacy. Furthermore, consumer privacy and the requirement to submit personal data are the primary factors that discourage online shopping (Dinev/Hart 2004). Owing to increasing concerns about data collection, storage, and exchange on the internet, many users seek to protect their privacy by supplying websites with false information (Lwin/Williams 2003; Phelps/Nowak/Ferrell 2000), managing the use of cookies (Culnan/Bies 2003), refusing to transact with particular websites, and warning other potential customers (Son/Kim 2008). Thus, marketers should address online consumer privacy concerns, which can undermine a firm's marketing effectiveness and may even lead to reputational damage. Furthermore, if consumers show protective responses by providing false information, firms' collected data are worthless. It is therefore crucial to understand which factors influence [when] consumers' privacy concerns, which may then cause [why] consumers to exhibit potentially protective responses [how].

Consumer Privacy

Privacy is a highly appreciated value; it refers to individuals' ability to control information about themselves (Stone et al. 1983). Although consumer privacy has been hotly debated in marketing and public policy for at least 20 years (Culnan 1995), the shift to data-driven purchase environments – and, hence, massive databases with much consumer information – has made it even more relevant now. Consumer privacy concerns about the extent to which individuals are able to control and protect their personal information are growing in data-driven environments (Dinev/Hart 2006).

In this study, privacy concern is modeled as a mediating construct between situational and consumer-related variables and consumer protective behaviors. This integrated view shows that certain situational and individual variables can act as predictors of potentially damaging consumer responses, and privacy concern plays both causal and consequential roles.

M. Sc. Mirja Bues

Research Assistant,
Institute of Marketing,
University of Muenster
m.bues@uni-muenster.de

Laura Pixa

Master Student,
University of Muenster
l_pixa01@uni-muenster.de

Consumer Protective Responses

Protective responses occur when consumers perceive their privacy as threatened (Lwin/Wirtz/Williams 2007; Smith/Milberg/Burke 1996; Son/Kim 2008). While most of the privacy literature focuses on consumers' willingness to disclose personal information and to transact (Dinev/Hart 2006; Nam et al. 2006), protective consumer responses (i.e. withholding or falsifying personal information, removing it from databases, or engaging in negative word-of-mouth (WoM) or complaining) have received little attention. Figure 1 provides an overview of these protective behaviors and their effects on consumer-company interactions.

While in the case of removal or withholding personal information, the databased consumer-company interaction can be regarded as terminated, other protective responses cause a disruption of the relationship and hence can therefore seriously harm a firm's database (in case of falsifying) or reputation (in case of complaining) and should be considered by companies.

To acquire a fundamental understanding of the relevance of protective privacy behaviors and to identify underlying influencing factors from the consumer perspective, we conducted a qualitative pre-study (i.e. focus groups). Based on these findings, we identified – among the variety of behaviors presented in the figure above – falsifying personal information and negative WoM as the most commonly observed protective responses.

Falsifying refers to consumers disguising their identity by using false information (Lwin/Williams 2003). It can be seen as a way to protect individuals' privacy freedom, and allows consumers to experience the benefit of disclosure

while maintaining their privacy. Negative WoM means that consumers communicate negative privacy experiences to others (Son/Kim 2008). Consumers engaging in negative WoM try to distance themselves from a company, thereby restoring their threatened privacy freedom and protecting others from the firm.

An Adapted S-O-R as the Baseline Framework

We chose an adapted process model and applied it to the research questions to ascertain which determinants cause which behavioral responses. The underlying idea of the S-O-R model is that environmental stimuli (S) lead to a reaction within the organism (O) that evokes behavioral responses (R) (Belk 1975; Mehrabian/Russell 1974). As stimuli, we consider situation-specific elements in the context of online shopping that a company can control. Based on the qualitative research and literature review, an online shop’s credibility, privacy policy perception, and information sensitivity have been identified as highly relevant to consumers when deciding how to behave concerning data disclosure in this context. Between stimuli and reaction, conscious or unconscious information processing occurs (i.e. the organism). This is ascribed to cognitive as well as affective effects, experiences, and attitudes. As underlying psychological processes provoked by situational influences, we consider privacy attitude (i.e. privacy concerns). Specifically, at this stage, a cost-benefit analysis of providing information takes place, known as the privacy calculus, which provides the basis for consumers’ decisions whether or not to disclose data (Dinev/Hart 2006; Milne/Gordon 1993). In addition, consumers’ individual experiences have been found to



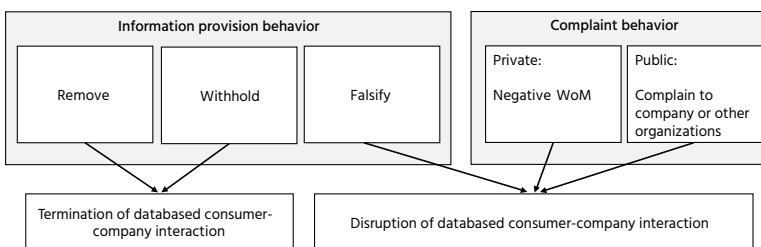
affect the formation of privacy concerns (Awad/Krishnan 2006; Smith/Milberg/Burke 1996). Thus, we consider both specific experiences (i.e. familiarity with an online shop) and general experience (i.e. previous privacy invasions) in the underlying model. In reaction to the stimuli, a specific behavior is provoked. As mentioned, we focus on the protective behaviors (i.e. falsifying information and negative WoM).

Situational Determinants

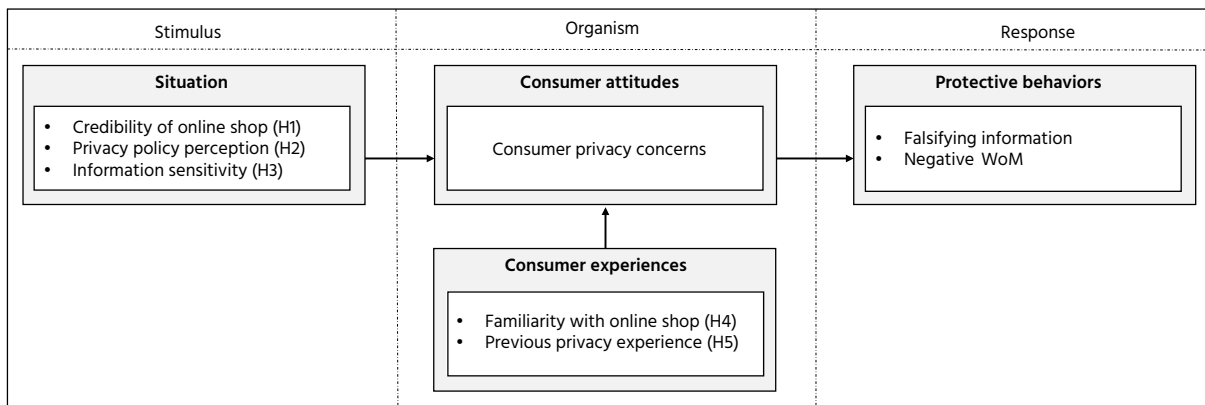
Credibility of online shop

In the online context, credibility refers to a consumer’s evaluation of a vendor based on his or her initial impression of its website (Lowry/Wilson/Haig 2014). Research has found that website credibility positively influences consumers’ willingness to provide personal information (Lowry/Wilson/Haig 2014; Wang/Beatty/Foxx 2004). As mentioned above, when individuals detect a request for information from an online shop, they initiate a risk-benefit calculus process (Xu et al. 2008). A risk of disclosing personal information could be electronic surveillance, while online shopping convenience could serve as a benefit. Because this assessment strongly depends on situational factors, consumers will also consider a website’s credibility (Metzger 2007). When a seemingly credible online shop requests information, indi-

Fig. 1: Overview of Protective Behaviours



Source: author’s illustration.

Fig. 2: Conceptual Framework

Source: author's illustration.

viduals will judge the shop as honest and reliable. Thus, the level of perceived risks will be lower, and consumers are more likely to find data disclosure acceptable. In contrast, if credibility is low, consumers are more likely to be concerned and are more likely to engage in protective responses (H1).

Perception of privacy policy

In the proposed model, privacy policy refers to consumers' perceptions of how a firm exercises ownership over the use of consumer data (Lwin/Wirtz/Williams 2007). This perception mirrors a company's efforts to ensure consumers that their personal information will be protected (Xu et al. 2008). Privacy policies help to signal that a firm protects its consumers' privacy (Xie/Teo/Wan 2006) and provides consumers with additional important information that they can consider when weighing the benefits of disclosure and risks (Pan/Zinkhan 2006). Consumers who cannot gain valuable information about a firm's privacy policy are expected to have less trust in the company, and will show higher concern about their own privacy (Lwin/Wirtz/Williams 2007). Thus, they will engage in protective behaviors (H2).

Information sensitivity

Information's perceived intimacy level has been found to play an important role in information privacy and resulting

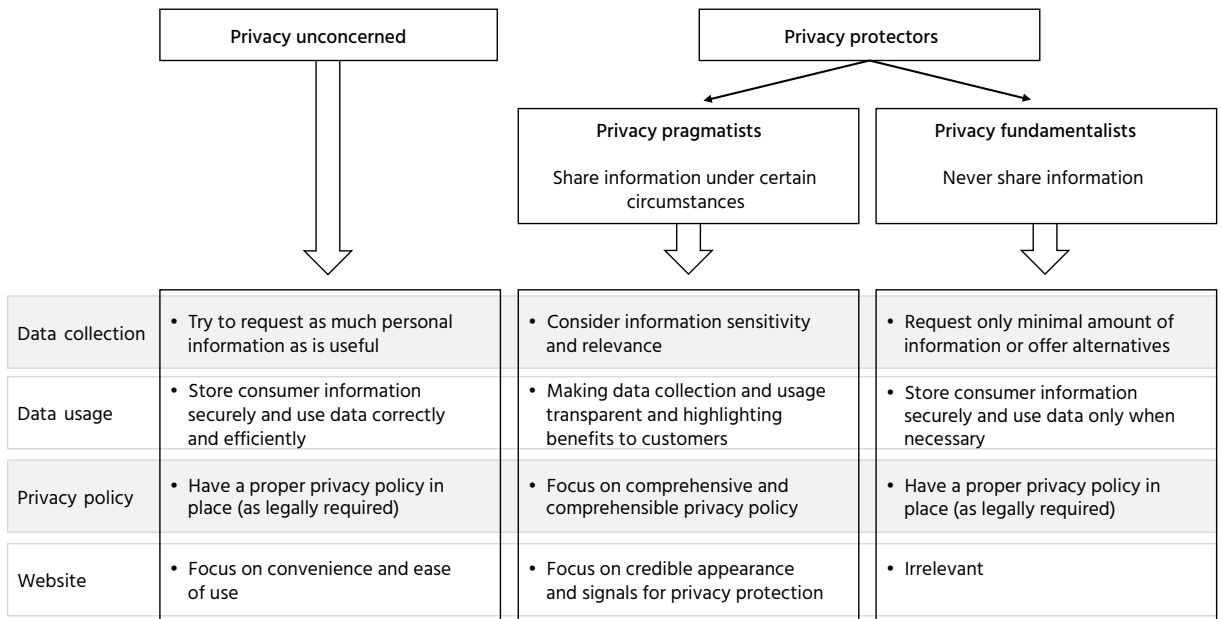
consumer behaviors (Lwin/Wirtz/Williams 2007; Wirtz/Lwin 2009). However, not all types of personal data being requested – for instance, demographic and lifestyle characteristics, purchasing habits, financial data, and personal identifiers (Phelps/Nowak/Ferrell 2000) – involve the same risk level, since different information lead to different perceived consequences of revealing and obscuring (Metzger 2007). Hence, more sensitive information is perceived as riskier to disclose than less sensitive information (Malhotra/Kim/Agarwal 2004). As a result, if an online shop's request to provide personal information is perceived as very sensitive by consumers and thus, as risky or even as privacy intrusion, this may cause higher concerns, and protective behaviors (H3).

Consumer-related Determinants

Familiarity with online shop

Personal familiarity refers to consumers' degree of acquaintance with a website, including knowledge of it and experiences such as information searches (Gefen 2000). Existing research finds a negative relationship between people's familiarity with a website and their privacy concerns (Sheehan/Hoy 2000). Being familiar with an online shop's buying process and its privacy concept allows consumers to form

Fig. 3: Overview of Approaches to Different Target Groups



Source: author's illustration.

favorable expectations of and trust in the vendor's handling of privacy issues. Since trust reduces perceived risk, consumers are more likely to consider the disclosure of their personal information acceptable (Gefen 2000). In contrast, low familiarity leads to higher privacy concern levels and a higher likelihood that consumers will engage in protective responses (H4).

Previous privacy experiences

Previous privacy experiences refer to consumers' personal online experiences during which their privacy was violated, for instance, through the misuse of data, or identity theft (Awad/Krishnan 2006). Such prior privacy invasions are found to increase privacy concerns (Bansal/Zahedi/Gefen 2010). When evaluating the risks and benefits of a disclosure, consumers rely on their past experiences. In case of negative experiences, consumers' trust may be reduced (Culnan/Bies 2003; Gefen 2000). As a result of reduced trust, consumers perceive the risk as higher and are more likely to develop privacy concerns and may engage in opportunistic behavior to protect themselves against negative experiences (Xu et al. 2008) (H5).

Method

The authors empirically examined the conceptualized relationships with a between-subjects design where two contrary real-life online shops, identified in a pretest, served as manipulating stimuli. The online survey had three parts, starting with a landing page and an introduction to the study. The participants were then provided with a screenshot of one of the two websites and their privacy policies. Part 3 contained general questions about the constructs. The participants were randomly assigned to one of the two conditions to avoid systematic differences between the subgroups. The final sample comprised 705 participants, of which 502 were female and 203 male. Most of the participants were between 21 and 30 years old (57.9%). Concerning education, most participants had a secondary school certificate (66.2%), followed by those with a university degree (27.6%). Concerning their experience with online shopping, the participants mostly shopped online 11 times and more per year.

The authors estimated the model using structural equation modeling (SEM), specifically using the software Smart-

PLS, which allows for simultaneously estimating interrelationships and causalities within the hypothesis system (Hair et al. 2014). Measurement validation shows that the data are well suited for an analysis using SEM. To assess the adequacy of the chosen measures, it is essential to analyze the constructs' objectivity, reliability, and validity. All the assumptions concerning Cronbach's Alpha (> 0.7), factor loadings (> 0.7) and discriminant validity (Fornell-Larcker criterion) were fulfilled.

Results and Managerial Implications

The results show that certain situation-related and consumer-related determinants have significant influences on privacy concerns and protective behaviors. Concerning situational factors, there is a direct significant influence of credibility on falsifying ($p < 0.01$) and on negative WoM ($p < 0.05$), but the relationship is not mediated by privacy concerns. On the contrary, the influence of perceptions of privacy policy on falsifying and negative WoM is partially mediated by privacy concerns ($p < 0.01$). The results imply that firms should clearly state and communicate their privacy policies to consumers via short, understandable notices. At least, privacy notices should be very visible on a firm's website. The authors also found that information sensitivity's effect on falsifying and negative WoM is partially mediated by consumer privacy concerns ($p < 0.01$). This implies that firms should consider carefully which kind of information they request in order to minimize potential protective behaviors. At the individual level, consumer privacy concerns do not mediate the relationship between familiarity with an

online shop and protective responses. In contrast, the relationship between previous privacy experiences and protective behaviors (i.e. falsifying and negative WoM) is mediated by privacy concerns ($p < 0.01$). This implies that companies should identify consumers with negative experiences in order to target them individually, to reduce their concerns and to (re)build trustful relationships.

Overall, the results imply that consumers' reactions to situational factors in the privacy context differ significantly. Most importantly, responses might differ not only owing to the examined situational factors but also owing to consumers' personalities. One can generally categorize consumers into those not concerned with privacy and privacy protectors, including the privacy pragmatists, who share information under certain circumstances, and the privacy fundamentalists, who never share information

The results imply that firms should clearly state and communicate their privacy policies to consumers.

(Westin 1967). These different types should be targeted differently concerning data collection, data usage, privacy policy, and website appearance. Different target options are presented in Figure 3.

Managers should focus on consumers not concerned with privacy in order to exploit the full potential of data

Management Summary

When disclosing personal information online, consumers may face privacy threats, which lead to growing privacy concerns and protective responses. This article develops a conceptual framework with a focus on situational and consumer-related determinants of behavioral responses, aimed at protecting oneself or others. Furthermore, based on the findings, the authors propose strategies to deal with different consumer groups.

Lessons Learned

- Managers of online firms should consider individuals' privacy needs and experiences and should preempt potentially protective responses.
- Consumers should be categorized based on their tendency to be concerned about privacy and to engage in protective responses.
- This enables companies to develop different approaches to data collection and use, privacy policy communication, and website appearance.



Main Propositions

1. Situation-specific determinants, such as credibility of an online shop, privacy policy perception and information sensitivity, as well as consumer-related experiences, such as familiarity with a website and previous privacy invasions, will affect the likelihood of consumers engaging in protective responses in case of data disclosure.
2. The effects of situational and consumer-related factors on protective responses will be mediated by consumer attitudes, i.e. privacy concerns.
3. Consumer concern-specific strategies will be required to reduce the likelihood of consumers engaging in protective responses.

usage (i.e. profiling, by targeting them individually) and on the privacy pragmatists by providing transparency, appearing credible, and communicating data usage benefits. As shown above, information sensitivity strongly influences consumer privacy concerns and may thus cause protective

responses. However, assuring the relevance of required information and informing consumers about its usage might help companies to reduce concerns, especially in case of privacy pragmatists. Privacy fundamentalists could be neglected in companies' efforts because it is unlikely that a


Literature

- Ansari, A./Mela, C. F. (2003): E-Customization, in: *Journal of Marketing Research*, 40, 2, pp. 131–145.
- Awad, N. F./Krishnan, M. S. (2006): The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization, in: *MIS Quarterly*, 30, 1, pp. 13–28.
- Bansal, G./Zahedi, F. M./Gefen, D. (2010): The Impact of Personal Dispositions on Information sensitivity, Privacy Concern and Trust in Disclosing Health Information Online, in: *Decision Support Systems*, 49, 2, pp. 138–150.
- Belk, R. W. (1975): Situational Variables and Consumer Behavior, in: *Journal of Consumer Research*, 2, 3, pp. 157–164.
- Culnan, M. J. (1995): Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing, in: *Journal of Direct Marketing*, 9, 2, pp. 10–19.
- Culnan, M. J./Bies, R. J. (2003): Consumer Privacy: Balancing Economic and Justice Considerations, in: *Journal of Social Issues*, 59, 2, pp. 323–342.
- Dinev, T./Hart, P. (2004): Internet Privacy Concerns and Their Antecedents: Measurement Validity and a Regression Model, in: *Behaviour & Information Technology*, 23, 6, pp. 413–422.
- Dinev, T./Hart, P. (2006): An Extended Privacy Calculus Model for E-Commerce Transactions, in: *Information Systems Research*, 17, 1, pp. 61–80.
- Gefen, D. (2000): E-Commerce: The Role of Familiarity and Trust, in: *Omega*, 28, 6, pp. 725–737.
- Hair, J. F. et al. (2014): *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Los Angeles.
- Lowry, P. B./Wilson, D. W./Haig, W. L. (2014): A Picture is Worth a Thousand Words: Source Credibility Theory Applied to Logo and Website Design for Heightened Credibility and Consumer Trust, in: *International Journal of Human-Computer Interaction*, 30, 1, pp. 63–93.
- Lwin, M. O./Williams, J. D. (2003): A Model Integrating the Multidimensional Development Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online, in: *Marketing Letters*, 14, 4, pp. 257–272.
- Lwin, M. O./Wirtz, J./Williams, J. D. (2007): Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective, in: *Journal of the Academy of Marketing Science*, 35, 4, pp. 572–585.
- Malhotra, N. K./Kim, S. S./Agarwal, J. (2004): Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, in: *Information Systems Research*, 15, 4, pp. 336–355.
- Mehrabian, A./Russell, J. A. (1974): *An Approach to Environmental Psychology*, Cambridge.
- Metzger, M. J. (2007): Making Sense of Credibility on the Web: Models for Evaluating Online Information and Recommendations for Future Research, in: *Journal of the American Society for Information Science and Technology*, 58, 13, pp. 2078–2091.
- Milne, G. R./Gordon, M. E. (1993): Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework, in: *Journal of Public Policy & Marketing*, 12, 2, pp. 206–215.

company can change their fundamental beliefs and attitudes to privacy via initiatives.

Today, companies have multiple possibilities to target consumers individually based on geographic, sociodemographic, lifestyle, and purchase history information. In addition, new ways of communication (i.e. behavioral targeting) will accelerate the importance and relevance of consumer privacy concerns and protective responses. Especially the emerging, promising field of mobile marketing requires an even more careful handling of individual privacy needs and attitudes (Stafflage 2016; White et al. 2008; Xu et al. 2011), since consumers might feel invaded in their private space and might react if communication is too personalized. Thus, companies always face a tradeoff between the potential advantages gained through customization and consumers' needs for privacy; if they do not consider individual privacy spaces, they will undermine customer loyalty.

To conclude, this is the first study to identify both situation-related and consumer-related predictors of protective responses. In a time when companies require big data, it is more important than ever that the data they store and

use for business purposes are correct. If not – in case consumers provide false information – they cannot create valuable customer profiles – the key success factor in many new e-commerce business models. Furthermore, negative WoM, especially via social media, can lead to substantial damage to a company's image and reputation (Verhoef/Reinartz/Krafft 2010). Thus, companies should be aware of and should actively address predictors that may cause consumer privacy concerns and protective responses. However, the authors addressed only a manageable set of influencing factors on protective responses. For more comprehensive insights into the formation of protective responses, it could be worth examining consumer attitudes towards an online shop and individual online purchase frequency. Furthermore, an online shop's reputation seems relevant, as well as the convenience offered by an online shop, which matters strongly in practice. 

Nam, C. et al. (2006): Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online, in: *Advances in Consumer Research*, 33, 1, pp. 212–217.

Pan, Y./Zinkhan, G. M. (2006): Exploring the Impact of Online Privacy Disclosures on Consumer Trust, in: *Journal of Retailing*, 82, 4, pp. 331–338.

Phelps, J./Nowak, G./Ferrell, E. (2000): Privacy Concerns and Consumer Willingness to Provide Personal Information, in: *Journal of Public Policy & Marketing*, 19, 1, pp. 27–41.

Sheehan, K. B./Hoy, M. G. (2000): Dimensions of Privacy Concern Among Online Consumers, in: *Journal of Public Policy & Marketing*, 19, 1, pp. 62–73.

Smith, H. J./Milberg, S. J./Burke, S. J. (1996): Information Privacy: Measuring Individuals' Concerns About Organizational Practices, in: *MIS Quarterly*, 20, 2, pp. 167–196.

Son, J. Y./Kim, S. S. (2008): Internet Users' Information Privacy-Protective Responses. A Taxonomy and a Nomological Model, in: *MIS Quarterly*, 32, 3, pp. 503–529.

Stafflage, M. (2016): *In-store Mobile Marketing-Kommunikation*, Wiesbaden.

Stone, E. F. et al. (1983): A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations, in: *Journal of Applied Psychology*, 68, 3, pp. 459–468.

Taylor, C. R. (2004): Consumer Privacy and the Market for Customer Information, in: *The RAND Journal of Economics*, 35, 4, pp. 631–650.

Verhoef, P. C./Reinartz, W. J./Krafft, M. (2010): Customer Engagement as a New Perspective in Customer Management, in: *Journal of Service Research*, 13, 3, pp. 247–252.

Wang, S./Beatty, S. E./Foxy, W. (2004): Signaling the Trustworthiness of Small Online Retailers, in: *Journal of Interactive Marketing*, 18, 1, pp. 53–69.

Westin, A. F. (1967): *Privacy and Freedom*, New York.

Wirtz, J./Lwin, M. O. (2009): Regulatory Focus Theory, Trust, and Privacy Concern, in: *Journal of Service Research*, 12, 2, pp. 190–207.

White, T. B. et al. (2008): Getting too Personal: Reactance to Highly Personalized Email Solicitations, in: *Marketing Letters*, 19, 1, pp. 39–50.

Xie, E./Teo, H. H./Wan, W. (2006): Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior, in: *Marketing Letters*, 17, 1, pp. 61–74.

Xu, H. et al. (2008): Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View, in: *ICIS 2008 Proceedings*, Paper 6.

Xu, H. et al. (2011): The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing, in: *Decision Support Systems*, 51, 1, pp. 42–52.

Zhang, J./Krishnamurthi, L. (2004): Customizing Promotions in Online Stores, in: *Marketing Science*, 23, 4, pp. 561–578.