Introducing new products that affect consumer privacy: A mediation model

Caroline Lancelot Miltgen, Jörg Henseler, Carsten Gelhard, Aleš Popovič

Introducing new products that affect consumer privacy: A mediation model

Caroline Lancelot Miltgen, AUDENCIA Business School

Jörg Henseler, University of Twente & NOVA IMS

Carsten Gelhard, University of Twente

Aleš Popovič, University of Ljubljana & NOVA IMS

Submission: November 2015

Revision: February 2016

The authors thank the European Commission for its funding for studying "Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions, and Acceptance of Risk." (EC JRC Contract IPTS n° 150876-2007 F1ED-FR). Caroline Lancelot Miltgen was the principal investigator of this research contract. Jörg Henseler acknowledges a financial interest in ADANCO and its distributor, Composite Modeling. The authors are further grateful to the comments by Special Issue Guest Editors and the reviewers on prior versions of this article. Send correspondence to Aleš Popovič, Faculty of Economics, University of Ljubljana, Kardeljeva ploščad 17, 1000 Ljubljana, Slovenia, ales.popovic@ef.uni-lj.si. Caroline Lancelot Miltgen, AUDENCIA Business School, 8 route de la Jonelière, BP 31222, 44312 Nantes Cedex 3, France, clancelot@audencia.com. Jörg Henseler, Department of Design, Faculty of Engineering Technology, University of Twente, 7500 AE Enschede, The Netherlands, j.henseler@utwente.nl. Carsten Gelhard, Department of Design, Faculty of Engineering Technology, University of Twente, 7500 AE Enschede, The Netherlands, c.gelhard@utwente.nl.

Introducing new products that affect consumer privacy: A mediation model

Abstract

Many innovative products can only fully deploy their value if they rely on consumers' personal information. This issue challenges the confidence consumers have in new innovations, and revolutionizes marketing practices. Malhotra, Kim, and Agarwal's (2004) framework provides the theoretical basis for hypotheses on the consequences of privacy concerns. An empirical study in the context of four pervasive IT innovations involving various privacy issues helps to test these hypotheses. The findings consistently show that privacy concerns have an adverse effect on consumers' intention to accept IT innovation. However, trust and risk perceptions both mediate this relationship. By understanding the underlying mechanism, firms can alleviate the potential downsides of their products and increase the odds of their market success.

Keywords: New product adoption; technological innovation; consumer privacy concerns; structural equation modeling

1. Introduction

Reliable personal identification represents a critical factor for many business activities. With personal information, “marketers are better able to identify the best prospects, create promotions and reward programs that build customer loyalty, customize advertising and promotion strategies, and evaluate the effectiveness and cost efficiency of advertising and promotions” (Phelps, Nowak, & Ferrell, 2000). However, technologies that better enable reliable automatic personal recognition, and the existence of more opportunities for marketers to associate an individual with other personal activities, cause the concern that this information violate consumers’ right to privacy (Prabhakar, Pankanti, & Jain, 2003).

Scholars consider privacy as a high-profile public policy and practice concern that affects consumers and marketers alike (Phelps et al., 2000). Definitions of the privacy concept range from the famous conception of the right to be let alone (Warren & Brandeis, 1890), to the right to control information of oneself (Westin, 1968). Consumer privacy, which refers to consumers’ control over their personal information, potentially occurs during information exchanges with marketers (Milne, 2000). According to social contract theory, marketers should view consumers' exchange of personal information as an implied social contract (Phelps et al., 2000, p. 29). Circumstances such as firms not informing consumer about information collection, or selling consumers’ personal information to third parties without permission, or consumers not having the chance to restrict the dissemination of their personal information, breach this social contract (Phelps et al., 2000). Ultimately, this infringement of consumers’ privacy may harm the relationship between marketers and consumers (Foxman & Kilcoyne, 1993).

Marketing practice emphasizes that consumer information privacy concerns play an important role for long-term consumer satisfaction and commercial success (Phelps, D'Souza, &

Nowak, 2001). Presently, this requirement is even more important as information privacy concerns "evolve under pressure of new technologies, shifting social priorities, and changes in generational norms of reticence and risk" (McCreary, 2008, p. 124). Nevertheless, marketers should not regard the management of consumer information as a burden. Instead, firms should view "the establishment of a framework of consumer privacy controls as an important marketing and strategic variable that conveys considerable benefits" (Goldfarb & Tucker, 2013, p. 10).

Extant studies suggest that consumers' privacy concerns have an unfavorable effect on their subsequent consumer behavior, such as personal information disclosure and online purchasing (Foxman & Kilcoyne, 1993). Firms that provide goods or services with a potential impact on consumer privacy should understand that consumers, in order to alleviate the adverse consequences, integrate their privacy concerns into their decision-making and their actions.

Within the realm of information systems, and drawing on social contract theory, Malhotra, Kim, and Agarwal (2004) offer a theoretical framework to explain the dimensions of consumers' information privacy concerns on the Internet, and the consequences of such concerns for their willingness to disclose personal information online. These authors' causal model integrates the social contract theory, the trust-risk framework, and the theory of reasoned action, and, therefore, applies to a variety of traditional marketing and other privacy contexts. Building on Malhotra et al.'s (2004) work, this paper investigates the proposed theoretical model within the context of technology-enabled personal identification. Compared to the previously deeply explored privacy concerns in online environments (e.g. Malhotra et al., 2004; Sheehan & Hoy, 2000; H. Wang, Lee, & Wang, 1998; Wirtz, Lwin, & Williams, 2007), prior literature still lacks a clear understanding of privacy concerns that relate to technology-enabled personal identification

(Tang, Bringer, Chabanne, & Pointcheval, 2008) despite the growing interest in this issue (Pons & Polak, 2008).

Privacy concerns refer to strong inhibitors to behavior, in particular to technology adoption (e.g. Vijayasarathy, 2004). However, prior literature shows that users can adopt relaxed attitudes in front of privacy invasive actions or technologies even when they hold strong privacy concerns, a result that refers to the privacy paradox effect (Norberg, Horne, & Horne, 2007). This research therefore tests whether different beliefs (i.e., trust and risks) can explain this paradox by mediating the effect of concerns on resulting technology acceptance. With the prevalence of technologies that nowadays enable third parties to extract personal data from electronic databases, users indeed expect that organizations have the competence to protect customer-sensitive data. In addition, considering that personal data might represent a source of economic value, consumers further rely on the organization's good intention of not using customer-related data for purposes inconsonant with the actual reasons for data collection (Beldad, de Jong, & Steehouder, 2011). Whenever users question the protection of their data, they tend to associate the disclosure of personal data with a risky action. Thus, although users may trust that a particular organization will not abuse or misuse their personal data, concerns about the probability of data abuse by third parties might still exist. Taken together, the present study entails the following research questions: What are the effects of risks and trust on behavioral intention to adopt a privacy-invasive technology? Could trust and risk be mediators of the impact of privacy concerns on intention to adopt? In particular, could trust mitigate the negative impact of privacy concerns?

Drawing on the findings of a quantitative study of young European consumers' acceptance of four different pervasive technological innovations that involve information privacy risks, this study advances the understanding of consumers' information privacy concerns and the

consequences of these concerns on marketing practice efficiency. The study entails three important contributions. First, it extends the information privacy concern model from the online personal information disclosure setting to a product adoption decision-making context by analyzing how consumers' privacy concerns impact their intention to accept a potentially pervasive technological innovation. Second, the analysis of the respective information privacy concern effect sizes of the Malhotra et al. (2004) study and the current study provides a better understanding of the different effects between the online disclosure of personal information and the adoption of technology-enabled personal identification solution. Third, this study makes use of a multi-method approach and applies a set-theoretic method as complementary analysis to structural equation modeling. Variance-based structural equation modeling helps assess the model fit, test for mediation, and examine the predictive validity of the proposed model. The qualitative comparative analysis (QCA) abandons the assumption that each exogenous variable has its own isolated net effect on the outcome of interest (here: behavioral intention) and assumes that (i) the interplay of different causal conditions constitutes an outcome and (ii) the causal conditions that lead to absence of an outcome are not necessarily the inverse of the causes of its presence. The combination of the two methods of analysis provides a more holistic picture on the mediated relationship between privacy concerns and behavioral intention.

2. Procedure

2.1 Data Collection

Like Malhotra et al. (2004), this study aims to test the structural model depicted in Figure 1. This model consists of five direct effects but explicitly shows no direct privacy concern effect

on behavioral intention. The theory considers this absence of a link as a full mediation effect, comprising risk and trust as two essential mediators.

Figure 1 here.

The authors collect data using cautiously designed written descriptive scenarios (vignettes) to gauge the participants' technology adoption decisions (see Appendix A). Prior research demonstrates that scenario-based approaches suits well for studying individual decision-making (Bateson & Hui, 1992; Seawright & Sampson, 2007; B. Wang & Manning, 1999). This method is particularly appropriate for technology adoption research, as the process of deciding whether to use a technology for the first time inherently involves some kind of imagination such as the following: when reading the scenario, the individuals must envision themselves doing something that does not belong to their sphere of experience. Thus, the use of hypothetical scenarios provides a good approximation of the adoption process, and comprises the opportunity to better control and measure than real-world behavior. The proposed scenarios outline electronic identification (eID) devices for personal identification purposes. Although the study incorporates four different scenarios representing four eID technologies, the authors show each participant just one scenario.

The first scenario examines a location tracker within a mobile phone that can store personal information and geographically locate the consumer and other users of the service. Being subject to little state regulation and enabling the tracking of the consumer's movements, the location tracker is a highly invasive technology.

The second scenario examines a Single Sign-On (SSO) technology that offers access to remote services via a unique PIN / Password combination. This technology offers the ability to

access numerous e-services and websites without identifying oneself on each occasion. In fact, the services which utilize this technology offer consumers the opportunity to have all their online activities accessible from a single website, thereby meaning the consumer must only remember a single access credential.

The third scenario examines a contactless token, an electronic microchip which can function as add-on to a modern electronic passport and contains additional information about an individual (e.g., medical information, emergency money, digital signature). Such technology is fairly invasive as it (optionally) uses geolocalization techniques in addition to requesting and registering sensitive personal data.

The fourth scenario examines a biometric identification technology for retina scanning. This technology is, along with face recognition, fingerprint recognition, hand geometry, and voice recognition, one of the most notable biometric technologies to identify people. While ensuring both hedonic and utilitarian purposes, biometric identification systems have potential to both enhance and threaten an individual's privacy.

The authors invite 531,443 Europeans between 15 and 25 years old to participate in this study. The sample refers to a sample from a Net Surfers database that the French company 1000mercis manages. By using quotas that steam from Eurostat, the authors ensure a balance of genders and ages across the population. A total of 12,143 participants respond, for a useful sample size of 4,479 fully completed questionnaires. The final sample includes only 18-25 years old people (this study removes persons from 15 to 17) to focus on an adult population. In addition, to avoid missing data, this study removes the participants who do not answer the whole questionnaire.

The structure of respondents by country reveals that most of participants come from France (around 43%), followed by UK and Spain (each of them totaling around 21%) to end with those from Germany (around 15%). Most of the respondents have advanced IT skills (75%) whereas a minority feels possessing merely a basic level of expertise (around 25%). The participants comprise the following groups: students (40%), collar workers (26%), postgraduates (31%), professionals (26%), or MSc/MA graduates (15%).

The data collection differs in three substantial ways from that of Malhotra et al. (2004). Malhotra et al. (2004) use face-to-face interviews instead of an online questionnaire, snowball sampling instead of quota sampling, and include respondents of all age groups, whereas this study only considers 18-25-year-old consumers. The final sample comprises an equal distribution amongst the 18-25 category (around 12-14% per age).

This research measures four main constructs, namely perceived risks, trust, privacy concerns, and the behavioral intention regarding eID acceptance. In so doing, this study adapts established scales from extant privacy and technology adoption literature (e.g. Bélanger & Carter, 2008; Fogel & Nehmad, 2009; Pavlou, 2003) to fit the context (see Appendix B).

2.2 Structural Equation Modeling (SEM)

The authors use variance-based structural equation modeling and make use of the software package ADANCO 2.0 (Henseler & Dijkstra, 2015) to analyze the data. This method has a favorable convergence behavior (Henseler, 2010) and determines composite scores of all the constructs. Consistent PLS allows to handle the constructs' reflective nature (Dijkstra & Henseler, 2015b). Variance-based structural equation modeling requires particular caution with regard to model identification (Henseler, Hubona, & Ray, 2016). Every construct requires a nomological net, which means that any construct has a relationship with at least one other

construct in the model. The strong theoretical basis and the previous empirical evidence for the conceptual model render identification most likely.

Bootstrap-based tests of the model fit over the least squares and the geodesic discrepancy between the empirical and the model-implied correlation matrix allow the assessment of the global goodness of model fit (Dijkstra & Henseler, 2015a). As long as the discrepancy between these two matrices is insignificant, scholars might not reject the model. Furthermore, as a measure of approximate fit, the standardized root mean square residual can help quantify the degree of (mis-)fit (Henseler et al., 2014). The SRMR of well-fitting models typically does not exceed a value of 0.08 (Hu & Bentler, 1999).

The construct measurement should demonstrate sufficient reliability and validity. The only consistent measure of internal consistency reliability is ρ_A (Henseler et al., 2016). More traditional, yet inconsistent reliability measures are Jöreskog's rho and Cronbach's alpha. While reliability values as low as 0.7 indicate proper reliability in early phases of research, higher values such as 0.8 or 0.9 should prevail in more advances research (Nunnally, 1978) which exceeds the common threshold values. The average variance extracted serves as a measure of unidimensionality (Fornell & Larcker, 1981). Finally, a heterotrait-monotrait ratio of correlations (HTMT) clearly below one provides evidence of discriminant validity (Henseler, Ringle, & Sarstedt, 2015). Monte Carlo simulations show that the HTMT outperforms more traditional measures of discriminant validity (Voorhees, Brady, Calantone, & Ramirez, 2016).

The path coefficients are the most important result of the structural model. They indicate the change in a dependent variable as a consequence of a unit change in an independent variable if all other independent variables remain constant. Bootstrap percentile confidence intervals of the path coefficients help generalize from the sample to the population. Scholars should prefer

bootstrap percentile confidence intervals over mere null hypothesis significance testing (Cohen, 1994). The direct and indirect effects jointly provide evidence for mediation (Nitzl, Roldán, & Cepeda, 2016).

To assess the predictive validity of model results, prior literature recommends to make use of holdout samples (Woodside, 2013). Concretely, applying the parameter estimates from one eID technology to the data of the other eID technologies quantifies the level of out-of-sample prediction. The coefficient of determination $R^2_{(h)}$ for a holdout sample stems from Hotelling (1936) and draws from the vectors of path coefficient of the calibration sample b and the holdout sample $b_{(h)}$ as well as the correlation matrix of independent variables of the holdout sample **R**:

$$R^2_{(h)} = \frac{b'\mathbf{R}b_{(h)}}{b'\mathbf{R}b \cdot b'_{(h)}\mathbf{R}b_{(h)}}$$

At last, a comparison of the findings of the four scenarios with Malhotra et al.'s (2004) results improve the understanding of how the importance of consumers' online disclosure of personal information differs from that of the adoption of technological innovations for personal identification.

2.3 Fuzzy Set Qualitative Comparative Analysis (fsQCA)

Multiple regression analysis procedures as well as structural equation modeling comprise limitations when scholars not only seek to test symmetric relationships but also intend to identify asymmetric causality (Fiss, 2011; Ragin, 2008; Woodside, 2013; Woodside, Hsu, & Marshall, 2011; Woodside, Ko, & Huan, 2012). Multiple regression analyses as well as structural equation modeling generally embrace a correlational understanding of causality within their statistical foundation. Fiss (2011, p. 394), in this context, argue that "a correlational understanding of

causality implies causal symmetry because correlations tend to be symmetric. For instance, if one were to model the inverse of high performance, then the results of a correlational analysis would be unchanged, except for the sign of the coefficients". Hence, low values of a dependent variable (or complex sets of dependent variables) associate with low values of the independent variable, and high values of a dependent variable with high values of the independent variable (Woodside, 2013). This relationship, however, might not always represent the truth as relationships might also comprise an asymmetric nature. Here, high values of a dependent variable might suffice for high values of the independent variable, but might not be necessary (Woodside, 2013). To actually address the potential presence of asymmetric relationships within the research model, this study reanalyzes the present data by applying a fuzzy-set qualitative comparative analysis (fsQCA) as complementary analysis method to variance-based structural equation modeling. Although prior scholars initially conceive fsQCA as an approach for small sample sizes (10-50 cases), recent studies show that configurational comparative methods also apply for larger sample sizes (more than 1,000 cases) (e.g. Cooper & Glaesser, 2015; Fiss, 2011). FsQCA represents a set-theoretic method and, as such, not only accounts for asymmetric relationships, but also captures conjunction and considers the possibility of equifinality. While regression analyses, such as variance-based structural equation modeling, focus on the isolated net influence of each variable on the outcome of interest, fsQCA considers that causal factors might not influence the outcome of interest independently from each other (i.e., conjunction) and different sets of causal factors can achieve the same outcome (i.e., equifinality) (Ragin, 2000). Thus, contrasting variance-based structural equation modeling, fsQCA considers the relationship between multiple factors in terms of set memberships (Fiss, 2011). As result of a fuzzy set membership, each case of the underlying sample belongs to a specific configuration to a certain degree and has varying

degrees of memberships in different configurations. The fsQCA procedure, therefore, implies the calibration of all the variables into a set of membership values ranging from 0 (full non-membership) to 1 (full membership) (Fiss, 2011; Woodside, 2013). For the reduction of numerous, complex causal conditions into a set of conditions that causes the outcome of interest fsQCA uses Boolean algebra (Fiss, 2011).

Since asymmetric causality and equifinality should either occur or not occur in all of the four samples, the additional analysis with fsQCA examines the combined set of the different samples, which comprises a total of 4,479 cases. The fsQCA consists of the following stages: (i) transformation of construct measures into fuzzy-set memberships (i.e., calibration), (ii) construction and refinement of the truth-table, and (iii) analysis of sufficient configurations (Fiss, 2011).

To transfer the information on the measurement model of the structural equation model into the subsequent analysis using the QCA software package fsQCA 2.5, the analysis incorporates unstandardized construct scores as input, which represents an alternative to the use of the mean scores of the underlying constructs. Following prior research (Ordanini, Parasuraman, & Rubera, 2014), the transformation includes the following three anchors for the construct scores using a seven (five) point Likert-type scale: 6 (4) as a threshold for full membership, 2 (2) as a threshold for full non-membership, and 4 (3) as indifference point.

The construction of the truth table eventually results in 2^k logically possible combinations of causal conditions with k representing the number of causal conditions (in the present study k = 3). The subsequent refinement of the initial truth table requires the selection of the frequency threshold (i.e., the number the minimum number of cases required for a solution to be considered) and the consistency level (i.e., extent to which cases with a given causal condition, or

combination of causal conditions, correspond to the outcome of interest) (Fiss, 2011). Owing to the large sample size, this study applies a frequency level of 100. Furthermore, since no rules determine the exact minimum consistency level of a solution, the present analysis refers to the ordered consistency values in the truth table and selects a clear drop of consistency as a cutoff value (Leischnig & Kasper-Brauer, 2015). The resulting minimum consistency levels are: 0.68 (presence) and 0.95 (absence). Hence, the consistency value to analyze the presence of the measure behavioral intention is slightly below the recommended threshold of 0.75 (Ragin, 2006, 2008). A selection of a more restrictive consistency threshold would eventually lead to all the configurations being considered as insufficient for the outcome.

3. Results

The conceptual model has an excellent fit for all four studies. Table 1 demonstrates that all discrepancies do not exceed the 95% percentile of their bootstrap distribution. In other words, the empirical and the model-implied correlation matrices do not differ significantly. The fit values are also impressive in absolute terms: All SRMR values do not exceed 0.03 and thus lie clearly below common cut-off thresholds such as 0.08.

Table 1 here.

The construct measurement shows decent reliability and validity throughout (see Table 2). Dijkstra-Henseler's ρ exceeds 0.8 in all instances, which speaks for a high internal consistency reliability of the construct scores. Appendix C further entails the individual items loadings. Since all variance extracted values exceed the value of 0.5, no second factor of equal importance to confound the first factor with. Hence, the results confirm the unidimensionality of the constructs.

The study-wide maximum HTMT is 0.6257, which is far below the strictest threshold of 0.85, and thus confirms the discriminant validity of measurement.

Table 2 here.

Table 3 contrasts the results of the paper by Malhotra et al. (2004) with the empirical findings of this study's four cases. The findings show a consistent pattern of effects across all four techniques. Although the effects of Malhotra et al. (2004) are of different sizes in parts, the majority of findings are similar with respect to the hypotheses: Privacy concerns have a positive effect on risk perceptions and a negative effect on trust. Trust has a negative effect on risk perceptions. Trust has a positive effect on behavioral intention, but risk perceptions affect it negatively.

Table 3 here.

The direct effect of privacy concerns on behavioral intention is not significant in any study, whereas the indirect effect (see Table 4) is consistently negative and significant. With regard to the difference in effect sizes, the antecedents of behavioral intention deserve particular attention. Whereas Malhotra et al. (2004) find that a decrease in the perceived risk increases the behavioral intention most, trust is the most important predictor of behavioral intention with regard to all four technologies.

Table 4 here.

Table 5 provides insights in the predictive relevance of the model. It compares the R^2 values of the final outcome variable intention to adopt from the calibration samples (in the main diagonals) with the proportions of variance explained by the coefficients from the other three samples. Every sample thus serves once as calibration sample and three times as holdout sample.

Table 5 shows that the R^2 values hardly vary between calibration sample and holdout samples. This finding implies an excellent generalizability of the findings.

Table 5 here.

Table 6 summarizes the findings of the fsQCA, with the notion ~ indicating the absence of a condition. While (c) indicates core conditions, (p) indicates peripheral conditions. Table 6 shows that the analysis of the causes that stimulate behavioral intention to adoption results in one distinct configuration, namely the presence of privacy concerns, the absence of risk perception, and the presence of trust. The overall consistency level for the presence (absence) of behavioral intention is 0.68 (0.95). The final configuration reveals an overall solution coverage of 0.42 (0.12) for the presence (absence) of behavioral intention, which indicates that the final configuration accounts for 42% (12%) of the membership in the presence (absence) of behavioral intention. Since the analysis only reveals a single solution, and the causes of non-behavioral intention are the opposite of the causal conditions leading to the presence of behavioral intention, the reanalysis with fsQCA does not disclose asymmetric causality with regard to the combined sample.

Table 6 here.

4. Discussion and Conclusion

The present study comprises manifold findings. First, this study confirms that consumers' privacy concerns have a negative influence on the intention to adopt an eID technology. Hence, consumer privacy concerns principally endanger the successful introduction of potentially privacy-invading technologies. Second, the influence of consumers' privacy concerns on the intention to adopt such a technology is purely indirect. For all four technologies, trust and risk

jointly mediate the effect of consumers' privacy concerns on the intention to adopt. Third, trust and risk have direct, yet opposite effects on the intention to adopt an eID technology. Whereas risk reduces the intention to adopt, trust increases the intention to adopt. Trust therefore mitigates the negative impact of privacy concerns on the intention to adopt whereas risks on the contrary reinforces this adverse effect and diminishes the adoption intention. Finally, the analysis of various technologies discloses stable findings, which implies a high external validity.

The findings of this research confirm previous literature in this area and reinforce them while adding additional validity. The outcomes extend Malhotra et al.'s (2004) results by means of a new context (i.e., technological innovation) and new outcomes (technology acceptance vs. information self-disclosure decisions). Thereby, this study confirms that, for all four technological innovations, the perceived risks and trust fully mediate the effect of privacy concerns on behavioral intention to adopt the technology. This study totally supports Malhotra et al.'s (2004) work and supplies additional external validity. However, some differences appear between both studies in the corresponding effect sizes: Malhotra et al. (2004) find that risk is the most important predictor of behavior, whereas this study's results suggest that trust mostly drives behavioral responses. From a socio-consumer perspective, this finding implies that young consumers do not have sufficient information to overcome the fears that technology-enabled personal identification innovations generate and engage in a relationship with the service providers based on their perception of trust.

This study provides a qualitative confirmation of Malhotra et al.'s (2004) main findings, but the results show no quantitative differences in the magnitudes of the effects. While the time between the studies, or their different scopes, may potentially influence the findings, this study allows to at least partially examine the differences with regard to the sample composition.

Malhotra et al. (2004) survey respondents across all age groups, whereas this study uses age as a blocking factor and only surveys young consumers. Younger individuals usually have a higher level of personal innovativeness (Im, Bayus, & Mason, 2003).

The fsQCA findings complement the results of the structural equation modeling and give more information about what combinations of exogenous variables lead to behavioral attention. As the fsQCA shows, neither the absence of risk perception nor the presence of trust in isolation, but the interplay of both mediators might cause consumers to eventually adopt eIDs devices used for personal identification purposes. Hence, instead of following an either-or-strategy in the pursuit of improved behavioral intention, firms should direct their customer-relationship activities towards both the reduction of perceived risk as well as the establishment of trust. The fsQCA further provides support for the existence of a symmetric relationship between privacy concerns, risk perception and trust, on the one side, and behavioral intention, on the other side. While high values of privacy concerns and trust as well as low values of perceived risk associate with high values of behavioral intention, low values of privacy concerns and trust as well as high values of perceived risk associate with low values of consumers' intention to adopt eIDs devices. Taken together, improving both risk perception and trust is indispensable to increase the consumers' behavioral intention.

This study's findings have several important practical implications for new product/service adoption dealing with potential privacy risks. First, if a firm can succeed in its customers' only perceiving a low risk of misusing their personal information, firms can alleviate the effect of consumers' privacy concerns on behavioral intention. Second, if a firm manages to achieve high trust in its innovation, this trustworthiness will mitigate the effect of privacy concerns on behavioral intention. The remaining direct effect of consumers' privacy concerns on

behavioral intention – although still negative with regard to the sign of the parameter estimates – becomes insignificant.

The results of this study elucidate the controversy in the literature regarding the privacy paradox, which involves perceived contradictions between stated attitudes (here privacy concerns) and declared or actual behavior from a theoretical perspective (Brandimarte, Acquisti, & Loewenstein, 2013; Norberg et al., 2007). Although scholars extensively discuss the privacy paradox, they do not empirically fully explore this important phenomenon ((with the notable exception of Spiekermann, Grossklags, & Berendt, 2001). A possible explanation for such paradoxical behavior may lie in the indirect effects of privacy concerns on behavioral intention. The direct effect of consumers' privacy concerns on behavioral intention shows no link, which previous literature mostly interprets as a privacy paradox. The indirect effects, however, show that other variables mediate the link between privacy concerns and behavioral intentions, which partly adjust the behavioral consequences. Understanding the total effects rather than only the pure direct effect, helps resolve the paradox between privacy concerns and behavioral intention.

References

Bateson, J., E. G., & Hui, M. K. (1992). The Ecological Validity of Photographic Slides and Videotapes in Simulating the Service Setting. *Journal of Consumer Research, 19*(2), 271-281.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165-176. doi:10.1016/j.jsis.2007.12.002

Beldad, A., de Jong, M., & Steehouder, M. (2011). A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet. *The Information Society, 27*(4), 220-232. doi:10.1080/01972243.2011.583802

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science, 4*(3), 340-347. doi:10.1177/1948550612455931

Cohen, J. (1994). The earth is round (p<.05). *American Psychologist, 49*(12), 997-1003. doi:10.1037/0003-066X.49.12.997

Cooper, B., & Glaesser, J. (2015). Exploring the robustness of set theoretic findings from a large n fsQCA: an illustration from the sociology of education. *International Journal of Social Research Methodology*, 1-15. doi:10.1080/13645579.2015.1033799

Dijkstra, T. K., & Henseler, J. (2015a). Consistent and asymptotically normal PLS estimators for linear structural equations. *Computational Statistics & Data Analysis, 81*, 10-23. doi:10.1016/j.csda.2014.07.008

Dijkstra, T. K., & Henseler, J. (2015b). Consistent Partial Least Squares Path Modeling. *MIS Quarterly, 39*(2), 297-316.

Fiss, P. C. (2011). Building Better Causal Theories: A Fuzzy Set Approach to Typologies in Organization Research. *Academy of Management Journal, 54*(2), 393-420. doi:10.5465/amj.2011.60263120

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160. doi:10.1016/j.chb.2008.08.006

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.

Foxman, E. R., & Kilcoyne, P. (1993). Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing, 12*(1), 106-119.

Goldfarb, A., & Tucker, C. (2013). Why Managing Consumer Privacy Can Be an Opportunity. *MIT Sloan Management Review, 54*(3), 10-12.

Henseler, J. (2010). On the convergence of the partial least squares path modeling algorithm. *Computational Statistics, 25*(1), 107-120.

Henseler, J., & Dijkstra, T. K. (2015). ADANCO 1.1. Kleve: Composite Modeling.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M., & Calantone, R. J. (2014). Common Beliefs and Reality About PLS: Comments on Rönkkö and Evermann (2013). *Organizational Research Methods, 17*(2), 182-209. doi:10.1177/1094428114526928

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems, 116*(1), 2-20. doi:10.1108/IMDS-09-2015-0382

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135. doi:10.1007/s11747-014-0403-8

Hotelling, H. (1936). Relations between two sets of variates. *Biometrika, 28*(3/4), 321-377.

Hu, L. t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal, 6*(1), 1-55.

Im, S., Bayus, B. L., & Mason, C. H. (2003). An Empirical Study of Innate Consumer Innovativeness, Personal Characteristics, and New-Product Adoption Behavior. *Journal of the Academy of Marketing Science, 31*(1), 61-73. doi:10.1177/0092070302238602

Leischnig, A., & Kasper-Brauer, K. (2015). Employee Adaptive Behavior in Service Enactments. *Journal of Business Research, 68*(2), 273-280. doi:10.1016/j.jbusres.2014.07.008

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355. doi:10.1287/isre.1040.0032

McCreary, L. (2008). What Was Privacy? *Harvard Business Review, 86*(10), 123-131.

Milne, G. R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing, 19*(1), 1-6. doi:10.1509/jppm.19.1.1.16934

Nitzl, C., Roldán, J. L., & Cepeda, G. (2016). Mediation Analyses in Partial Least Squares Structural Equation Modeling: Helping Researchers to Discuss More Sophisticated Models. *Industrial Management & Data Systems, Forthcoming*.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. doi:10.1111/j.1745-6606.2006.00070.x

Nunnally, J. (1978). Psychometric theory: New York: McGraw-Hill.

Ordanini, A., Parasuraman, A., & Rubera, G. (2014). When the Recipe Is More Important Than the Ingredients: A Qualitative Comparative Analysis (QCA) of Service Innovation Configurations. *Journal of Service Research, 17*(2), 134-149. doi:10.1177/1094670513513337

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce, 7*(3), 101-134. doi:10.2307/27751067

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2-17. doi:10.1002/dir.1019

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

Pons, A. P., & Polak, P. (2008). Understanding user perspectives on biometric technology. *Communications of the ACM, 51*(9), 115-118. doi:10.1145/1378727.1389971

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy, 1*(2), 33-42.

Ragin, C. C. (2000). *Fuzzy-set social science*. Chicago, IL: University of Chicago Press.

Ragin, C. C. (2006). Set Relations in Social Research: Evaluating Their Consistency and Coverage. *Political Analysis, 14*(3), 291-310. doi:10.1093/pan/mpj019

Ragin, C. C. (2008). *Redesigning Social inquiry: Fuzzy sets and beyond*. Chicago, IL: University of Chicago Press.

Seawright, K. K., & Sampson, S. E. (2007). A video method for empirically studying wait-perception bias. *Journal of Operations Management, 25*(5), 1055-1066. doi:10.1016/j.jom.2006.10.006

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73. doi:10.1509/jppm.19.1.62.16949

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). *E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior*. Paper presented at the Proceedings of the 3rd ACM conference on Electronic Commerce, Tampa, Florida, USA.

Tang, Q., Bringer, J., Chabanne, H., & Pointcheval, D. (2008). A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes. In L. Chen, Y. Mu, & W. Susilo (Eds.), *Information Security Practice and Experience* (Vol. 4991, pp. 56-70): Springer Berlin Heidelberg.

Vijayasarathy, L. R. (2004). Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. *Information & Management, 41*(6), 747-762. doi:10.1016/j.im.2003.08.011

Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: an analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science, 44*(1), 119-134.

Wang, B., & Manning, E. R. (1999). Computer Simulation Modeling for Recreation Management: A Study on Carriage Road Use in Acadia National Park, Maine, USA. *Environmental Management, 23*(2), 193-203. doi:10.1007/s002679900179

Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70. doi:10.1145/272287.272299

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348. doi:10.1108/09564230710778128

Woodside, A. G. (2013). Moving beyond multiple regression analysis to algorithms: Calling for adoption of a paradigm shift from symmetric to asymmetric thinking in data analysis and crafting theory. *Journal of Business Research, 66*(4), 463-472. doi:10.1016/j.jbusres.2012.12.021

Woodside, A. G., Hsu, S.-Y., & Marshall, R. (2011). General theory of cultures' consequences on international tourism behavior. *Journal of Business Research, 64*(8), 785-799. doi:10.1016/j.jbusres.2010.10.008

Woodside, A. G., Ko, E., & Huan, T. C. (2012). The new logic in building isomorphic theory of management decision realities. *Management Decision, 50*(5), 765-777. doi:10.1108/00251741211227429

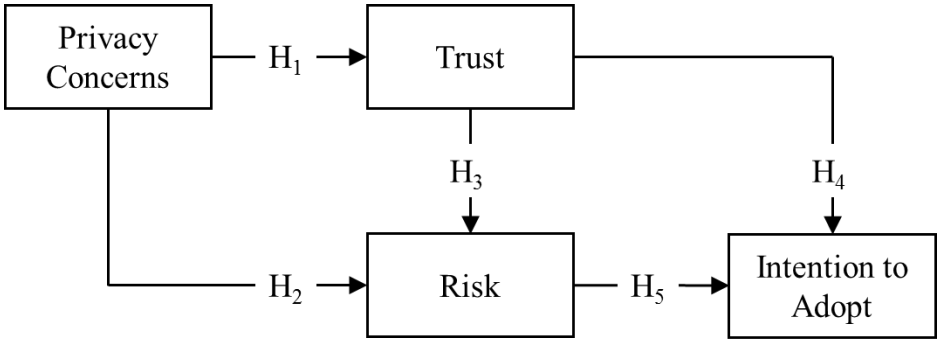

Figure 1

Conceptual Model

Table 1

Global goodness of fit and bootstrap-based 95% and 99% quantiles

Goodness-of-Fit Measure		Study			
		Location Tracker	SSO	Contactless Token	Retina Scanning
Standardized Root Mean Square Residual	SRMR	0.03	0.02	0.02	0.03
	Hi_{95}	0.03	0.03	0.03	0.03
	Hi_{99}	0.03	0.03	0.04	0.04
Unweighted Least Squares Discrepancy	d_{ULS}	0.04	0.04	0.03	0.05
	Hi_{95}	0.05	0.05	0.06	0.08
	Hi_{99}	0.07	0.07	0.08	0.11
Geodesic Discrepancy	d_G	0.04	0.04	0.03	0.04
	Hi_{95}	0.04	0.05	0.05	0.06
	Hi_{99}	0.06	0.08	0.07	0.08

Table 2

Reliability and validity of construct measurement

Construct	Number of indicators	Study	Study: Location Tracker	Study: SSO	Study: Contactless Token	Study: Retina Scanning
Privacy Concerns	4	Dijkstra-Henseler's rho (ρ_A)	0.87	0.88	0.85	0.85
		Jöreskog's rho (ρ_c)	0.85	0.88	0.85	0.84
		Cronbach's alpha (α)	0.85	0.87	0.85	0.84
		Average Variance Extracted	0.60	0.64	0.59	0.57
		Maximum HTMT	0.39	0.33	0.36	0.29
Trust	2	Dijkstra-Henseler's rho (ρ_A)	0.91	0.92	0.92	0.92
		Jöreskog's rho (ρ_c)	0.90	0.92	0.92	0.90
		Cronbach's alpha (α)	0.90	0.91	0.91	0.89
		Average Variance Extracted	0.82	0.85	0.85	0.82
		Maximum HTMT	0.60	0.61	0.63	0.44
Risk	3	Dijkstra-Henseler's rho (ρ_A)	0.83	0.87	0.81	0.83
		Jöreskog's rho (ρ_c)	0.82	0.85	0.78	0.83
		Cronbach's alpha (α)	0.82	0.85	0.78	0.83
		Average Variance Extracted	0.60	0.66	0.55	0.62
		Maximum HTMT	0.39	0.35	0.36	0.29
Intention to Adopt	2	Dijkstra-Henseler's rho (ρ_A)	0.88	0.88	0.89	0.87
		Jöreskog's rho (ρ_c)	0.88	0.88	0.89	0.87
		Cronbach's alpha (α)	0.88	0.87	0.89	0.87
		Average Variance Extracted	0.78	0.78	0.81	0.77
		Maximum HTMT	0.60	0.61	0.63	0.44

Table 3

Structural model results (standardized coefficients incl. lower and upper bounds of 95% confidence interval and coefficient of determination)

Dependent variable	Independent variable	Own study																Malhotra et al. (2004)
		Location Tracker				SSO				Contactless Token				Retina Scanning				
		Value	95%-CI_{LO}	95%-CI_{HI}	R^2	Value	95%-CI_{LO}	95%-CI_{HI}	R^2	Value	95%-CI_{LO}	95%-CI_{HI}	R^2	Value	95%-CI_{LO}	95%-CI_{HI}	R^2	Value
Trust	Privacy Concerns	-0.13	-0.20	-0.06	0.02	-0.15	-0.22	-0.08	0.02	-0.13	-0.21	-0.06	0.02	-0.13	-0.21	-0.06	0.02	-0.34
Risk	Privacy Concerns	0.35	0.28	0.43	0.20	0.28	0.21	0.35	0.20	0.32	0.25	0.39	0.20	0.26	0.19	0.34	0.13	0.26
	Trust	-0.24	-0.31	-0.16		-0.30	-0.37	-0.23		-0.27	-0.34	-0.20		-0.21	-0.28	-0.13		-0.15
Intention to Adopt	Privacy Concerns	-0.05	-0.11	0.02	0.39	-0.01	-0.07	0.06	0.39	0.00	-0.07	0.06	0.40	0.01	-0.06	0.09	0.21	n/a
	Trust	0.55	0.47	0.62		0.57	0.50	0.64		0.59	0.52	0.65		0.40	0.32	0.48		0.23
	Risk	-0.16	-0.24	-0.08		-0.12	-0.20	-0.03		-0.12	-0.19	-0.04		-0.15	-0.24	-0.06		-0.63

Table 4

Indirect effects (incl. lower and upper bounds of 95% confidence interval)

Dependent variable	Independent variable	Study											
		Location Tracker			SSO			Contactless Token			Retina Scanning		
		Value	95%-CI_{LO}	95%-CI_{HI}	Value	95%-CI_{LO}	95%-CI_{HI}	Value	95%-CI_{LO}	95%-CI_{HI}	Value	95%-CI_{LO}	95%-CI_{HI}
Risk	Privacy Concerns	0.03	0.01	0.05	0.05	0.02	0.07	0.04	0.02	0.06	0.03	0.01	0.05
Intention to Adopt	Privacy Concerns	-0.13	-0.19	-0.08	-0.12	-0.17	-0.08	-0.12	-0.17	-0.07	-0.10	-0.14	-0.06
Intention to Adopt	Trust	0.04	0.02	0.06	0.04	0.01	0.06	0.03	0.01	0.06	0.03	0.01	0.05

Table 5

Predictive validity

	R^2 values obtained predicting the intention to adopt…			
using the coefficients based on the study of …	Location Tracker	SSO	Contactless Token	Retina Scanning
Location Tracker	0.39	0.38	0.38	0.38
SSO	0.38	0.39	0.39	0.38
Contactless Token	0.40	0.40	0.40	0.40
Retina Scanning	0.21	0.21	0.21	0.21

Table 6

Configurations for Behavioral Intention

Behavioral Intention	Solution	Raw Coverage	Unique Coverage	Consistency
Presence	Privacy Concerns (p) * Trust (c) ~ Risk Perception (c)	0.42	0.42	0.68
Absence	~ Privacy Concerns (c) ~ Trust (p) * Risk Perception (p)	0.12	0.12	0.95

Appendix A: Description of the scenarios

SCENARIO	Technology	Applications
Your friend **Claudia** is 16 and always busy hanging around with her friends. A company offers her a service to keep in touch with her friends and know new people. To help her identify people she may like to meet and friends feeling like the same in the vicinity (bars, clubs, gym and university), the service requires some of her personal data, such as age, gender and location. The service is accessible through her mobile phone, based on the SIM card. If Claudia switches on the service her whereabouts and current activities are charted, to match other people's whereabouts.	Communicating device (SIM card)	Access to shared information spaces
Your friend **Max** is 18; he moved from his village to Dublin to work in a call centre during the summer. To keep in touch with his friends and manage his new life, he needs to access his email accounts and mobile devices, and make use of a range of websites such as Facebook, Skype, online banking, paying tax online, online grocery shopping etc. As he has no internet at home, he uses a close-by internet café. The owner of the café offers him to manage all his activities (social, leisure and financial) from a single website, using a single login and password.	SSO (Single PIN/password)	Access to remote services (SNS, e-commerce)
Your friend **Alice** is turning 18, and is planning a 3-months trip abroad over the summer. She will carry her electronic passport to visit all the countries she has in mind. A company offers to add to the passport chip additional information of her choice, such as her travel preferences, food tastes, her digital signature, some emergency money etc. With this enhanced chip she could access a range of services without carrying around additional documents. For instance, shopping malls could advise on clothes she may like as she walks past them; travel agents may suggest additional sights seeing based on her route, and credit could be added to the card in case of medical emergency.	Contactless token	Access to remote services (e-commerce)

SCENARIO	**Technology**	**Applications**
Your friend **Alex** is 17. Every day he goes to the library to practice for his driving test on one of the driving simulators provided by the local council. To enter the library, he could join the queue at the counter, which is half-dozen people long, including people he knows, and have his library card scanned. In this case, the librarian will look at his file, ask him a few questions and allocate the right simulator. Alternatively, he could use the eye-scan machine at the entrance. This automatically allocates him a simulator to use, based on his previous test results and on his preferences. The second procedure will probably take him less time.	Biometrics	Facilitating person-bound (non-remote) services

Appendix B: Measurement Items

Privacy concerns (PC)

How concerned are you about the following risks in relation to your personal information?		Very concerned	To	Not at all concerned
PC1	My personal data is shared with third parties without my agreement	1		5
PC2	My behavior and activities can be monitored online	1		5
PC3	My online personal data is used to send me commercial offers	1		5
PC4	My identity is reconstructed using personal data from various sources	1		5

Trust in technology (TT)

To what extent do you agree with the following description of the service?		Strongly disagree	To	Strongly agree
TT1	My personal data is shared with third parties without my agreement	1		7
TT2	My behavior and activities can be monitored online	1		7

Risk (R)

What are the potential risks you would mention to your friend?		Very concerned	To	Not at all concerned
R1	Information may be collected that could be used against you in future life	1		7
R2	Someone may use your identity instead of you	1		7
R3	Your personal data will be shared with unauthorized persons	1		7

Intention of eID Adoption (IA)

What would you recommend to your friend?		Very concerned	To	Not at all concerned
IA1	He/she should apply this service as soon as possible	1		7
IA2	He/she should use this service soon after it is launched	1		7

Appendix C: Indicator loadings

Construct	Indicator	Study			
		Location Tracker	SSO	Contactless Token	Retina Scanning
Privacy Concerns	pc1	0.87	0.82	0.73	0.89
	pc2	0.84	0.82	0.77	0.72
	pc3	0.58	0.74	0.74	0.70
	pc4	0.77	0.82	0.82	0.70
Trust	tt1	0.95	0.96	0.98	1.00
	tt2	0.87	0.88	0.86	0.80
Risk	r1	0.84	0.78	0.78	0.80
	r2	0.65	0.71	0.56	0.71
	r3	0.82	0.93	0.86	0.84
Intention to Adopt	ia1	0.92	0.91	0.89	0.88
	ia2	0.85	0.85	0.91	0.87