Consumer Informational Privacy: Current Knowledge and Research Directions
Other titles in Foundations and Trends® in Marketing

Entertainment Marketing
Natasha Zhang Foutz
ISBN: 978-1-68083-332-4

The Cultural Meaning of Brands
Carlos J. Torelli, Maria A. Rodas and Jennifer L. Stoner
ISBN: 978-1-68083-286-0

Ethnography for Marketing and Consumer Research
Alladi Venkatesh, David Crockett, Samantha Cross and Steven Chen
ISBN: 978-1-68083-234-1

The Information-Economics Perspective on Brand Equity
Tulin Erdem and Joffre Swait
Consumer Informational Privacy: Current Knowledge and Research Directions

Frank T. Beke
University of Groningen, The Netherlands
f.t.beke@rug.nl

Felix Eggers
University of Groningen, The Netherlands
f.eggers@rug.nl

Peter C. Verhoef
University of Groningen, The Netherlands
p.c.verhoef@rug.nl

Full text available at: http://dx.doi.org/10.1561/1700000057
Foundations and Trends® in Marketing
Volume 11, Issue 1, 2018
Editorial Board

Editor-in-Chief
Jehoshua Eliashberg
University of Pennsylvania

Associate Editors
Bernd Schmitt
Columbia University

Editors
David Bell
University of Pennsylvania
Gerrit van Bruggen
Erasmus University
Christophe van den Bulte
University of Pennsylvania
Amitava Chattopadhyay
INSEAD
Pradeep Chintagunta
University of Chicago
Dawn Iacobucci
Vanderbilt University
Raj Ranganathan
University of Texas, Austin
J. Miguel Villas-Boas
University of California, Berkeley

Full text available at: http://dx.doi.org/10.1561/1700000057
Editorial Scope

Topics

Foundations and Trends® in Marketing publishes survey and tutorial articles in the following topics:

- B2B Marketing
- Bayesian Models
- Behavioral Decision Making
- Branding and Brand Equity
- Channel Management
- Choice Modeling
- Comparative Market Structure
- Competitive Marketing Strategy
- Conjoint Analysis
- Customer Equity
- Customer Relationship Management
- Game Theoretic Models
- Group Choice and Negotiation
- Discrete Choice Models
- Individual Decision Making
- Marketing Decisions Models
- Market Forecasting
- Marketing Information Systems
- Market Response Models
- Market Segmentation
- Market Share Analysis
- Multi-channel Marketing
- New Product Diffusion
- Pricing Models
- Product Development
- Product Innovation
- Sales Forecasting
- Sales Force Management
- Sales Promotion
- Services Marketing
- Stochastic Model

Information for Librarians

Foundations and Trends® in Marketing, 2018, Volume 11, 4 issues. ISSN paper version 1555-0753. ISSN online version 1555-0761. Also available as a combined paper and online subscription.
Consumer Informational Privacy: Current Knowledge and Research Directions

Frank T. Beke\textsuperscript{1}, Felix Eggers\textsuperscript{2} and Peter C. Verhoef\textsuperscript{3}

\textsuperscript{1}University of Groningen, The Netherlands; f.t.beke@rug.nl
\textsuperscript{2}University of Groningen, The Netherlands; f.eggers@rug.nl
\textsuperscript{3}University of Groningen, The Netherlands; p.c.verhoef@rug.nl

ABSTRACT

In the current age of information and big data, consumer informational privacy has become an important issue in marketing. Besides being worried about the growing collection, storage, and use of personal information, consumers are anxious about a lack of transparency or control over their personal data. Despite these growing concerns, understanding of how firms’ privacy practices affect consumers remains limited. We review the relevant literature on consumer privacy from a marketing perspective and summarize current knowledge about how information collection, information storage, information use, transparency, and control influence consumers’ behavior. In addition, we discuss to what extent the influence of firms’ privacy practices differs between firms, consumers, and environments. On the basis of this knowledge, we formulate several hypotheses aimed at providing direction for future research regarding the role of consumer informational privacy in marketing.
1

Introduction

We are living in the *age of information*. Since firms started to realize that data could generate value for them and for their customers, they began collecting, storing, and using more data (or information) about consumers. Every year 16.1 trillion gigabytes of data are recorded, and forecasts are that this will grow to 163 trillion gigabytes by 2025 (Reinsel *et al.*, 2017). Consumer data allow firms to better understand their customers and provide products and services that better match consumers’ need and preferences. Customer relationship management, customer intelligence, and, more recently, one-to-one marketing have all emerged by virtue of collecting information (Rust and Huang, 2014).

However, controversial revelations regarding the expansion of information collection and privacy in general (e.g., Edward Snowden’s disclosures about data collection and surveillance programs) has resulted in a worldwide surge of privacy concern. In the United States, 92% of consumers worry about their online privacy (TRUSTe, 2016), while globally 57% of consumers were more concerned about their privacy compared to last year (CIGI-Ipsos, 2017). These concerns could deter consumers from accepting information collection, which matters even more in times in which privacy legislation and technological innovations —
such as cookie blockers and privacy-protective browsers — provide consumers more control over their privacy. For example, a recent study by Pew Research shows that 60% of consumers have chosen to not install an app when the collection of information was considered excessive, while 43% have uninstalled an app after finding out about excessive information collection (Olmstead and Atkinson, 2015). Even when consumers might not immediately abandon firms that neglect privacy it could result in bad publicity and a loss of trust in case consumers find out about the collection, storage, and use of information afterwards. For example, when consumers became aware Samsung was recording all interactions with their “smart” TVs, criticism went as far as accusing Samsung of spying on their customers (Forbes, 2015). Given the importance of information for firms, understanding how privacy affects consumers, and, more specifically, when and why consumers accept or reject the collection, storage, and use of information, has become crucial for the field of marketing (Wedel and Kannan, 2016; Montgomery and Smith, 2009).

Despite the growing attention for privacy, the understanding of how firms’ privacy practices affect consumers and their relationships with firms is in its infancy. As privacy is an interdisciplinary topic, the knowledge about privacy and information disclosure is dispersed across scientific domains, ranging from social psychology to information systems and public policy. Within marketing, privacy has mainly been studied in the direct or interactive marketing literature (Culnan, 1995; Nowak and Phelps, 1995; Milne and Boza, 1999; Schoenbachler and Gordon, 2002; Phelps et al., 2000; Milne and Gordon, 1993), as part of service quality (Parasuraman et al., 2005; Wolfinbarger and Gilly, 2003), or, more recently, in the literature on online advertising (Tucker, 2014; Bleier and Eisenbeiss, 2015a; Schumann et al., 2014; Goldfarb and Tucker, 2011a). Although Peltier et al. (2009) and Martin and Murphy (2017) have provided a global overview on the role of privacy within marketing, due to their broad focus the specific understanding of how firms’ privacy practices affect consumers need to be elaborated. While Lanier and Saini (2008) address part of this void by discussing (some) firm-related privacy issues, we believe a more structured overview focused on the influence of firms’ privacy practices on consumers is...
Introduction

necessary. Specifically, firms need a more detailed understanding of when and why consumers are (un)willing to disclose information and how a firm’s privacy strategy affects the relationship with their customers, such as when customers might consider switching to a competing firm. We therefore focus on how firms’ privacy practices have an impact on consumers, their privacy concerns, and the exchange of information.

Our objective of this paper is twofold. First, we use current knowledge about privacy and information disclosure to outline the main empirical findings regarding the influence of firms’ privacy practices on consumers’ behavior. In doing so, we also discuss how the influence of firms’ privacy practices on consumers differs between firms, consumers, and contexts. Second, drawing on current knowledge we identify areas in need of further research and formulate hypotheses for them. We start by conceptualizing consumer informational privacy and then derive a conceptual framework, which guides the subsequent sections.

1.1 Conceptualization of consumer informational privacy

In light of the rise of photography and growing circulation of newspapers at the beginning of the 20th century, legal scholars Warren and Brandeis (1890) stressed the importance of privacy as “the right to be let alone.” Besides preventing others from intruding an individual’s personal sphere, such as their house, they also stated that every individual should be protected against improper publications. While the initial focus was on others being physically present in someone’s personal sphere (physical privacy), the growing collection, storage, and use of personal information has shifted the attention to informational privacy (Goodwin, 1991; Rust et al., 2002; Mason, 1986). Informational privacy intrusion relates to others monitoring and recording an individual’s behavior, and thus to the collection and storage of information, without necessarily being physically present. Meanwhile, protection from improper publications

---

1 Given our focus on empirical findings we exclude papers describing economic models (for an overview, see Acquisti et al., 2016) or exploring the influence of public policy on firms (Miller and Tucker, 2009; Adjerid et al., 2016).

2 In line with recent legislation, we consider personal information to be all information that can be attributed to one individual (General Data Protection Regulation (EU), 2016).
1.1. Conceptualization of consumer informational privacy

relates to how the information is being used. The growing importance of consumer information directs the focus throughout this paper to informational privacy of consumers, to which we will simply refer to as privacy.

There has been much discussion on how privacy should be defined. Some scholars have suggested that privacy is context-specific so that it cannot be generally defined (Martin and Murphy, 2017; Pavlou, 2011; Smith et al., 2011). This literature stream has proposed to focus on harmful activities using information instead (Prosser, 1960; Solove, 2006), whereby context-specific norms determine whether activities are harmful and thus violate privacy (Nissenbaum, 2004). Despite these suggestions, we follow the juridical standpoint that privacy is matter of autonomy and control over the collection, storage, and use of information (Westin, 1967; Altman, 1975; Petronio, 1991; Stone et al., 1983; Smith et al., 1996; Malhotra et al., 2004). Recent privacy laws and guidelines in the United States and the European Union have also adopted this standpoint on privacy, as they aim to let consumers decide for themselves what happens with their information. This implies that privacy is only violated when information is collected, stored, or used against the consumer’s will. Consumers’ effective control depends on being aware of and having the ability to influence the collection, storage, and use of information (Goodwin, 1991; Foxman and Kilcoyne, 1993; Caudill and Murphy, 2000). Therefore, in the context of firms and consumers we define privacy as the extent to which a consumer is aware of and has the ability to control the collection, storage, and use of personal information by a firm. Thus, if firms want to respect consumers’ privacy they should explain what information they collect, how they store the information, and for which purposes they will use the information (transparency). Moreover, firms should allow consumers to prevent firms from collecting information, to have them discard information, and to prohibit them from using their information (control).

Across a wide range of disciplines, ranging from social psychology to information systems and, more recently, marketing, there has been a debate about what privacy is and what privacy is not (Smith et al., 2011; Spärck Jones, 2003). Because privacy is contingent on control, knowingly disclosing information or accepting information collection
is not a violation or deterioration of privacy. This implies that, unlike prior suggestions (Rust et al., 2002; Posner, 1981; Posner, 1978), we consider privacy not the same as concealing or withholding information. Although related, privacy is also not the equivalent of security, as that implies that (unknown) outsiders illegally — that is, without proper authorization — intercept or access information (Belanger et al., 2002; Martin et al., 2017; Hoffman et al., 1999). Given that information is collected, stored, or used without consumers knowingly consenting when security fails, security can be considered as one requirement for ensuring privacy and will be treated as such.

1.2 Conceptual framework

Figure 1.1 presents our conceptual framework, which guides our discussion of the literature. We will discuss how firms’ privacy practices, which encompasses the way firms handle the information and privacy of consumers, affects consumers’ attitudes, intentions, and behavior. Specifically, we discern five privacy practices that matter to consumers: information collection, information storage, information use, transparency, and (consumer) control. Understanding when consumers withhold (or falsify) information, reject information collection, or even refuse to interact or transact with a particular firm owing to its privacy practices has become crucial for managers. Moreover, firms need to know how consumers are affected when confronted with the storage and use of personal information, through marketing communication or location-based services.

Consumers’ attitudes or perceptions with regard to privacy, such as privacy concern, often mediate the effect of firms’ privacy practices on consumers’ intentions or behavior. Therefore, many studies have used these attitudes or perceptions either as proxies for firms’ privacy practices (predictor) or as surrogates for consumer behavior (outcome). What complicates matters is that the influence of firms’ privacy practices on consumers could differ between firms, consumers, and environments. For example, consumers accept the collection of medical information more easily when done by healthcare providers (firms), when being in
1.2. Conceptual framework

Figure 1.1: Conceptual framework.

Full text available at: http://dx.doi.org/10.1561/1700000057
perfect medical condition (consumers), or when privacy is regulated (environment).

To explain the influence of firms’ privacy practices on consumer behavior, most studies have focused on the construct of privacy concern. Although conceptualized and operationalized in various ways, privacy concern always captures consumers’ perceptions (or attitudes) of how the collection, storage, and use of personal information, or (lack of) transparency or control, negatively affect them (Smith et al., 1996; Malhotra et al., 2004). Whereas the collection, storage, and use of personal information matter due to the negative consequences consumers may endure (distributive fairness), social contract theory suggests that transparency and control also matter as consumers also take the procedures and interpersonal treatment (procedural fairness) into account (Donaldson and Dunfee, 1994). The importance of transparency and control is also established in reactance theory, which proposes that consumers resist being restricted in their choices (Brehm, 1966). In the context of privacy this implies that consumers will respond positively (negatively) when they believe firms are (not) transparent and provide (no) control over the collection, storage, and use of personal information (Culnan and Bies, 2003; Son and Kim, 2008). Besides privacy concern, Table 1.1 provides an overview of related constructs scholars have used to capture consumers’ worries or uneasiness (attitudes and perceptions), such as privacy risk (Featherman et al., 2010), perceived privacy (Dinev et al., 2013), information sensitivity (Mothersbaugh et al., 2012), intrusiveness (Li et al., 2002; Burgoon et al., 1989), and vulnerability (Martin et al., 2017).

Prior work has applied various theoretical frameworks to explain why consumers disclose information despite being concerned. Consumers’ ability to protect their own privacy (protection motivation theory) (Rogers, 1975; Youn, 2009), or their trust in specific firms (Morgan and Hunt, 1994; Wirtz and Lwin, 2009) might diminish consumers’ concerns in a specific context. More recently the rationale that consumers look beyond the negative outcomes (concerns), and also take the positive outcomes of the collection, storage, and use of personal information into account, has taken root. Being closely related to social exchange theory (Homans, 1958; Premazzi et al., 2010) and expectancy theory
1.2. Conceptual framework

Table 1.1: Privacy concern and related constructs.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy concern</td>
<td>A consumer’s worries or uneasiness with regard to the collection, storage, and use of personal information, or (a lack of) transparency and control</td>
<td>Smith <em>et al.</em> (1996) and Malhotra <em>et al.</em> (2004)</td>
</tr>
<tr>
<td>Privacy risk</td>
<td>Subjective assessment of potential losses of confidential personally identifying information, including potential misuse</td>
<td>Featherman <em>et al.</em> (2010)</td>
</tr>
<tr>
<td>Perceived privacy</td>
<td>An individual’s self-assessed state in which external agents have limited access to information about him or her</td>
<td>Dinev <em>et al.</em> (2013)</td>
</tr>
<tr>
<td>Information sensitivity</td>
<td>The potential loss or risk for consumers when information is disclosed</td>
<td>Mothersbaugh <em>et al.</em> (2012)</td>
</tr>
<tr>
<td>Intrusiveness</td>
<td>The extent to which an individual perceives unsolicited invasion in his or her personal sphere</td>
<td>Burgoon <em>et al.</em> (1989)</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Perception of susceptibility to harm owing to unwanted use of personal data</td>
<td>Martin <em>et al.</em> (2017)</td>
</tr>
</tbody>
</table>

(Vroom, 1964; Hann *et al.*, 2007), the privacy calculus suggests that consumers determine for themselves whether they regard the consequences of the collection, storage, and use of personal information to be beneficial (providing benefits) or detrimental (incurring costs or risks) in a specific situation (Laufer and Wolfe, 1977; Culnan and Armstrong, 1999; Dinev and Hart, 2006). These consequences can be tangible (e.g., monetary discount) or intangible (e.g., uncomfortable feeling), and have been explained using more generic theoretical frameworks, such
as the theory of reasoned action (Fishbein and Ajzen, 1975) or the technology acceptance model (Davis, 1989). The privacy calculus is however considered as the “most useful framework” to understand the acceptance of information collection (Culnan and Bies, 2003, p. 326). Since the privacy calculus can accommodate most theoretical frameworks it has seen many explicit or implicit applications (Mothersbaugh et al., 2012; Premazzi et al., 2010; Dinev and Hart, 2006; Xie et al., 2006), and will serve as foundation for this review as well.

1.3 The privacy calculus and the privacy paradox

Despite the growing prominence of the privacy calculus, in some situations consumers’ privacy attitudes or perceptions are inconsistent with their actual privacy-related behavior — a discrepancy that has been termed the privacy paradox (Berendt et al., 2005; Norberg et al., 2007). Researchers have offered various explanations for its existence (Acquisti et al., 2015; Dinev et al., 2015). Besides that some part of consumer behavior is inherently inconsistent or suffers from bounded rationality (Ariely, 2009), consumers’ privacy concerns are seldom triggered. Especially in low-involvement situations, such as when consumers search online or use their mobile phone, the influence of biases and heuristics can be strong (Petty and Cacioppo, 1986; Chaiken, 1980). In other instances, consumers are unable to respond because they are unaware that information is being collected or used (Acquisti and Grossklags, 2005b), lack the ability to control firms’ privacy practices (Turow et al., 2009), or have no suitable alternatives.

Apart from irrational behavior or situations in which consumers are unaware or unable to exert control, the privacy paradox has also been a measurement issue. Given that consumers’ privacy preferences are strongly influenced by situational or contextual characteristics (Nissenbaum, 2004), when and for which context privacy concern is measured matters — that is, privacy concern with regard to a specific technology (e.g., the Internet), a specific firm (e.g., Google), or a specific situation (e.g., when searching for a product). Moreover, benefits have either been ignored, measured incompletely, or using only very generic measures (e.g., Xu et al., 2009; Xu et al., 2011). In addition, the

Full text available at: http://dx.doi.org/10.1561/1700000057
1.3. The privacy calculus and the privacy paradox

Consequences (benefits and costs) of the collection, storage, and use of information are not always immediate and definite (Brandimarte et al., 2013), which suggests that the perceived probability of consequences should be taken into account (Risk Theory, Bauer, 1960; Conchar et al., 2004). So we suggest that consumers’ acceptance of the collection, storage, and use of personal information is best explained by their context-specific perception of the benefits and costs, taking into account transparency, control, and the uncertainty of these benefits and costs.

**Hypothesis 1:** Consumers’ acceptance of the collection, storage, and use of personal information is best explained by their context-specific perception of the benefits and costs, taking into account transparency, control, and the uncertainty of these benefits and costs.
Acknowledgments

Acknowledgments

References


References


Turow, J., J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy (2009). “Americans reject tailored advertising and three activities that enable it”.


