The Role of Privacy in the Era of Digital Customization

Bachelors Thesis

Claudia Zimmermann

Spring Term 2017

Advisor:
Veronica Valli

Chair of Quantitative Marketing and Consumer Analytics
L5, 2 - 2. OG
68161 Mannheim
www.quantitativemarketing.org

Table of Content

List Of Figures

List Of Abbreviations

RFID	Radio Frequency Identification
IoT	Internet of Things
IPC	Internet Privacy Concern
IBT	Information Boundary Theory
FDA	Federal Drug Administration
ECPA	Electronic Communications Privacy Act
FTC	Federal Trade Commission

Abstract

This thesis examines the role of privacy in the era of digital customization by means of a literature review. While personalized communication inhabits many benefits such as convenience to users, the necessary data collection threatens the consumers' information privacy. Even though privacy concerns are consumer-heterogeneous and context-dependent, a trade-off between personalization and privacy arises. If the data collection penetrates an individual's information boundaries, personalization will be perceived as an invasion to privacy. Trust, however, can have a mitigating effect on the trade-off and can facilitate the transfer of sensitive information from the user to the organization. Therefore, firms should focus on trust-building practices in order to compensate the insufficient privacy regulations, which are currently employed. Consequently privacy has a significant role in the era of digital customization and this thesis will introduce managerial implications and suggestions for future research.

1. Introduction

Global data volume grows exponentially every year due to new technologies like smartphones and social networks like Facebook (The Economist 2016). The ability to produce and store large amounts of data enables a more sophisticated decision process. For firms the buzzword "big data" is omnipresent and the essential base for managerial decisions is nowadays an extensive amount of collected data. Among others, data about consumers, their purchase behaviour and their preferences are collected. In order to collect this immense amount of information about customers not only the internet, but also chips and sensors are employed. One example is the Radio Frequency Identification (RFID) bracket Disney World utilizes to track visitors' entry and exit at its theme parks along with spots where visitors like to take pictures at (Park and Skoric 2017, p. 76). Another example is State Farm, which installed a speed-tracking device in customers' cars and granted them insurance discounts in return (Park and Skoric 2017, p. 76).

Now wearable devices, such as fitness trackers and Google Glass, overtake the market and contribute to the exponential growth in data volume. Companies can use the gathered information to communicate relevant content to the users and make selective product offers. Therefore, this personalized communication inhabits various benefits for customers and organizations. However, these devices and their data collection can exacerbate an already existing threat to an individual's privacy. It does not seem to be apparent to users what kind of information is collected by firms and for how long this data is stored. Neither can users say with certainty how this information is utilized and whether organizations might sell the obtained data. This uncertainty has multiple reasons, but clearly impacts users' perceived integrity of their privacy.

Therefore, this thesis will conduct a literature review to examine the role of privacy in the era of digital customization. In order to do so, we first need to define the technological

context with the benefits of personalized communication. Subsequently we can elaborate the concepts of privacy and privacy concerns in the digital era. Furthermore, we will depict the arising trade-off between personalization and privacy and elaborate to what extend data collection is perceived as invasive. Additionally, the role of trust in this inverse relationship will be outlaid along with the currently employed regulations to protect an individual's privacy. After illustrating the managerial implications of these findings, and giving suggestions for future research, we will then draw a conclusion about the role of privacy in the digital era of customization.

2. Digital Customization And The Internet Of Things

The Internet of Things (IoT) consists of smart devices, which enable wireless communication through microchips and sensors (Thierer 2014, p. 1). The terminology 'thing' in IoT refers to a tagged item, which allows for the communication of data concerning the item and its close surroundings (Zhou and Piramuthu 2015, p. 21). Wearable technologies build a subset of the IoT and cannot only collect data by tracking activities but also "customize experiences to users' needs and desires" (Thierer 2014, p. 1). This is achieved through a communication with the item in a personalized manner (Zhou and Piramuthu 2015, p. 21). Customized devices inherit many beneficial features, which will be illustrated in the following subchapter.

2.1. Benefits Of Personalization For Organizations And Users

The main function of personalization is to deliver users what they want when they want it (Tam and Ho 2006, p. 868). Research suggests, that personalized communication is identified as more useful by users and can create a positive mindset towards recommended offers through relevant content (Tam and Ho 2006, p. 885). Furthermore, personalized messages can help users in their decision-making process by cutting down information overload and providing relevant content only (Tam and Ho 2006, p. 887). This customized content, which

is coherent with the user's self-concept, can likely influence the individuals' brand preference and purchase intention in a positive manner (Hong and Zinkhan 1995, p. 53).

This positive effect on the users' purchase intention through personalization does not necessarily translate directly into actual purchases, but could increase the advertising revenue or sales revenue of organizations (Ho and Bodoff 2014, p. 518). Consequently, the benefits of personalization are evident and are manifested in the convenience for users as well as in the potential revenue of organizations employing this practice. Wearable devices , however, can add another layer to the benefits of personalization, which will be shown subsequently.

2.2. Wearables As An Enhancement Of Human Empowerment

Our lives are already unimaginable without personalized technologies like Smartphones and Tablets, but wearable technologies like fitness bands and Google Glass go one step further. While the former is only being carried and used when needed, the latter is constantly worn directly on the human body. Hence, wearable devices form a more intense integration, which allows for real-time data collection (Park and Skoric 2017, p. 80). These wearable devices are capable of gathering information about the wearer's heart rate, body temperature, stress level, location, movement, sleep patterns and other related information (Langley 2015, p. 1642). Through their significant convenience, these computing devices can augment human freedom and empowerment (Park and Skoric 2017, p. 80).

Despite its positive aspects, wearable innovations face barriers in form of individuals' privacy concerns (Zhou and Piramuthu 2015, p. 19). The following questions arise in the users' mind: What kind of information is collected? For how long is this data stored? What is done with the personal information besides the intended use? Park and Skoric argue, that "privacy should [not] be an absolute point of defence against the hyper-commercialization of personal data" but a better fit between policy and technological innovations needs to be achieved (2017, p. 80).

In the following chapters, we will take a closer look at the individuals' privacy concerns, the role of trust and the policies, which are currently in place to protect the privacy at stake.

3. Privacy In The Digital Era

Multiple definitions exist for the concept of general privacy. While legal and political theories define general privacy as a human right, the economic perspective views general privacy as a commodity in exchange for benefits and, finally, Psychology and Marketing interpret general privacy as control (Smith, Dinev, and Xu 2011, p. 993). In the online world, though, these definitions face new challenges. In this particular medium information privacy is of foremost interest and has been defined as an individual's control over the personal data held by another party and its use (Clarke 1999, p. 60).

According to Martin the perception of privacy in the online world can be outlaid by identifying online privacy as a social contract between the firm and consumers (2012, p. 520). This social contract serves as an agreement about the usage and distribution of information and is beneficial to both parties (Martin 2016, p. 551). Since firms represent one side of the social contract, it is their responsibility to employ solutions, which are also beneficial and sustainable to the users (Martin 2016, p. 551). The privacy norms, which follow from the social contract, govern the type of information shared, limit the data access and negotiate how the information is used (Martin 2016, p. 557). These norms are not constant across different dimensions and their variation will be illustrated in the following. Afterwards, we will discuss the evolved personalization-privacy trade-off, the mitigating role of trust in this issue and the currently employed privacy regulations.

3.1. Concerns For An Individuals' Privacy

Recently developed methods such as data mining make it possible for firms to target customers specifically based on their online search patterns (Dinev and Hart 2006, p. 65).

This, however, requires an extensive amount of data about the customers online behaviour, which consequently leads to the users' increasing concern about how the extracted data is used and who has access to it (Dinev and Hart 2006, p. 65). The customers' perception of companies to be profit-driven creates uncertainty about the possible retention and selling of their personal data (Park and Skoric 2017, pp. 72–75).

This development intensifies with the introduction of wearable technologies. While a desktop computer can only collect data when the user is physically present, wearables allow for a constant real-time data tracking (Park and Skoric 2017, p. 76). The features of fitness trackers or Google Glass may inhabit a new height of data exploitations e.g. through a non-stop data collection, the possibility of processing and selling a user's health records and following their eye movements in every aspect of their life (Park and Skoric 2017, p. 79). These concerns for privacy can manifest in different dimensions, which will be demonstrated subsequently, along with the underlying aspects of justice theories.

3.1.1. Dimensions of an individuals' internet privacy concerns. Due to disagreements on how to conceptualize Internet Privacy Concerns (IPC) in past research, Hong and Thong developed and validated a third-order conceptualization with two second-order factors and six first-order factors, which is shown in Figure 1 (2013, pp. 284–92). The two dimensions in the second-order are interaction management and information management with the following six key dimensions in the first order: collection, secondary usage, errors, improper access, control and awareness (Hong and Thong 2013, p. 293).

While interaction management includes the individuals' concerns about the movement of personal data between themselves and companies, information management consists of the concerns about the firms' management of the personal information (Hong and Thong 2013, p. 293). The collection dimension entails the worry about the amount of personal information, which a company acquires, relative to the customers' perceived benefit obtained (Malhotra, Kim, and Agarwal 2004, p. 338). Secondary usage focuses on the fear that information, that

has been collected for a specific purpose, is also used for a secondary purpose without asking the individual for permission (Smith, Milberg, and Burke 1996, p. 171). The error dimension refers to the concern that firms can make deliberate and accidental errors in the database without employing sufficient protection against them (Smith, Milberg, and Burke 1996, p. 173). Another key dimension called improper access reflects the concern that people, who are not appropriately authorized, have access to the personal information of customers (Smith, Milberg, and Burke 1996, p. 173). The control dimension exhibits the worry about the degree to which an individual has control over the information held by a firm (Malhotra, Kim, and Agarwal 2004, p. 339). Finally, the last dimension called awareness encompasses an individuals' concern about being aware of the information privacy practice a firm deploys (Malhotra, Kim, and Agarwal 2004, p. 339). The awareness dimension is viewed independently since a firm's choice of interaction and information management practices do not influence the decision on making the customer aware of these practices (Hong and Thong 2013, p. 291).

This representation of IPC reconciles the different conceptualizations of internet privacy concerns, which have been established through research. It focuses rather on the users' concern than on their expectations of firms' behaviour (Hong and Thong 2013, p. 293). Now that we have established a concept for privacy concerns, we can examine its relationship to the theories of justice.

3.1.2 Privacy concerns and theories of justice. Research suggests that the collection and dissemination of information through online channels can be viewed as an exchange of users' personal data for online benefits as illustrated in Figure 2 (Ashworth and Free 2006, p. 110). When examining the inputs (e.g. providing personal information) and outcomes (e.g. receiving a compensation) of such an exchange, the user evaluates whether the exchange can be perceived as fair or not (Ashworth and Free 2006, p. 112). The notions of justice and fairness have been studied in many fields of studies, but we will be focusing on the

psychological viewpoint in which justice consists of two components, namely distributive and procedural justice (Ashworth and Free 2006, p. 112). In the following, we will illustrate these two theories of justice, which underlie and explain the previously established concept of IPC.

Distributive justice relates to the perceived fairness of the distribution of outcomes of such an information exchange (Ashworth and Free 2006, p. 113). This is investigated through an equity theory, comparing the ratio of consumer's outcomes relative to their inputs with the ratio of firm's outcomes relative to their inputs (Ashworth and Free 2006, p. 114). A fair allocation, therefore, requires the each parties' outcomes to be in proportion with the inputs (Ashworth and Free 2006, p. 113). For example, the IPC's collection dimension is grounded in the principle of distributive justice (Malhotra, Kim, and Agarwal 2004, p. 338). This means that the information exchange is only perceived as fair if the personal data collected by the firm is in proportion with the benefits the customer receives (Malhotra, Kim, and Agarwal 2004, p. 338). A disproportioned allocation increases the perceived inequity and decreases the perceived justice and, consequently, leads to an increase in privacy concerns (Ashworth and Free 2006, p. 117).

Procedural justice relates to the perceived fairness of the rules and policies, which are in place to distribute the outcomes (Leventhal 1980, p. 5). Research suggests that individuals undertake this judgement through a comparison of their personal treatment with normative standards of respectful behaviour (Miller 2001, p. 531). Relevant benchmarks for the collection of personal data can be the norms of openness, information access, permission, notice and honesty (Ashworth and Free 2006, p. 115). For example, the IPC's dimension of awareness is decisive for the procedural judgement (Ashworth and Free 2006, p. 116). A lack of awareness relates to the violations of the norms permission and notice, which can lead to a decrease in perceived procedural fairness and, thus, to an increase in privacy concerns (Ashworth and Free 2006, p. 117). This means that the information exchange is only perceived as fair if the individual has given his consent to the information collection and is

aware of the data accumulation (Ashworth and Free 2006, p. 115; Malhotra, Kim, and Agarwal 2004, p. 339).

Consumers' fairness judgement of the information exchange manifests in their privacy concerns and can be a source of positive or negative consumer behaviour (Ashworth and Free 2006, p. 118). For that reason, firms need to consider not only direct outcomes, but also allocation procedures of the online interaction to influence the consumers' fairness judgement and privacy concerns.

3.1.3. Individuals hold heterogeneous privacy concerns. Despite the established universal framework of IPC and underlying justice theories, not every individual has privacy concerns to the same extent since it is argued that privacy is consumer-heterogeneous and context-dependent (Zhou and Piramuthu 2015, p. 19). Privacy concern as an independent variable is influenced by the user's previous privacy experience, demographics and culture (Smith, Dinev, and Xu 2011, p. 998). Previous privacy experience signifies that individuals who have already experienced a violation of their information privacy norms in the past, might hold stronger privacy concerns from then onwards (Smith, Milberg, and Burke 1996, p. 186). In terms of demographic differences research, for instance, suggests that women are generally more concerned about information privacy than men (Lowry, Cao, and Everard 2011, p. 188; Sheehan 1999, p. 24). With regard to the cultural differences, Hofstede's four cultural dimensions (1980) have been tested for their relationship with privacy concerns. The results show that uncertainty avoidance and collectivism increase information privacy concerns, whereas power distance decreases IPC (Lowry, Cao, and Everard 2011, p. 188).

We conclude that the degree to which an individual has privacy concerns depends on various aspects including the six key dimensions, the underlying perception of fairness and further facets. This heterogeneity across consumers has different managerial implications, which will be further discussed towards the end of this thesis. In the subsequent part we will investigate how these privacy concerns can build barriers to personalized innovations.

3.2. Trade-off Between Customization And Privacy

The previously stated benefits of personalization features such as usefulness and convenience in technological devices rely heavily on the collection of personal information. The collection of personal data, however, can interfere with the user's privacy preferences (Sutanto et al. 2013, p. 1141). Users worry that the collection and usage of their personal data can be invasive to their privacy (Lee, Ahn, and Bang 2011, p. 423). Although data tracking of preferences and behaviours can form a greater connectivity and personalization, the individual's information privacy can be threatened by it, thus creating a personalization-privacy trade-off (Sutanto et al. 2013, p. 1141; Xu et al. 2009, p. 136). A perceived violation of privacy can result in negative behaviours and attitudes like boycotts, complaining, negative word of mouth and attempts to punish the firm (Ashworth and Free 2006, p. 118). Furthermore, such a transgression can raise privacy concerns again through the influence of past experience on IPC (Smith, Milberg, and Burke 1996, p. 186). Therefore, we will shed light on the invasion of privacy, the role of information transparency in this personalization-privacy trade-off, and explain the privacy paradox in the following subchapters.

3.2.1. Invasion of an individual's privacy. When is personalization perceived as an invasion of privacy and when does customization become an intrusion? In order to elaborate this issue we will scrutinize the information boundary theory (IBT). This theory is based on the assumption, that the disclosure of private information is associated with a certain risk and vulnerability (Petronio 1991, p. 311). Hence, individuals construct a metaphorical protective boundary, which limits the informational spaces around them (Petronio 1991, p. 311). These information boundaries manage the inflow and outflow of private information from one's self to others and vice versa (Petronio 1991, p. 311). Attempts by external parties like marketers to cross those information boundaries may be perceived as an invasion and cause the individual to feel uncomfortable and uneasy (Solove 2006, p. 553). This crossing is perceived as an actual intrusion if the consumer considers the data collection to be rather harmful than

worthwhile (Petronio 1991, p. 311). Thus, the user undertakes a privacy calculus, in which the costs and benefits of revealing private information are assessed (Dinev and Hart 2006, p. 61). This assessment depends on the riskiness of revealing the information, the absence of control over the information and the lack of worthwhile benefits (Sutanto et al. 2013, p. 1146). For instance, the information about a user's poor health is rather associated with high risk and without control or benefits the information collection is likely perceived as an intrusion (Sutanto et al. 2013, p. 1146). The type and nature of information is therefore decisive in this evaluation.

Consequently, the benefits of customization may be restricted by an individual's information boundaries according to the IBT. Research suggests that personalization can increase process gratification but does not significantly enhance an individual's content gratification, which reflects the user's enjoyment of using the offered content (Sutanto et al. 2013, p. 1143). This is caused by the consumer's worry that the firm may be breaching their personal information boundary, leaving them uncomfortable (Sutanto et al. 2013, p. 1148). The information boundary penetration in turn will raise privacy concerns significantly (Sutanto et al. 2013, p. 1143). Therefore, the trade-off between customization and privacy is evident and needs to be balanced carefully. The IBT also offers means to prevent intrusive information collection, which will be elaborated in the chapter for managerial implications.

3.2.2. Importance of information transparency. Information transparency is the degree to which consumers have access to their personal information collected by a firm and are informed about how the data is going to be utilized (Awad and Krishnan 2006, p. 14). Oulasvirta observes that transparency about the identity, purpose or practice of the data collector can lower a consumer's privacy concerns (2014, p. 637). In his research he found that transparency about a collector's intentions has the greatest impact (Oulasvirta et al. 2014, p. 637). Hence, users will possess a decreased level of privacy concerns if information about the organization's intentions is transparent.

Furthermore, individuals can evaluate features, which enhance information transparency, as more or less essential. According to Awad and Krishnan consumer-rated importance of transparency features can negatively affect their willingness to be profiled online for personalized services and advertising as shown in Figure 3 (2006, p. 24). The eagerness to share personal information for a customized service is, therefore, also influenced by the perceived importance of information transparency. If an individual puts greater weight on information transparency features, which provide knowledge of information collection and usage, he/she will be less likely to be profiled online (Awad and Krishnan 2006, p. 24).

In addition, the information transparency importance is positively affected by a user's privacy concerns and the consumer-rated importance of privacy policies (Awad and Krishnan 2006, p. 24). Significant privacy concerns and policy relevance can strengthen transparency importance, which in turn reduced the consumer's willingness to be profiled online for customized services (Awad and Krishnan 2006, p. 24). Hence, transparency importance and privacy concerns closely interact with readiness to share personal information online and can contribute to the personalization-privacy trade-off.

3.2.3. Privacy paradox. This relationship between privacy concerns and behavioural intentions is noticeable yet biased. The so-called privacy paradox describes the bias between individuals' stated privacy concerns and their actual behaviour, which is often contradicting (Smith, Dinev, and Xu 2011, p. 1000). For example, research discovers that an individual's level of actual information disclosure is often significantly greater than his/her intentions to do so (Norberg, Horne, and Horne 2007, p. 118). One explanation of this privacy paradox is given by economic literature, which suggests that future events may be discounted differently compared to near-term events (Acquisti 2004, p. 2). The gain of personal information disclosure may be immediate to the customer, whereas the risk associated with the information exposure might be either inconspicuous or spread over time (Smith, Dinev, and Xu 2011, p. 1000). This finding indicates that users may state higher privacy concerns than

they actually have, and that the effect of privacy concerns on the utilization of customized devices might be less severe in reality.

Despite this privacy paradox, it is evident that a relationship between personalized features and privacy exist. We exemplified that the data collection for personalized services can be invasive to users and needs to be managed carefully. Nonetheless, information transparency can alleviate privacy concerns in the personalization-privacy trade-off. However, the interconnection between personalization and privacy can be influenced through the role of trust, which we will clarify in the next subchapter.

3.3. The Role Of Trust

Trust as a cognitive concept entails the individuals' expectation from trustees to behave in a certain way when these actions are to some extend uncertain (Lewicki, McAllister, and Bies 1998, p. 439). Trust is characterized by confident positive expectations regarding another's behaviour with hope and assurance at its highest end and hopelessness and uncertainty at its lowest end (Lewicki, McAllister, and Bies 1998, p. 439). In the era of digital customization a subject of trust can be service providers, since consumers may be concerned about a firm's competence, integrity and altruism (Turel, Yuan, and Connelly 2008, p. 125). In this case the user might be uncertain about the organizations' actual utilization of the shared personal data but through the role of trust he/she might hold a specific expectation about the usage. At this point is has to be noted, that we will only focus on the concept of trust in this thesis and neglect the concept of distrust, which inhabits fear and scepticism. Trust and distrust are linked but still separate concepts and don't represent opposite ends of a single scale, meaning that an individual can hold believes of trust and distrust at the same time (Lewicki, McAllister, and Bies 1998, p. 439).

3.3.1. The repercussion of trust on the customer. Establishing trust can have a positive effect on the user's loyalty and purchase intention as well as satisfaction (Grayson, Johnson, and Chen 2008, p. 252; Yim, Tse, and Chan 2008, p. 746). But of far more importance in the

personalization-privacy issue is that trust can facilitate the transfer of sensitive personal data to the organization (Tang, Hu, and Smith 2008, p. 153). As previously stated the sharing of sensitive personal information is associated with risk, but trust can ease the transmission of data between users and firms. Consequently, trust can affect privacy concerns and the willingness to provide personal information.

However, the concrete relationship between trust and privacy remains unclear and is still subject to discussion. While some research suggests trust to be a mediator of privacy concerns and information disclosure, other research views trust to be an antecedent to privacy, an outcome of privacy, or as a moderator of the influence of privacy concerns on a consumer's behaviour (Smith, Dinev, and Xu 2011, p. 1000). Yim, Tse and Chan, for example, identify firm trust as a mediator linking customer satisfaction positively to loyalty, which in turn impacts purchase intention (2008, p. 746). Furthermore, Eastlick shows that even though privacy concerns have a direct negative effect on purchase intention, the greatest impact of privacy concerns on purchase intention is through the mediation effect of trust (2006, p. 884). He implies that the immediate negative repercussion is only temporal, but the mediated impact may be lasting longer since trust is held deeply in a consumer's attitude (Eastlick, Lotz, and Warrington 2006, p. 884). Eastlick concludes that trust exacerbates the negative effect of privacy concerns on purchase intention (2006, p. 884). Because research has uncovered multiple facets and relationships of trust, it becomes apparent that trust has a significant role in the interplay of privacy concerns and information disclosure.

3.3.2. Trust and theories of justice. The relationship of trust and an individual's behaviour has also been analysed in the light of justice theories. As previously illustrated, theories of justice can be seen as an underlying concept of the dimensions to internet privacy concerns. On the one hand, the impact of justice theories on an individual's behavioural intention to use a service has been studied by Turel, who found trust to be a mediating variable in this relationship (2008, p. 140). Judgements about procedural and distributive justice affect trust

in the service and its representatives respectively, and the degree of trust, in turn, forms the intention to use the service (Turel, Yuan, and Connelly 2008, pp. 138–40). These findings suggest that perceived fairness of the allocation of outcomes and the procedure of distribution can both enhance trust in the firm and its representatives, which can be an important managerial implication to enhance a customer's intention to use the firms' services.

Ashworth and Free, on the other hand, have a reversed conceptualization of trust by viewing trust as the moderating variable affecting the justice judgement, and therefore also contributing to privacy concerns (Ashworth and Free 2006, p. 117). According to this study trust can likely alter a consumer's evaluation of the information exchanges' fairness in both distributive and procedural dimensions by affecting the inference of inputs, outputs, and data utilization. Thus, established trust can enhance an individuals' perceived fairness of the exchange and lower the resulting privacy concern. However, heightened trust in an organization may also precipitate the firms' comparison to higher normative standards, which in turn can decay fairness judgements in case of a normative violation (Ashworth and Free 2006, p. 117). Consequently, a violation of a trusted firm may be recognized as more severe than of an unfamiliar company.

The Role of trust has shown to be significant in the privacy issue of customized devices even though a fully agreed upon conceptualization cannot be laid out at this point. Subsequently, our focus will be on the currently employed regulations to protect an individuals' information privacy.

3.4. Regulations To Assure Information Privacy

Governmental laws of privacy vary across countries and deal with the different concepts of privacy. Our concern does not focus on data-security matters or illegal access to personal data, but rather on the collection, retention and secondary usage of personal information. There are two possible basic concepts: the government establishes mandatory standards for all firms or corporations can manage their standards through self-regulation and are only

controlled by the free-market (Ashworth and Free 2006, p. 108). While the U.S. government employs rather the latter mechanism by viewing privacy as a commodity, the EU legislation states privacy as a fundamental right and restricts the transfer of personal information to other countries, which do not offer an equal level of protection (Ashworth and Free 2006, p. 109). The currently employed European Data Protection Directive 95/46/EC has been superseded by the General Data Protection Regulation (EU) 2016/679, which will apply from May 2018 onwards. This new regulation will not only affect citizens of all European member states, but also foreign firms like Facebook and Google, which are targeting EU citizens with their services. All firms will have to comply with new regulations like the right to be forgotten, or restrictions on forwarding data (Official Journal L 119 , 04/05/2016).

Despite country-based differences in legislations, it becomes apparent that the currently employed regulations do not adequately address the recently upwelling privacy concerns of consumers. For example, the institutional practices of collection, retention and secondary usage are legitimate under the current U.S. regulation (Park and Skoric 2017, p. 74). This indicates that the personal data, which is collected by wearable devices, can currently be processed and sold without any impediments in real-time (Park and Skoric 2017, p. 74). Even an individual's health information is not fully protected in the U.S. due to the fact that the Federal Drug Administration (FDA) is restrained when commercial wearables are no longer used strictly for medical purposes (Langley 2015, p. 1642). To address this issue the Electronic Communications Privacy Act of 1986 (ECPA) needs to be updated in order to regulate this information disclosure (Langley 2015, p. 1642). The current regulation through the ECPA might have been appropriate 31 years ago, and thus demonstrates the obsolescence of the present privacy legislation. Current policy is out-dated because it fails to keep up with technical innovations and industry changes (Park and Skoric 2017, p. 71). Due to new technologies and intensified personal data marketing, privacy concerns are deteriorating and clear boundaries are essential (Park and Skoric 2017, p. 72).

However, it is unclear how to balance privacy protection and at the same time allow for ingenious innovations. For example, Google would "be quick to point out that any strict regulations would hinder their efforts toward creative digital innovations" (Park and Skoric 2017, p. 80). Even though privacy is an important value, so too are innovation, entrepreneurship and economic growth (Thierer 2014, p. 3). Firms would naturally favour a self-regulation approach in order to be in control of their own privacy standards and further allow for creative products. Nevertheless, studies suggest that self-regulation is ineffective in the online industry, since U.S. companies did not conform to the voluntary consumer protection through notice and choice in the early years and are unlikely to do so now (Park 2011, p. 658). This self-regulation prevailingly consists of a user notification and an opt-out choice, whereas opting out prevents the consumer from engaging in any digital activities (Park and Skoric 2017, p. 76). This leaves the consumer with no choice but to accept the default setting in order to carry out the same online functions, thus, this cannot be seen as an optimal solution.

Prevailing regulations, whether they are established through the government or self-regulating, do not appeal satisfactorily to the customers. This is a call for change, and therefore we will be dealing with the managerial implications of privacy in the digital era in the following chapter.

4. Discussion

In the following subchapters we will summarize the findings, give respective managerial implications, and demonstrate further areas of research to investigate the role of privacy in the digital era of customization.

4.1. Managerial Implications

It becomes apparent that the current regulation is in need of remodelling in order to adequately address consumers' privacy concerns. Because of the recent rise in privacy

concerns, some individuals are reluctant in accepting new technologies with customization features. This is partly due to firms' opaque practices and intentions of data collection and usage. Trust, however, can play a mitigating role in this privacy-personalization trade-off. There are multiple proposals for firms and the government to gain a user's trust and we will illustrate some of them in the subsequent subchapter. Moreover, the advantages of a customized privacy policy and a regulation proposition will be discussed.

4.1.1. Gaining an individuals' trust. Trust has an indisputable influence on the relationship of privacy and personalized technology even though the concrete interaction remains subject to discussion. Firms as well as the government have ways to affect a customer's level of trust, which thereafter alters their behavioural intentions.

Research provides evidence that organizations can induce trust through a clear and credible privacy policy and through justice judgements. On the one hand, Pan and Zinkhan suggest that a straightforward privacy policy signals customers that they can trust the entity and, moreover, that it serves as a safety net (Pan and Zinkhan 2006, p. 336). This assurance is especially important when users associate the sharing of private information with a high level of risk. If a consumer perceives the information collection to be risky, he/she will pay more attention to a firm's privacy policies (Pan and Zinkhan 2006, p. 336). Consequently, the absence of privacy statements leads to diminishing trust with a higher decrease if the perceived risk is high (Pan and Zinkhan 2006, p. 336). The policy communication becomes more effective if the used language is not too technical or complicated, but rather clear and credible (Pan and Zinkhan 2006, p. 336). However, the wording does not appear to be of significant value since consumers usually do not read the policy statement after all (Pan and Zinkhan 2006, p. 337). Nevertheless, users expect the existence of a privacy policy and perceive it as a trust building component. A straightforward statement is perceived as more comprehensive, but does not significantly enhance trust according to Pan and Zinkhan (2006, p. 332).

Tang, Hu and Smith, on the other hand, found that a firm's ability to send clear and credible signals in general can strengthen trust (2008, p. 153). This can facilitate the transfer of personal information, even when they are associated with a high level of risk (Tang, Hu, and Smith 2008, p. 153). The study also implies that on the downside ambiguous signals can impair believes of trust. But with accurate signals of trustworthiness in handling personal data, a firm can enhance user's trust and stimulate their willingness to provide personal information (Tang, Hu, and Smith 2008, p. 154). A sophisticated privacy policy has the following characteristics: it clearly communicates which type of data is being collected as well as shared, the consequences of sharing and the parameters of aggregated data (Singer and Perry 2015, pp. 24–26). Further research adds that in pursuance of establishing profitable customer relationships, consumers' reactions to a firm's privacy policy need to be considered (Ashworth and Free 2006, p. 118). Accordingly, "firms will be better off providing consumers with concrete, detailed information" about likely consequences and benefits of the information collection (Ashworth and Free 2006, p. 118). This indicates that the negative consequences of not stating a clear privacy policy or none at all outweigh the cost savings.

Furthermore, a firm can alter trust through the influence of justice and fairness judgements as previously analysed by Turel, Yuan and Connelly (2008, p. 143). An organization's ability to employ procedural fairness as well as a fair distribution of outcomes can help gain a user's trust (Turel, Yuan, and Connelly 2008, p. 140). This includes an analysis of equity theory and normative standards in order to evaluate the information exchange. Users will only consider an information exchange as fair if its outcomes are proportional to its inputs and the procedures are in accord with normative standards (Ashworth and Free 2006, pp. 114–17). Ashworth and Free contribute to this finding by adding that "online practices that are considered fair may well build trust and encourage consumers to engage in more online transactions" (2006, p. 118). Therefore, a positive

development in tangible outcomes and procedural fairness judgements can gain a customer's trust.

If firms, however, fail to establish a trusted relationship in which customers' privacy concerns are adequately addressed, consumers may call for governmental actions through mandatory standards (Smith, Dinev, and Xu 2011, p. 1000). By enacting strict privacy protection standards for all firms across different industries, the government assures a certain degree of privacy protection since firms get fined for illegal behaviour (Tang, Hu, and Smith 2008, p. 155). With sufficient standards and monitoring the government can help establish trust and ease the transfer of personal data from a consumer to the firm as privacy protection is guaranteed. In spite of its effectiveness, Tang, Hu and Smith argue that mandatory standards are not necessarily the most efficient way to ensure privacy preservation (2008, p. 156). Although consumers may benefit from a uniformly increased protection in privacy matters, firms may experience higher costs, which they in turn can pass on to their customers in form of higher prices (Tang, Hu, and Smith 2008, p. 170). Consequently, this regime can lead to an unfavourable social welfare loss, and thus is not considered as socially optimal (Tang, Hu, and Smith 2008, p. 170).

In summary, an individual's perception of trust can be influenced by firms through clear privacy policies and fairness judgements as well as by the government through mandatory standards, with the latter not being socially optimal in all environments.

4.1.2. Customized Privacy. Until now we mainly focused on the consumer perspective of privacy policies and how they can decrease privacy concerns. According to the social contract approach – a way to view privacy – an agreement is meant to be beneficial to both parties (Martin 2016, p. 551). Therefore, we will illustrate the firm's benefits of employing adequate privacy policies in an economic perspective.

Just like the consumer, firms undertake a privacy calculus, in which they assess the costs and benefits related to privacy protection (Dinev and Hart 2006, p. 62; Lee, Ahn, and

Bang 2011, p. 424). On the one hand, the establishment of an adequate privacy protection for all customers is undoubtedly associated with costs (Zhou and Piramuthu 2015, p. 20). These costs include among others spending on IT, staff, training, policies, auditing. The benefit of an appropriate privacy policy, on the other hand, comprises the basis for a competitive advantage (Ashworth and Free 2006, p. 108). In order to illustrate this matter Lee, Ahn, and Bang divided consumers into three groups: while the privacy unconcerned users willingly share personal information, the privacy pragmatists only do so if their privacy is protected, and privacy fundamentalists never disclose personal data (Lee, Ahn, and Bang 2011, p. 425). According to this study "privacy protection can work as a competition-mitigating mechanism in personalization" (Lee, Ahn, and Bang 2011, p. 425). This implies that privacy protection can expand the group of users sharing information with a firm by also including privacy pragmatists. A larger targeted segment of consumers along with charging higher prices enables the firm to extract substantial profits and embodies the benefit of privacy policies for firms (Lee, Ahn, and Bang 2011, p. 426). Since consumers become more concerned about privacy, there can be a shift in the consumer distribution resulting in fewer unconcerned users and an increase in either privacy pragmatists or fundamentalists or both (Lee, Ahn, and Bang 2011, p. 436). This makes the implantation of an adequate privacy policy even more beneficial for firms.

However, Zhou and Piramuthu argue that this privacy protection should be on a customizable basis, allowing consumers to choose their preferred privacy settings (2015, p. 20). The previously illustrated heterogeneity of consumers results in individuals with different demands for privacy depending on the context. Zhou and Piramuthu propose that each of these needs can be satisfied at an appropriate cost, including an underlying base of protection for all users (2015, p. 26). By means of this differentiation approach unconcerned consumers don't have to bear the costs of more concerned users, while the latter can enjoy a higher level of protection (Zhou and Piramuthu 2015, p. 20). Differentiation can be horizontal through

quality adjustments or vertical through different functions (Zhou and Piramuthu 2015, p. 26). A customization of privacy encourages users who might have been overly concerned before to use the firm's service. This leads to an enhanced social welfare along with the possibility of a firm's profit improvement (Zhou and Piramuthu 2015, p. 29).

Therefore, not only users but also companies can benefit from an appropriate privacy protection policy. This finding implicates the desire for an applicable regulatory solution, which allows both parties to profit from. Hence, we introduce more suited regulation propositions in the next subchapter.

4.1.3. Regulation Propositions. The Federal Trade Commission (FTC) has established a self-regulation regime in the U.S.A. in 1996 and has retained this non-intervention approach unrevised ever since (Park and Skoric 2017, p. 76). As previously stated a self-regulation approach is preferable to mandatory standards in terms of social welfare. However, research suggests the ineffectiveness of the non-intervention approach in the online sector and demands change (Park 2011, p. 658). The hands-off approach through notice and opt-out choice does not appropriately address the concerns associated with wearable technologies and is out-dated (Langley 2015, p. 1643). An improvement would be the utilization of an optional opt-in model instead, where the advantages of opting-in are clearly stated (Park and Skoric 2017, p. 77). This feature allows users to actively exercise data control by adjusting the access as well as retention of data and eliminates the default opt-in (Park and Skoric 2017, p. 81). In order to animate consumers to actually opt-in and allow for data collection, research proposes a compensation for opting-in rather than charging users, who don't give their consent (Park and Skoric 2017, p. 78; Xu et al. 2009, p. 136). The latter could be perceived as pressuring the consumer to give away their personal information, thus, a compensation approach is preferable. This is coherent with the IBT, in which compensations can keep consumers from perceiving information collection as an invasion as long as they embody worthwhile benefits (Sutanto et al. 2013, p. 1146). Another possibility to prevent privacy intrusion is Sutanto's

proposed personalized, privacy-safe application which retains the personal data locally on the smart device (Sutanto et al. 2013, p. 1141). This would still allow the user to participate in the benefits of personalization without the concern of a privacy intrusion, since the consumer is still in control and has access to the collected information (Sutanto et al. 2013, p. 1142).

Underlying to this new regulation model is the need to educate the consumer. Users are usually not equipped with the technical knowledge to protect their information privacy by themselves, some are not even aware that their privacy is threatened (Park and Skoric 2017, p. 77). This poor knowledge about information flows may deteriorate due to the introduction of innovative devices like wearables and with the collection of health and fitness data the urgency to educate the consumer increases (Park and Skoric 2017, p. 77). An education campaign in pursuit of enhancing relevant digital skills can empower users to make informed decisions about the flow of their personal information (Ashworth and Free 2006, p. 120). This consumer empowerment is, according to Ashworth and Free, preferable to limiting a marketer's activities to collect personal data (2006, p. 120). Privacy is indeed an important value, but so too are innovation and economic growth (Thierer 2014, p. 3). A bottom-up approach can cope with privacy concerns without suffocating technological innovations (Thierer 2014, p. 4).

Therefore, we propose that educating consumers along with providing them with the technical feasibility to alter the data flow through opting-in/out and equipping them with adequate control, will reduce privacy concerns without discouraging a firms' innovativeness.

4.2. Future Research

This thesis contains a literature review on the basis of the latest publications, but also reveals fields of further studies subsequently. Until now research has failed to develop a conceptualization of trust, which is mostly agreed upon, therefore we firstly call for investigations in this area of studies. The many facets and interrelations of trust with other concepts make it hard to establish consistent findings. A uniform treatment of trust would

facilitate comparable findings and corresponding advancements. Since privacy issues play an intensifying role in information technologies, a universal conceptualization of trust in this context will benefit research. Secondly, the proposed regulation with an opt-in approach and a consumer education campaign deserves further research. A validation of its effectiveness and guidelines for its implementation could have essential managerial implications for all firms utilizing personalization features. Lastly, the illustrated privacy paradox calls for a higher investigation of actual consumer behaviour. The bias between behavioural intentions and actual behaviour in privacy-related settings has to be taken into account when examining the utilization of personalized innovations. Therefore, studies should rather focus on actual consumer behaviour in order to make well-founded suggestions on how to overcome the personalization-privacy trade-off. With the analysis of these research questions we can gain a better understanding of privacy in the digital era and draw relevant conclusions for managerial implications.

5. Conclusion

In summary, new technological advancements in the digital era are not only associated with numerous benefits including convenience, but are also posing a threat to the users' privacy. A personalized service requires the collection of personal data, which does not always agree with an individual's information boundaries and, hence, can be perceived as intrusive. The resulting privacy concern comprises the concerns about awareness, control, collection, secondary usage, errors, and improper access. Distributive and procedural justice are underlying explanations for a consumer's privacy concerns and call for a fair information exchange. These privacy concerns can hinder individuals to utilize customized services and create a personalization-privacy trade-off. Trust, however, can play a mitigating role in this issue and facilitate the transfer of personal information from users to organizations. Therefore, a firms' main objective in this matter should be to employ trust-building practices like clear

and credible privacy policies along with transparency. Since privacy concerns are consumer-heterogeneous, a customized privacy policy seems to be most promising. Our proposed regulatory approach includes an opt-in model along with a customer education to ensure that users can make informed decisions about their privacy.

All in all, the significant role of privacy in the era of digital customization is indisputable and deserves further investigation. The introduction of new technologies can fail due to the psychological impact of privacy concerns on costumers, which results in an extensive loss for firms. Additionally, through the customers' growing familiarity with technological devices, privacy issues demand an increasing attention. As a conclusion, privacy concerns do exist in this digital era of customization and are in need of proper management.

Appendix

Figure 1: Conceptualization of Internet Privacy Concern (IPC).

Source: Hong, Thong 2013

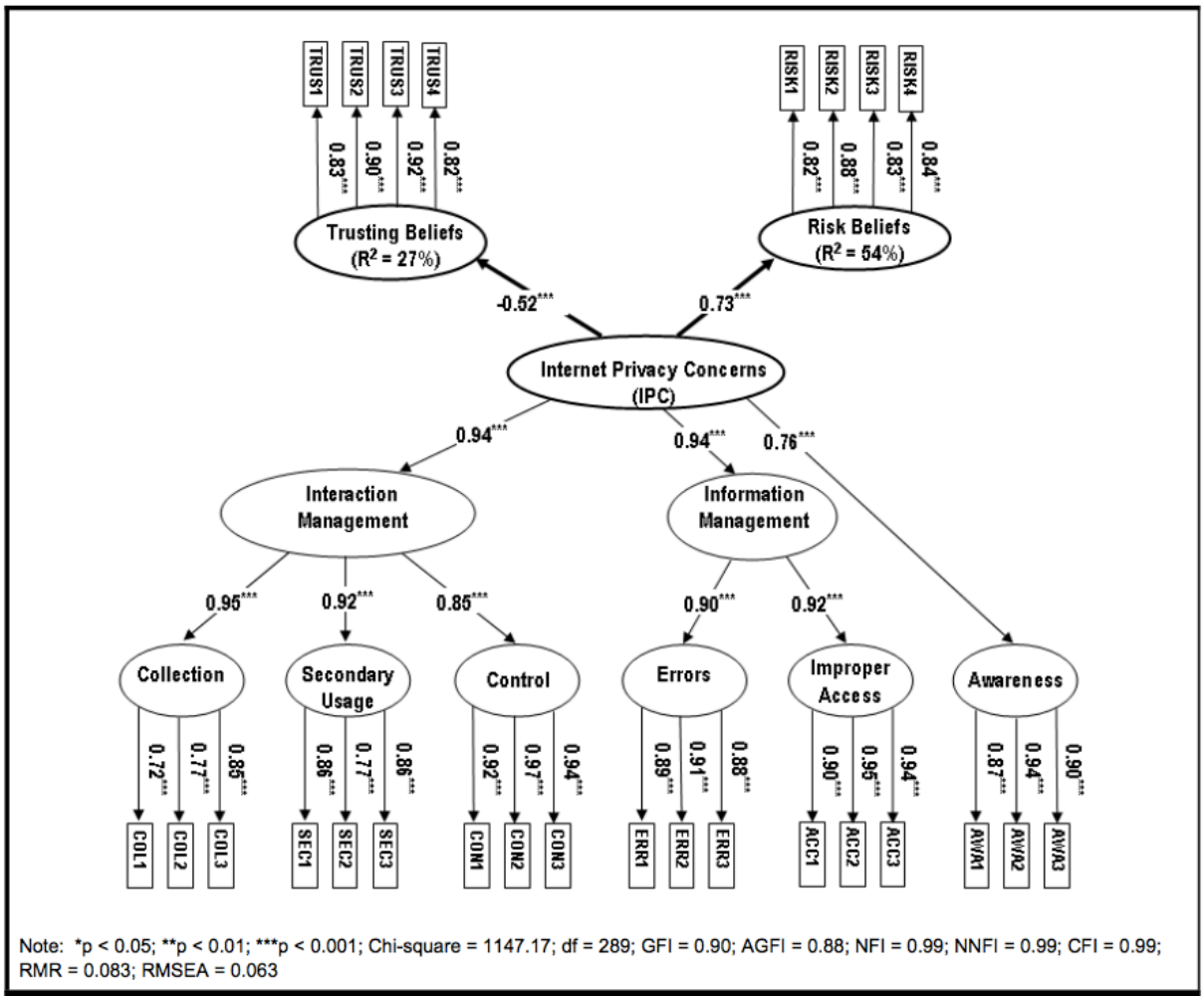


Figure 2: Information exchange model with outcome and input of consumer and firm.

Source: Ashworth, Free 2006

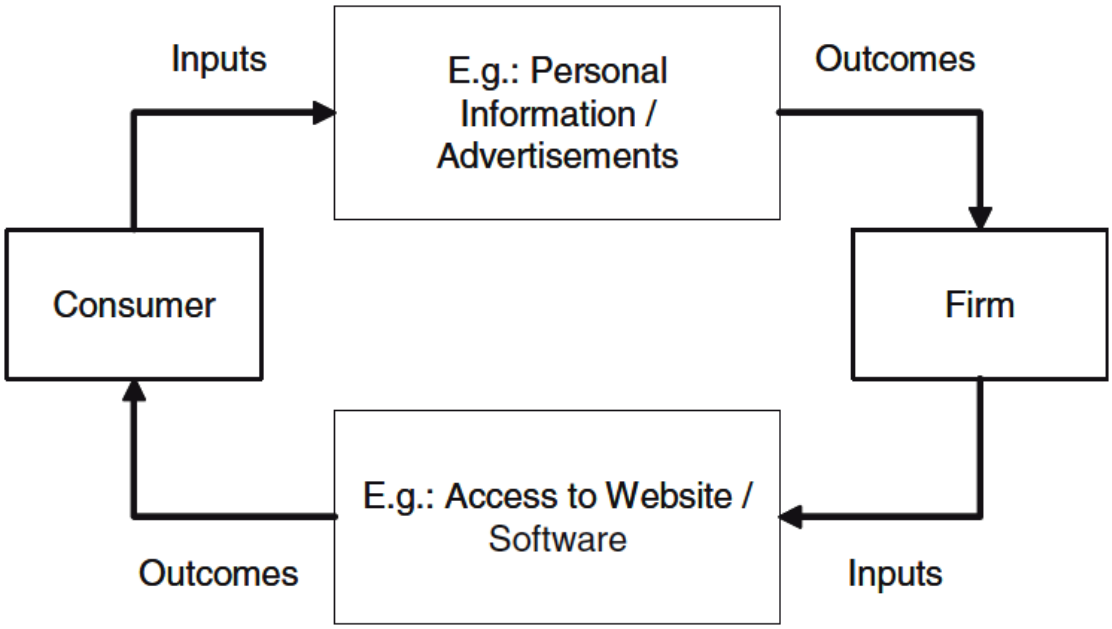
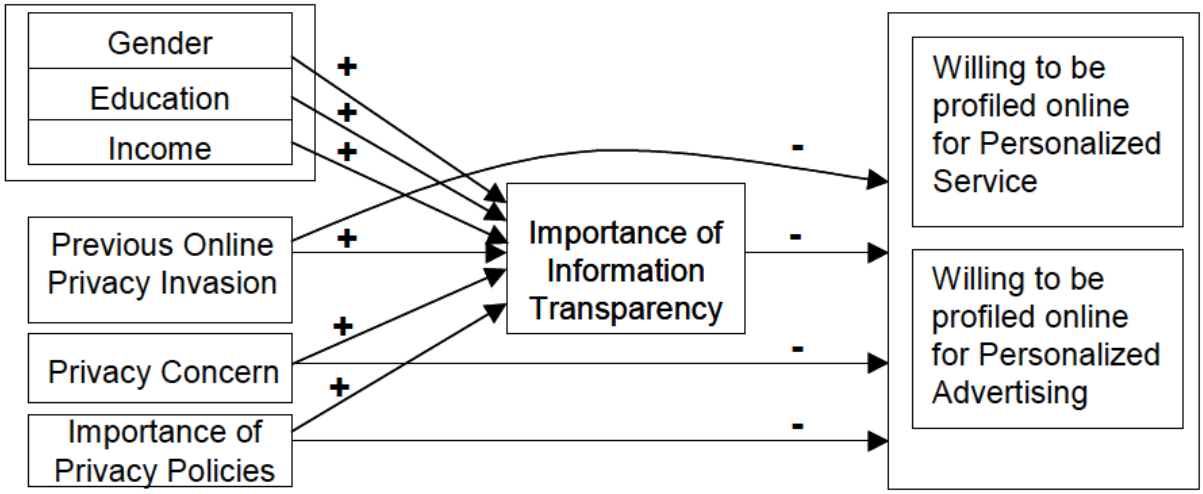


Figure 3: Framework of a consumer's perceived importance of information transparency.

Source: Awad, Krishnan 2006



References

Acquisti, Alessandro (2004), "Privacy in electronic commerce and the economics of immediate gratification," *ACM Press, 21*.

Ashworth, Laurence and Clinton Free (2006), "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns," *Journal of Business Ethics*, 67 (2), 107–23.

Awad, Naveen Farag and M. S. Krishnan (2006), "The Personalization Privacy Paradox: An Empirical Evaluation Of Information Transparency And The Willingness To Be Profiled Online For Personalization," *MIS Quarterly*, 30 (1), 13–28.

Clarke, Roger (1999), "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, 42 (2), 60–67.

Dinev, Tamara and Paul Hart (2006), "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, 17 (1), 61–80.

Eastlick, Mary Ann, Sherry L. Lotz, and Patricia Warrington (2006), "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," *Journal of Business Research*, 59 (8), 877–86.

Grayson, Kent, Devon Johnson, and Der-Fa Robert Chen (2008), "Is Firm Trust Essential in a Trusted Environment? How Trust in the Business Context Influences Customers," *Journal of Marketing Research*, 45 (2), 241–56.

Ho, Shuk Ying and David Bodoff (2014), "The Effects Of Web Personalization On User Attitude And Behavior: An Integration Of The Elaboration Likelihood Model And Consumer Search Theory," *MIS Quarterly*, 38 (2), 497-A10.

Hong, Weiyin and James Y. Thong (2013), "Internet Privacy Concerns: An Integrated Conceptualization And Four Empirical Studies," *MIS Quarterly*, 37 (1), 275–98.

——— and George M. Zinkhan (1995), "Self-concept and advertising effectiveness: The

influence of congruency, conspicuousness, and response mode," *Psychology and Marketing*, 12 (1), 53–77.

Langley, Matthew (2015), "Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables," *Georgetown Law Journal*, 103 (6), 1641–59.

Lee, Dong-Joo, Jae-Hyeon Ahn, and Youngsok Bang (2011), "Managing Consumer Privacy Concerns In Personalization: A Strategic Analysis Of Privacy Protection," *MIS Quarterly*, 35 (2), 423-A8.

Leventhal, Gerald S. (1980), "What Should Be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships."

Lewicki, Roy J., Daniel J. McAllister, and Robert J. Bies (1998), "Trust And Distrust: New Relationships And Realities," *Academy of Management Review*, 23 (3), 438–58.

Lowry, Paul B., Jinwei Cao, and Andrea Everard (2011), "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *Journal of Management Information Systems*, 27 (4), 163–200.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, 15 (4), 336–55.

Martin, Kirsten E. (2012), "Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract," *Journal of Business Ethics*, 111 (4), 519–39.

——— (2016), "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics*, 137 (3), 551–69.

Miller, Dale T. (2001), "Disrespect And The Experience Of Injustice," *Annual Review of Psychology*, 52 (1), 527.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer*

Affairs, 41 (1), 100–126.

Official Journal L 119 (04/05/2016), "General Data Protection Regulation (EU) 2016/679," (accessed May 28, 2017); [available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC].

Oulasvirta, Antti, Tiia Suomalainen, Juho Hamari, Airi Lampinen, and Kristiina Karvonen (2014), "Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance," *Cyberpsychology, Behavior, and Social Networking*, 17 (10), 633–38.

Pan, Yue and George M. Zinkhan (2006), "Exploring the impact of online privacy disclosures on consumer trust," *Journal of Retailing*, 82 (4), 331–38.

Park, Yong Jin (2011), "Provision of Internet privacy and market conditions: An empirical analysis," *Telecommunications Policy*, 35 (7), 650–62.

——— and Marko Skoric (2017), "Personalized Ad in Your Google Glass? Wearable Technology, Hands-Off Data Collection, and New Policy Imperative," *Journal of Business Ethics*, 142 (1), 71–82.

Petronio, Sandra (1991), "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples," *Communication Theory*, 1 (4), 311–35.

Sheehan, Kim B. (1999), "An Investigation Of Gender Differences In On-Line Privacy Concerns And Resultant Behaviors," *Journal of Interactive Marketing (John Wiley & Sons)*, 13 (4), 24–38.

Singer, Randi W. and Adrian J. Perry (2015), "Wearables: The Well-Dressed Privacy Policy," *Intellectual Property & Technology Law Journal*, 27 (7), 24–27.

Smith, H. Jeff, Tamara Dinev, and Heng Xu (2011), "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, 35 (4), 980-A27.

———, Sandra J. Milberg, and Sandra J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, 20 (2), 167–

96.

Solove, Daniel J. (2006), "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 154 (3), 477.

Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang (2013), "Addressing The Personalization-Privacy Paradox: An Empirical Assessment From A Field Experiment On Smartphone Users," *MIS Quarterly*, 37 (4), 1141-A5.

Tam, Kar Yan and Shuk Ying Ho (2006), "Understanding The Impact Of Web Personalization On User Information Processing And Decision Outcomes," *MIS Quarterly*, 30 (4), 865–90.

Tang, Zhulei, Yu (Jeffrey) Hu, and Miichael D. Smith (2008), "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems*, 24 (4), 153–73.

The Economist (2016), "International data flows: Priceless", (accessed May 28, 2017), [available at http://www.economist.com/news/finance-and-economics/21700700-trade-data-seems-very-important-there-are-no-good-er-data-it-priceless].

Thierer, Adam D. (2014), "The Internet of Things And Wearable Technology: Addressing Privacy And Security Concerns Without Derailing Innovation," *Richmond Journal of Law & Technology*, 21 (2), 1–118.

Turel, Ofir, Yufei Yuan, and Catherine E. Connelly (2008), "In Justice We Trust: Predicting User Acceptance of E-Customer Services," *Journal of Management Information Systems*, 24 (4), 123–51.

Xu, Heng, Hock-Hai Teo, Bernard C. Y. Tan, and Ritu Agarwal (2009), "The Role of Push--Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems*, 26 (3), 135–73.

Yim, Chi Kin (Bennett), David K Tse, and Kimmy Wa Chan (2008), "Strengthening Customer Loyalty Through Intimacy and Passion: Roles of Customer–Firm Affection

and Customer–Staff Relationships in Services," *Journal of Marketing Research*, 45 (6), 741–56.

Zhou, Wei and Selwyn Piramuthu (2015), "Information Relevance Model of Customized Privacy for IoT," *Journal of Business Ethics*, 131 (1), 19–30.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Acquisti, Alessandro (2004) [*ACM Press*]	Lessons from the research on behavioural economics are applied to understand the individual decision making process with respect to privacy in electronic commerce.	Privacy Paradox, Immediate Gratification	Economic equations of a rational agent are used to theoretically predict a rational behaviour and then compared with available data.	• Rational privacy behaviour is unrealistic. • Individuals who genuinely would like to protect their privacy may not do so because of psychological distortions. • These distortions may affect not only naive individuals but also sophisticated ones. • These inconsistencies may occur when individuals perceive the risks from not protecting their privacy as significant.
Ashworth, Laurence and Clinton Free (2006), [*Journal of Business Ethics*]	• Theories of justice are used to help understand the way consumers conceive of, and react to, privacy concerns. • A number of prescriptions, aimed at both firms and regulators are made.	Theories of distributive and procedural justice	Qualitative, theoretical analysis of privacy as an information exchange.	• It is argued that an important component of consumers' privacy concerns relates to fairness judgments, which in turn comprise of the two primary components of distributive and procedural justice. • Consumers will also attend to the firm's outcomes (and both of their inputs) as well as the manner in which the information was collected.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Awad, Naveen Farag and M. S. Krishnan (2006) [*MIS Quarterly*]	Examination of the relationship between information technology features, specifically information transparency features, and consumer willingness to share information for online personalization	Information transparency	• Online survey with n=400 participants from the Digital Research, Inc. (DRI) Family Panel. • Hypothesis testing was conducted using a covariance fitting approach for estimating structural equation models (SEM). • Polychoric correlations were estimated between the dichotomous item Previous privacy invasion and all other items.	• Consumers who value information transparency are also less likely to participate in personalization. • In order to manage this dilemma, it is suggested that firms adopt a strategy of providing features that address the needs of consumers who are more willing to partake in personalization.
Clarke, Roger (1999) [*Communications of the ACM*]	Public confidence in matters of online privacy seemingly lessens as the Internet grows. Indeed, there is mounting evidence the necessary remedy may be a protective framework that includes (gulp) legislative provisions.	Information privacy	Qualitative, theoretical analysis	• Privacy has always been about trade-offs, and infotmation law will involve the formalization of balancing processes between ownership and access, and between freedoms to know, to publish, and to express on the one hand, and freedoms to be, to hide, and to deny on the othet. • Trust must be earned, and intrusion-permissive and intrusionenabling arrangements preclude trust.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Dinev, Tamara and Paul Hart (2006) [*Information Systems Research*]	• Attempting to better understand the predictors of a user withholding or surrendering personal information when using the Internet. • Develop and empirically test an extended model of the privacy calculus in which a set of contrary beliefs was hypothesized to affect individuals' willingness to provide personal information to complete transactions on the Internet.	Privacy calculus of individuals	• 1. Pilot Test with n=70 business students in a southeastern university • 2.Pilot Test with n=70 business students in a southeastern university due to substantial changes • Final survey with n=369 individuals in the southeastern United States. • Model testing using structural equations modeling (SEM) with LISREL.	• A higher level of perceived Internet privacy risk is related to a higher level of Internet privacy concerns and a lower level of willingness to provide personal information. • A higher level of Internet trust is related to a higher level of willingness to provide personal information.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Eastlick, Mary Ann, Sherry L. Lotz, and Patricia Warrington (2006) [*Journal of Business Research*]	• Investigate whether a traditional business-to-business relationship marketing framework could be applied to the information-intensive online business-to-consumer channel. • Effects of opt-in versus opt-out choice strategies on consumers' privacy concerns and trust were also studied.	Framework from information privacy and relationship marketing	• Focus group of n=10 male and female to develop the questionnaire. • Pretest with n=63 students • Written questionnaire with n=477 U.S. households who are identified as primary shoppers for computer and electronic products. • Drawings to win $75 were provided as incentives for participation.	• Results showed that the strongest relationships leading to online purchase intent were those between trust in and commitment toward an e-tailer and between firm reputation and trust. • Privacy concerns influenced purchase intent with strong negative effects, both directly and indirectly through trust. • Privacy concerns has its greatest impact on purchasing intent through its relationship with trust.
Grayson, Kent, Devon Johnson, and Der-Fa Robert Chen (2008) [*Journal of Marketing Research*]	Test of two rival sociological perspectives regarding the influence of customer trust in the broader context: • Trust in the context replaces trust in individual firms and their representatives. • Or trust in the context fosters and legitimates trust in firms and their representatives	Narrow-scope and broad-scope trust	• 1. Survey with n=586 customers who purchased a pension from an independent financial adviser in the United Kingdom. • 2. Survey with n=261 individuals in Taiwan to address limitations of study 1 and minimize cultural reasons for the results	• Both studies support the proposition that trust in firms and their representatives is a necessary mediator of trust in the broader context.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Ho, Shuk Ying and David Bodoff (2014) [*MIS Quarterly*]	Provide a model of attitude formation toward a personalization agent and how attitudes relate to the two behaviours item sampling and item selection.	The elaboration likelihood model (ELM) and consumer search theory (CST)	• Pilot test with n=12 participants • 1. Lab study: A personalized online bookstore (Amazon's interfaces) was visited by n=379 undergraduate students to select books for their study and report their thoughts on sampled books (thought-listing technique) for 2 weeks. • 2. Field study: A personalized music website was visited by n=205 to view music track details, listen to track previews, and download tracks for 6 months.	• For online merchants, this research highlights the trade-off between item sampling and item selection. • Personalization could offer a basis for generating revenue because users are generally willing to sample and select personalized items as their final choice, but the amount of personalized sampling diminishes with attitude confidence, while selection of a personalized item depends on it.
Hong, Weiyin and James Y. Thong (2013) [*MIS Quarterly*]	Conceptualization of internet privacy concerns (IPC) in terms of its key dimensions and its factor structure	Multidimensional development al theory	• Review of the prior literature. • 1. Online survey with n=968 participants • 2. Online survey with n=961 participants • 3. Online survey with n=992 participants • 4. Online survey with n=887 participants	• Third-order conceptualizations of IPC: two second-order factors of interaction management and information management, and six first-order factors (collection, secondary usage, errors, improper access, control, and awareness).

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Hong, Weiyin and George M. Zinkhan (1995) [*Psychology and Marketing*]	Would advertising appeals congruent with viewers' self-concept be superior to incongruent appeals in terms of enhancing advertising effectiveness?	Self-Concept and Advertising Effectiveness (brand memory, brand attitude, and purchase intentions)	• The sample consisted of n=165 subjects who were exposed to four test stimuli (ads), two for automobiles and two for shampoos. • One ad within a product class used an introvert appeal, and the other used an extrovert appeal.	• The study results indicate that brand memory is not mediated by the extent to which advertising expressions are congruent with viewers' self-concept. • However, brand preference and purchase intention were shown to be influenced by the self-congruency of an ad.
Langley, Matthew (2015) [*Georgetown Law Journal*]	Analyzing the currently employed regulations on health information in the U.S.A of and the possibility that firms can sell this sensitive information collected by wearable devices.	U.S. Privacy Regulation	Qualitative, theoretical analysis of the U.S. privacy regulation on health information.	• Old laws must adapt to modern times in the same way that old methods of communication evolved with technology. • A loophole in section 2702(c)(6) of the SCA allows health apps to freely disclose its customers' sensitive health information. • Until congressional intervention occurs, consumer wearables will continue to provide the platform for companies to, quite literally, profit from our heartbeats.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Lee, Dong-Joo, Jae-Hyeon Ahn, and Youngsok Bang (2011) [*MIS Quarterly*]	Explore the motivation of firms for privacy protection and its impact on competition and social welfare in the context of product and price personalization.	Game-theory, personalization–privacy tradeoff	Game theory stages of decision making: • Stage 1: Privacy protection decision by firms. • Stage 2: Pricing of standard products by firms. • Stage 3: Pricing of personalized products by firms. • Consumer Choice: Product choice by consumers. • Analysis of the game by backward induction	• We find that privacy protection can work as a competition-mitigating mechanism by generating asymmetry in the consumer segments to which firms offer personalization, enhancing the profit extraction abilities of the firms. • Further, as consumers become more concerned about their privacy, it is more likely that all firms adopt privacy protection. • That autonomous choices of privacy protection by personalizing firms can improve social welfare at the expense of consumer welfare. • That regulation enforcing the implementation of fair information practices can be efficient from the social welfare perspective mainly by limiting the incentives of the firms.
Leventhal, Gerald S. (1980) [*Wayne State University*]	To distinguish procedural justice from the predominant distributive justice judgements.	Justice theories, Equity theory	Qualitative, theoretical analysis of distributive and procedural fairness and equity theory.	• Distribution rules follow certain criteria: the individual's contributions, his needs, and the equality theory. • A procedural justice judgment sequence estimates the individual's deservingness based on each rule.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Lewicki, Roy J., Daniel J. McAllister, and Robert J. Bies (1998) [*Academy of Management Review*]	• Development of a new theoretical framework for understanding simultaneous trust and distrust within relationships. • Exploration of the theoretical and practical significance of the framework for future work on trust and distrust relationships within organizations.	Trust and Distrust frameworks	Qualitative, theoretical analysis of trust and distrust concepts and scales.	• Trust and distrust are separate but linked dimensions and not opposite ends of a single continuum. • An individual can simultaneously hold believes of trust and distrust. • Trust are confident positive expectations regarding another's conduct, and distrust are confident negative expectations regarding another's conduct.
Lowry, Paul B., Jinwei Cao, and Andrea Everard (2011)	• Examine the relationships between self-disclosure technology use and culture. • Exploration of the effects of culture on information privacy concerns and the desire for online interpersonal awareness, which influence attitudes toward, intention to use, and actual use of self-disclosure technologies.	Social exchange theory	• Study with n=35 senior-level and master's-level IS students. • Online survey with n=486 Undergraduate college students in China (284) and the United States (202). • A drawing for $100 in cash was offered as an incentive.	• Cross-cultural dimensions are significant predictors of information privacy concerns and desire for online awareness, which are, in turn, found to be predictors of attitude toward, intention to use, and actual use of instant messaging. • Uncertainty avoidance and collectivism increased information privacy concerns, power distance decreased information privacy concerns, and uncertainty avoidance and collectivism positively increased desire for online awareness. • Information privacy concerns were higher for women.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004) [*Information Systems Research*]	Develop a theoretical framework on the dimensionality of Internet users' information privacy concerns (IUIPC) and test a causal model on the relationship between IUIPC and behavioral intention toward releasing personal information at the request of a marketer.	Social contract theory, Justice theories	• Review of previous literature. • 1. Field survey: Personal interview with n=293 households. • 2. Field survey: Personal one-on-one, face-to-face interview with n=449 households	A second-order IUIPC model has been established, which consists of three first-order dimensions—namely, collection, control, and awareness.
Martin, Kirsten E. (2012) [*Journal of Business Ethics*]	Validation of a social contract approach to privacy by examining whether and how privacy norms vary across communities and contractors.	Social contract, privacy norms	• Theoretical examination through the use of the factorial vignette survey technique. • Online survey with n=831 both students and non-students as participants. Respondents were asked to judge the named protagonist in the story who shared information with others. • The rating task was an ordinal scale, with the dependent variable ranging from 0 (Expected to Share information) to 4 (Wrong to Share Information)	• Insiders to a community had significantly different understandings of privacy norms as compared to outsiders, and outsiders have difficulty in understanding the privacy norms of a particular community. • Individuals hold different privacy norms without necessarily having diminished expectations of privacy, thereby suggesting privacy norms are contextually understood within a particular community of individuals.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Martin, Kirsten E. (2016) [*Journal of Business Ethics*]	• Examine how privacy norms develop through social contract's narrative. • Describe privacy violations given the social contract approach. • Critically examine the role of business as a contractor in developing privacy norms.	Social contract approach to privacy	Review of previous literature and qualitative, theoretical analysis of a social contract approach to privacy.	• Rather than giving away privacy, individuals discriminately share information within a particular community and with norms governing the use of their information. • Shift of the responsibility of firms from adequate notification to the responsibility of firms as contractors to maintain a mutually beneficial and sustainable solution.
Miller, Dale T. (2001) [*Annual Review of Psychology*]	Examining what role the perception of disrespect plays in the experience of injustice. The focus is primarily on the links between disrespect and anger, disrespect and injustice, and anger and injustice	Psychology of injustice, respect and anger	Review of previous literature.	Links between disrespect and anger, disrespect and injustice, and anger and injustice are outlaid. Relations to injustice are illustrated.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007) [*Journal of Consumer Affairs*]	Exploration of the ‘‘privacy paradox’’ or the relationship between individuals’ intentions to disclose personal information and their actual personal information disclosure behaviors.	Privacy Paradox	• Two prestests with n=43 and n=83 graduate students. • Two studies: Individuals were asked their willingness to disclose specific pieces of information in Phase 1 of each study and then several weeks later were asked to actually provide the same specific pieces of information to a market researcher in Phase 2. • 1. Study with n=23 graduate students at a university in the Northeast • 2. Study with n=68 graduate students	• The willingness to disclose was significantly different from actual disclosure. • Risk is salient when asking for behavioural intention responses but is less so in actual disclosure situations.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Oulasvirta, Antti, Tiia Suomalainen, Juho Hamari, Airi Lampinen, and Kristiina Karvonen (2014) [*Cyberpsychology, Behavior, and Social Networking*]	Understand how data disclosure practices in ubiquitous surveillance affect users' privacy concerns.	Privacy concerns, transparency	• Online questionnaire with n=1.897 Finnish-speaking respondents. • Five respondents were randomly chosen and awarded with a 20€ price.	• Privacy concerns were found to differ across the scenarios and were moderated by knowledge about the collector's identity and intentions. • Knowledge about intentions exhibited a stronger effect. • When no information about intentions was disclosed, the respondents postulated negative intentions. • A positive effect was found for disclosing neutral intentions of an organization or unknown data collector, but not for a private data collector
Pan, Yue and George M. Zinkhan (2006) [*Journal of Retailing*]	• To explore the impact of privacy disclosures on online shoppers' trust in an e-tailer. • To test whether the presence of an online privacy policy influences consumer trust. • Examination of the effects of different forms of privacy disclosures.	Privacy disclosure and trust	• Pretest: Survey with n=70 business students about a hypothetical e-sore. • 1. Study with a 2 (absence vs. presence of a privacy policy)×2 (high vs. low privacy risk) between-subjects factorial design and n=60 participants. • 2. Study between-subjects factor with three levels: Absence of a privacy policy and two presence of a privacy policy levels (long and legalistic vs. short and	• Consumers are likely to respond more favourably to a shopping site with a clearly stated privacy message. • Especially when privacy risks are high. • Online shoppers find a short, straightforward privacy statement more comprehensible than a lengthy, legalistic one. • However, how a privacy policy is presented (in terms of wording) does not affect a shopper's trust in the store to any significant degree.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
			straightforward) and n=90 participants.	
Park, Yong Jin (2011) [*Telecommunications Policy*]	Analysis of the relationship between the provision of Internet privacy protection and market conditions.	Internet privacy, market conditions	n=398 heavily trafficked and randomly selected U.S. commercial sites were examined as to their level of privacy protection, as indicated by interface features of Notice and Choice	• Limited supply of Notice and Choice functionalities by most websites, far short of the industry's standard of conduct. • The domain and website attributes, indicative of market conditions, had minimal impact on the likelihood of high privacy provision. • Indication of the need for a new set of interface-focused policy proposals in domain-context specific regulations.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Park, Yong Jin and Marko Skoric (2017) [*Journal of Business Ethics*]	Examining the disjuncture between institutional and policy forces in harnessing dual market mechanism, which frames how the new communication industry operates in the marketplace of ubiquitous personal advertising. Exemplified with Google Glass.	Privacy regulations, user competence	Review of previous literature. Google business practices are examined, currently employed U.S. regulations are analysed along with antitrust regulations and user competence.	Four policy propositions: • First, vertical integrations within and across new media firms need serious attention from the FTC in order to break the concentration of personal data in digital databases. • Second, the user interface in Google Glass and wearable devices should be mandated to contain a function that restricts third-party data access and retention of personal records. • Third, there should be a long-term state and local public education campaign for promoting relevant digital skills. • Finally, at least in the U.S., Congress should empower the FTC to enact and enforce an updated opt-in model regarding the use of mobile-based wearable platforms.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Petronio, Sandra (1991) [*Communication Theory*]	Understand the way individuals regulate disclosure of private information. The focus is on the way marital couples manage talk about private matters with each other.	Communication boundary management	Review of previous literature and qualitative, theoretical analysis of the information boundary theory (IBT).	• Couples manage their communication boundaries in balancing a need for disclosure with the need for privacy. • Revealing private information is risky because there is a potential vulnerability when revealing aspects of the self. • Receiving private information from another may also result in the need for protecting oneself. • In order to manage both, individuals erect a metaphoric boundary to reduce the possibility of losing face and as a means of protection. • Also, people use a set of rules or criteria to control the boundary and regulate the flow of private information to and from others.
Sheehan, Kim B. (1999) [*Journal of Interactive Marketing*]	Examination whether gender differences are apparent in attitudes and behaviours toward advertising and marketing practices involving information gathering and privacy on-line.	Communication patterns of men and women	Two pretests with n=350 participants. Electronic mail survey with n=889 U.S. participants	• Women and men differed significantly in their attitudes toward several practices, with women generally appearing more concerned about the effect the practice would have on their personal privacy. • Men were likely to adopt behaviors to protect their privacy when they became concerned; women, however, rarely adopted protective behaviors.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Singer, Randi W. and Adrian J. Perry (2015) [*Intellectual Property & Technology Law Journal*]	Recommendations for robust and adequate privacy policies so that customers understand what data are being collected and consent to their use.	Company best practices	Unscientific survey of the privacy policies of many popular wearable devices	Privacy Policies should: • Clearly communicate what data is being collected. • Clearly communicate what data are being shared. • Clearly explain the consequences of sharing data through a Social Network. • Explain the parameters of aggregated data.
Smith, H. Jeff, Tamara Dinev, and Heng Xu (2011) [*MIS Quarterly*]	To provide an interdisciplinary review of privacy-related research in order to enable a more cohesive treatment.	Information privacy	Sample of n=320 privacy articles and n=128 books and book sections	• First, there are many theoretical developments in the body of normative and purely descriptive studies that have not been addressed in empirical research on privacy. • Second, some of the levels of analysis have received less attention in certain contexts than have others in the research to date. • Third, positivist empirical studies will add the greatest value if they focus on antecedents to privacy concerns and on actual outcomes.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke (1996) [*MIS Quarterly]*	Develop and validate an instrument that identifies and measures the primary dimensions of individuals' concerns about organizational information privacy practices.	Information privacy	• 1. Stage: Literature review, experience surveys, focus groups, and expert judges. • 2. Stage: Exploratory factor analysis Interitem reliabilities, confirmatory factor analysis (LISREL) • 3. Stage: Three confirmation factor analysis (LISREL). • Across several heterogeneous populations, to provide a high degree of confidence in the scales' validity, reliability, and generalizability.	15-item instrument with four subscales tapping into dimensions of individuals' concerns about organizational information privacy practices.
Solove, Daniel J. (2006) [*University of Pennsylvania Law Review*]	Development of a taxonomy to identify privacy problems in a comprehensive and concrete man. Guide to a more coherent understanding of privacy and to serve as a framework for the future development of the field of privacy.	American privacy law, William Prosser's four interests of privacy (1960)	Qualitative, theoretical analysis of the American privacy law.	• Privacy is a multidimensional concept. • There is no common denominator to link all privacy violations. • Privacy is a form of protection against certain harmful or problematic activities. • To address privacy problems activities like the gathering, processing, and dissemination of information need to be regulated.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang (2013) [*MIS Quarterly*]	Conceptualize the extent to which privacy impacts the process and content gratifications derived from personalization, and find out how an IT solution can be designed to alleviate privacy concerns.	Uses and gratification theory and information boundary theory	• Pilot test with n=8 consumers. • Field experiment with n=629 participants. • The personalized, privacy-safe application is benchmarked against a non-personalized application, and a personalized, non-privacy safe application. • Follow-up survey with n=85 participants.	• There is a tension between personalization and privacy, which follows from marketers exploiting consumers' data to offer personalized product information (personalization–privacy paradox). • IT solution: A personalized, privacy-safe application, that retains users' information locally on their smartphones while still providing them with personalized product messages. • This application reduces users' perceptions that their information boundaries are being intruded upon, thus mitigating the personalization–privacy paradox and increases both process and content gratification.
Tam, Kar Yan and Shuk Ying Ho (2006) [*MIS Quarterly*]	Explore the effectiveness of web personalization and the link between the IT artifact (the personalization agent) and the effects it exerts on a user's information processing and decision making.	Social cognition and consumer research theory	• Two pretests with n=35 subjects. • 1. Laboratory experiment with n=207 undergraduate students from a major university in Hong Kong, where a token of appreciation (US$15) was provided. • 2. Field study with n=139 participants.	• The influence of a personalization agent is mediated by two variables: content relevance and self reference. • Content relevance, self reference, and goal specificity affect the attention, cognitive processes, and decisions of web users in various ways. • Users are found to be receptive to personalized content and find it useful as a decision aid.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Tang, Zhulei, Yu (Jeffrey) Hu, and Miichael D. Smith (2008) [*Journal of Management Information Systems*]	Development of analytic models of hidden information to analyze the effectiveness of three possible regimes (Caveat emptor, mandatory standards, self-of-approval program) to build trust and their efficiency in terms of social welfare.	Privacy concerns, concept of trust, game theory	Review of previous literature and qualitative, theoretical analysis of the three regimes through the utilization of game theory.	• A firm's ability to influence consumer beliefs about trust depends on whether firms can send unambiguous signals to consumers regarding their intention of protecting privacy. • Ambiguous signals can lead to a breakdown of consumer trust, while the clarity and credibility of the signal under industry self-regulation can lead to enhanced trust and improved social welfare. • Although governmental regulations an enhance consumer trust, it may not be socially optimal in all environments.
Thierer, Adam D. (2014) [*Richmond Journal of Law & Technology*]	Analyse how the Internet of Things (IoT) challenges traditional privacy norms and legal standards in the U.S.A. and what measures can be taken to protect privacy but still allow for innovations.	U.S. privacy law, Internet of Things	Qualitative, theoretical analysis of possible solutions.	• It is essential that experimentation and innovation in this space not be derailed on the basis of speculation about hypothetical worst-case scenarios. • Simple legal principles are greatly preferable to technology-specific, micromanaged regulatory regimes. • Ex ante (preemptive and precautionary) regulation is often highly inefficient.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Turel, Ofir, Yufei Yuan, and Catherine E. Connelly (2008) [*Journal of Management Information Systems*]	Examination how justice and trust affect user acceptance of a e-customer service.	Trust, justice theories	• Online experiment with n=380 participants in a 2x3 factorial design: Two levels of reputation of the other party (low, high), and three levels of fairness of the service (fais, biased toward the complainer, biased toward the respondent). • Reputation, procedural and interpersonal justice were manipulated.	• Trust in the e-customer service fully mediates the effects of trust in the service representative and procedural justice on intentions to reuse the e-customer service. • The effect of distributive justice on trust in the e-customer service was fully mediated by trust in the e-service representative. • The effect of information justice on user intentions to reuse the e-customer service was partially mediated by trust in the service representative and trust in the e-customer service.

Author/s (Year) [*Journal*]	Research Focus	Theoretical Background	Method/Analysis	Main Findings
Xu, Heng, Hock-Hai Teo, Bernard C. Y. Tan, and Ritu Agarwal (2009) [*Journal of Management Information Systems*]	This study extends the privacy calculus model to explore the role of information delivery mechanisms (pull and push) in the efficacy of three privacy intervention approaches (compensation, industry self-regulation, and government regulation) in influencing individual privacy decision making.	Privacy calculus, information privacy, theories of justice, location-based services	• Quasi-experimental survey with n=528 participants. • Structural equations modeling using partial least squares validated the instrument and the proposed model. • A 2 (pull-/push-based LBS) x 2 (with/without ompensation) x 2 with/without industry self-regulation) x 2 (with/without government regulation) between-subject, full-factorial design was used.	• The effects of the three privacy intervention approaches on an individual's privacy calculus vary based on the type of information delivery mechanism (pull and push). • Results suggest that providing financial compensation for push-based LBS is more important than it is for pull-based LBS. • It is also shown that privacy advocates and government legislators should not treat all types of LBS as undifferentiated but could instead specifically target certain types of services.
Yim, Chi Kin (Bennett), David K Tse, and Kimmy Wa Chan (2008) [*Journal of Marketing Research*]	The focus was to extend the existing satisfaction–trust–loyalty paradigm to investigate how customers' affectionate ties with firms (customer–firm affection)—in particular, the components of intimacy and passion—affect customer loyalty in services.	Concept of love, attachment theory, passion, intimacy	Netnography study and survey research in two service contexts	• The salience of intimacy and passion are two under recognized components of customer–firm affection that influence customer loyalty. • Customer–firm affection has a complementary and mediating role in strengthening customer loyalty. • There is a significant affect transfers from the customer–staff to the customer–firm level. • A dilemma emerges when customer–staff relationships are too close.

Author/s (Year) [*Journal*]	**Research Focus**	**Theoretical Background**	**Method/Analysis**	**Main Findings**
Zhou, Wei and Selwyn Piramuthu (2015) [*Journal of Business Ethics*]	Privacy differentiation and customization. To propose a contextual information relevance model of privacy.	Information privacy, social welfare, contextual privacy, vertical and horizontal differentiatio n	Review of existing privacy literature in the domain of business ethics, law and industrial organization. Theoretical development of the privacy relevance model with equations of economics.	• There exist individual differences with respect to unique security and privacy protection needs. • It is argued that it is unfair and socially inefficient to treat privacy in a uniform (or less differentiated) manner whereby a large proportion of the population remain unsatisfied by a common policy. • With privacy differentiation, the social planner will observe increases in demand and overall social welfare. • Business practitioners could profit from privacy customization.