Association for Information Systems
AIS Electronic Library (AISeL)

Research-in-Progress Papers   ECIS 2016 Proceedings

Summer 6-15-2016

FEARING ONLINE IDENTITY THEFT: A SEGMENTATION STUDY OF ONLINE CUSTOMERS

Gianfranco Walsh
Friedrich-Schiller University of Jena, walsh@uni-jena.de

Patrick Hille
Friedrich-Schiller University of Jena, patrick.hille@uni-jena.de

Mark Cleveland
The University of Western Ontario, mclevela@uwo.ca

Follow this and additional works at: http://aisel.aisnet.org/ecis2016_rip

FEARING ONLINE IDENTITY THEFT: A SEGMENTATION STUDY OF ONLINE CUSTOMERS

Research in Progress

Walsh, Gianfranco, Friedrich-Schiller University of Jena, Jena, Germany, walsh@uni-jena.de

Hille, Patrick, Friedrich-Schiller University of Jena, Jena, Germany, patrick.hille@uni-jena.de

Cleveland, Mark, The University of Western Ontario, London, Canada, mclevela@uwo.ca

Abstract

The growth of online transactions coincides with the rise of cyber-criminals' intent on stealing consumers' personal and financial data. This fosters fear of online identity theft (FOIT), which in turn may lead to changes in consumer behavior and negatively affect e-business performance. This research aims to identify empirically derived segments of FOIT-prone consumers. Using a large sample of online shoppers, four distinct clusters are identified—'less fearful shoppers', 'strong fear but ignoring shoppers', 'fearless shoppers', and 'fearful shoppers'. The clusters differ significantly with respect to primary cluster variables as well as numerous secondary cluster variables. The relevance of FOIT for segmenting online consumers and theoretical implications for IS research are discussed.

Keywords: Cluster Analysis, Consumer Fear of Online Identity Theft, E-commerce, Online Trust.

1   Introduction

Ever more business transactions are conducted on the Internet. Transacting online requires consumers to transfer their personal and financial data to third parties online (Forsythe et al., 2006). However, the growth in online transactions has been paralleled by a surge in online identity theft. Online identity theft is a cyber-crime and denotes the illegal use of another individual's identifying facts (name, birth date, address, credit card number, etc.) to commit an economic fraud, or to masquerade identity (Reyns, 2013).

Identity theft was the top consumer complaint reason in the U.S. in 2013, accounting for 14% of the more than 2m complaints filed with the Federal Trade Commission (2014). However, the true number of identity theft victims has been estimated to exceed 16.6m in 2012 with annual costs of $24.7bn for consumers in the U.S. according to the Bureau of Justice Statistics (Harrell and Langton, 2013). Media reports about high-profile data thefts such as Target's data breach involving millions of customers (Harris et al., 2014), and the recent Heartbleed virus compromising the OpenSSL (secure socked layering) encryption used by online merchants and online government services the world over (Orton and Schlag, 2014; Ruan, 2014). Such media reports further bolster consumers' anxieties, as they recognize that their personal and financial data in the online environment is highly valuable to identity thieves (Coles-Kemp et al., 2010). Studies report that more than 70% of consumers are concerned about the theft of personal data and highlight the fear of being personally victimized by identity theft (e.g., Montague, 2011).

Given these findings and the potential negative impact on e-commerce attitudes and intentions, it is not surprising that the importance of consumer privacy has been recognized in IS and e-commerce research (Bélanger and Crossler, 2011; Dinev and Hart, 2006; Pavlou, 2011; Tsai et al., 2011). Whereas extant studies have provided important insights into consumer responses to privacy concerns and detail measures that e-businesses can take to protect consumer data, they have neglected consumers' negative emotional states that can arise from perceptions of threat to their privacy. Among the negative emotions that can result from learning about or having directly experienced identity theft the fear of themselves becoming a victim of online identity theft is of particular relevance (Reisig et al., 2009; Wall, 2008). Fear of online identity theft (FOIT) is "an emerging negative consumer emotion activated through consumers' cognitive appraisal and/or own thoughts regarding the possibility of the theft of personal and financial data when conducting transactions online" (Hille et al., 2015, p. 2). This fear likely influences consumers' online behavioral outcomes such as the reluctance of customers to share personal and financial data online or online purchase intentions (Hille et al., 2015; Leyden, 2005). E-commerce firms should thus be interested in reducing FOIT. Because FOIT-reduction measures are likely costly to e-businesses it is imperative to identify online customer groups (i.e., segments) that are particularly prone to FOIT. Specifically, it is crucial for e-businesses to tailor specific FOIT-reduction measures for the identified segments and reassure both customers and non-customers alike to operate secure websites and to be safe from identity theft.

Drawing on the notion that consumers are particularly fearful of financial losses and damages to their reputation (e.g., Mitchison et al., 2004; Sproule and Archer, 2007; van der Meulen, 2006), Hille et al. (2015) recently proposed a FOIT measure comprising of two dimensions—fear of financial losses and fear of reputational damage. We argue that the FOIT scale gives e-commerce managers a means to identify and deal more effectively with FOIT-prone consumers by allocating resources (e.g., trust-enhancing communication) in a resource-efficient manner. To our knowledge, this is the first study that attempts to identify meaningful consumer segments based on their self-reported FOIT by using cluster analysis. Alongside consumers' FOIT, online trust and purchase intentions are incorporated as primary segmentation variables. We conclude with managerial and research implications that stem from the research.

2 Theoretical Background

IS research indicates that consumers differ in terms of their online privacy concern (Hann et al., 2007; Sheehan, 2002). However despite various advantages of grouping consumers together according to their degree of FOIT, no research in this field has been conducted so far. Identity theft is associated with severe and long lasting financial costs (Eisenstein, 2008; Mitchison et al., 2004) and in many cases with reputational damage for the victim (Miri-Lavassani et al., 2009). Reputational damage occurs, for example, when a cyber-criminal misuses stolen credit card information to purchase pornographic products or banned drugs from dubious online retailers. The typical victim of identity theft toiled an average of 141 hours to clear their name (Foley et al., 2010). The requirement of providing personal data online for an ever-expanding scope of commercial transactions (as well as for many government services) increases people's fear of being victimized, which is exacerbated by the frequency of reports in the media on identity theft occurrences (Heath and Gilbert, 1996; ITRC, 2009; Warr, 2000). Because people can be frightened of virtually almost everything (Rachman, 1977), FOIT may likewise occur as 'vicarious exposure' among consumers that have never (yet) personally experienced real online identity theft. Consequently, Hille et al. (2015) identify two FOIT dimensions (for a comprehensive literature review on FOIT see Hille et al., 2015). Fear of financial losses is "the fear of illegal or unethical appropriation and usage of personal and financial data by a cyber-criminal or other entity to gain financial benefits such as buying products on behalf of the victim" while fear of reputational damage is the "fear of misuse of illegally acquired personal data with the aim of impersonation which can cause reputational damage to the victim" (Hille et al., 2015, p. 6). Essentially, the relevance of FOIT ensues from changing a customer's behavioral intentions (Mukherjee and Dubé, 2012), including increasing consumers' reluctance to buy online (Montague, 2011) thus affecting e-commerce turnover. Such negative outcomes are likely because fear is "an activated, aversive emotion that serves to motivate escape and avoidance of threatening circumstances" (Öhman and Wiens, 2004, p. 58). To develop measures aimed at reducing consumer FOIT, e-commerce firms need to know toward which groups they need to direct measures such as employing certified trust seals or highlighting central security policies when customizing their websites depending on the consumers' FOIT-levels. Managers must first ascertain the best ways to divide the market. Scarce IS and management research, of either a conceptual or an empirical nature, has explicitly considered consumer FOIT as a possible basis for market segmentation. Combining affective variables (i.e., FOIT, along with existing measures for online trust, and uncertainty avoidance) with conventional IS segmentation variables (i.e., demographics, online shopping experience and online purchase intention) (e.g., Bhatnager and Ghose, 2004; Khalifa and Liu, 2007; Phang et al., 2010; Wu, 2006) we submit that our approach will be diagnostic for formulating key e-business decisions.

3 Methodology

3.1 Data collection and sample

To identify and profile FOIT-prone consumer segments, we collected data through a German online music customer panel (for a discussion on the appropriateness of panels for market research see Göritz, 2004). This is a suitable sample because panel members are not necessarily users of a particular website but shop online across different product categories at various e-retailers and may also differ in relation to their interests, hobbies, and online shopping experience. Moreover, in an online panel FOIT levels should be underemphasized, relative to the general population. If FOIT can be evidenced in this sample it would speak to the robustness of our findings. The invitation and link to the online survey was sent to panel members by e-mail. Respondents were directed to answer a series of questions with regard to online music shops they had visited. In addition to the two FOIT dimensions, the online questionnaire contained measures for online trust, online purchase intention, uncertainty avoidance, online shopping experience as well as demographics. The primary cluster analysis was derived on the

basis of respondents' scores on the two FOIT dimensions, online trust, and online purchase intention. The latter two constructs were purposefully chosen as primary cluster variables (aka active variables) because both active variables are likely to intervene directly in the formation of groups/segments and have been used in previous studies (e.g., Barnes et al., 2007; Dimitriadis et al., 2011; Fotopoulos and Krystallis, 2002). Trust plays a crucial role for consumers in adopting and using e-commerce (McCole et al., 2010; McKnight et al., 2002) and consumers' online purchase intention is the penultimate outcome variable for e-businesses to consider. Uncertainty avoidance, online shopping experience and demographics (i.e., age, gender, and education) were used as secondary (i.e., profiling) cluster variables since they are frequently used to profile customer segments (e.g., Bhatnagar and Ghose, 2004; Khalifa and Liu, 2007; Seabra et al., 2013).

Consumer FOIT was measured with eleven items taken from Hille et al. (2015). Online trust is the consumer's "trust in the infrastructure and the underlying control mechanism (technology trust) which deals with transaction integrity, authentication, confidentiality, and non-repudiation" (Ratnasingam et al., 2002, p. 384), which was measured with four items adapted from McKnight et al. (2002). Online purchase intention was measured with three items adapted from Salisbury et al. (2001). The items pertaining to the four primary cluster input variables appear in Table 2. Responses to these variables were measured along five-point Likert scales (1=strongly disagree to 5=strongly agree).

Uncertainty avoidance (UA) is defined as "the extent to which the members of a culture feel threatened by uncertain or unknown situations" (Hofstede, 2001, p. 161). Members of high UA cultures perceive life more as a threat and experience higher levels of anxiety than members of low UA cultures (Schumann et al., 2010). Accordingly, and at the individual consumer level, UA should amplify FOIT. Uncertainty avoidance was measured with three items adapted from Reardon et al. (2006): "I'm the kind of person who would try anything at least once", "I am cautious about trying new and different things", and "I enjoy taking chances in doing unfamiliar activities, just for variety". Online shopping experience was measured with one item "I consider myself as fairly experienced in using the Internet". Both constructs were measured along five-point Likert scales (1=strongly disagree to 5=strongly agree).

Data collection lasted two weeks. Out of the 1,286 people completed the online survey (response rate=42.9%); 45% were female. Respondents' average age was 36.7 years (standard deviation=12.49, ranging 11-81 years).

	Constructs	Mean (SD)	1	2	3	4
1	Fear of financial losses	3.37 (.98)				
2	Fear of reputational damage	2.99 (1.1)	.70** (.49)			
3	Online trust	3.02 (.76)	-.53** (.28)	-.32** (.10)		
4	Online purchase intention	4.27 (.87)	-.30** (.09)	-.24** (.06)	.29** (.08)	

*Table 1. Sample descriptive and correlations of cluster input variables (**p<.001; SD=standard deviation. Squared construct correlations are in parentheses).*

3.2 Reliability and validity assessments

To assess the reliability and validity of the four input variables (fear of financial losses, fear of reputational damage, online trust, and online purchase intention), a confirmatory factor analysis (CFA) measurement model was assessed using AMOS-20. The model fit was sound: with a chi-square divided by degrees of freedom [χ^2/d.f.] =3.35, a root mean square error of approximation [RMSEA] =.043, a standardized root mean square residual [SRMR] =.026, comparative fit index [CFI] =.99, and a goodness-of-fit index [GFI] =.96.

Next, the internal consistency of the four factors was assessed. Cronbach's alpha (α), and composite reliability (CR) for all factors exceeded .70 (Bagozzi and Yi, 1988; Gefen et al., 2000): fear of financial losses (α=.95, CR=.95), fear of reputational damage (α=.95, CR=.95), online trust (α=.86, CR=.86), and online purchase intention (α=.85, CR=.86). All factor loadings were significant at *p* <

.001 and loaded on their respective constructs (see Table 2). The correlations and descriptive statistics for the four variables appear in Table 1. Regarding convergent validity, the average variance extracted (AVE) of all four constructs was greater than .60, exceeding the threshold of .50 (Fornell and Larcker, 1981). Meeting the requirement for discriminant validity, squared construct correlations (Table 1) were all lower than the AVEs (Table 2) for their respective factors.

Construct	*Factor Loadings*	*AVE/CR*
Fear of financial losses (taken from Hille et al., 2015)		.72/.95
-I am afraid that somebody could steal my money while I am transferring my personal data online.	.86	
-I am scared that a criminal could use my bank account number to do online shopping in my name.	.90	
-I am scared that a criminal could use my credit card account number to do online shopping in my name.	.79	
-I am frightened that somebody could do online shopping at my expense.	.88	
-I am worried about an unauthorized person making online purchases using my personal data.	.90	
-I am scared that when I have to give my credit card number to shop online that it could be misused.	.80	
-I am scared that when I have to give my bank account number to shop online that it could be misused.	.81	
-The thought that a stranger could gain access to my customer's account at an online store by using my personal data frightens me.	.82	
Fear of reputational damage (taken from Hille et al., 2015)		.85/.95
-I am frightened of somebody using my personal data on the Internet in order to run me down.	.88	
-I am very worried that the unauthorized use of my personal data online could damage my reputation.	.95	
-I am worried about my reputation being damaged due to the illegal use of my personal data online.	.94	
Online trust (adapted from McKnight et al., 2002)		.61/.86
-The Internet has enough safeguards to make me feel comfortable using it to transact personal business.	.84	
-I feel assured that legal and technological structures adequately protect me from problems on the Internet.	.74	
-I feel confident that encryption and other technological advances on the Internet make it safe for me to do business there.	.74	
-In general, the Internet is now a robust and safe environment in which to transact business.	.80	
Online purchase intention (adapted from Salisbury et al., 2001)		.68/.86
-I would use the Internet for purchasing a product.	.70	
-Using the Internet for purchasing a product is something I would do.	.86	
-I could see myself using the Internet to buy a product.	.90	

Table 2.   Primary cluster variables (All factor loadings significant (p<.001); CR=composite reliability; AVE=average variance extracted).

3.3   Identifying FOIT-prone consumer segments

The composite items for each respective factor were averaged to operationalize the two FOIT dimensions, online trust, and online purchase intention. We used the respective mean values as primary input variables for clustering. Distances between the clusters were calculated with the Euclidean distance measure and aggregated clusters using Ward's procedure. The dendogram and the elbow criterion were scrutinized to ascertain the optimal number of clusters (Mooi and Sarstedt, 2011). Thresholds existed at three, four, and five clusters, respectively. In order to decide on the appropriateness of each of these three alternative solutions, we conducted a multiple discriminant analysis for each. The hit rate, or proportion of customers correctly classified was highest for the four-cluster solution, whereas the hit rate was lower for the three- and five-cluster solutions. Thus, the four-cluster solution was deemed the most suitable representation of FOIT segments.

Following a two-step clustering procedure (e.g., Ganesh et al., 2010; Punj and Stewart, 1983), we conducted a *k*-means analysis (partitioning method) next, incorporating these four primary variables. *K*-means analysis is one of the most used clustering methods in segmentation research (Wedel and Kamakura, 2012) that suits large data sets (Anil et al., 1997) and results in clusters that are considered more homogenous than those attained from hierarchical clustering (Furrer et al., 2000). To test whether the mean values differed between the four clusters, one-way analyses of variance (ANOVA, followed by a

Scheffé post-hoc-test using 95% confidence intervals) were conducted across all primary (the two FOIT dimensions, online trust, and online purchase intention) and secondary (i.e., UA, online shopping experience, and age) cluster variables. To examine differences with regard to gender and education a chi-square analysis was performed. Results revealed significant differences between all combinations of clusters (see Table 3) for all save one case of a primary input variable (i.e., online purchase intention, where the difference was not significant between clusters 1 and 3). After assessing the clusters, they were defined and labelled. The four segments are also profiled using the secondary segmentation variables (see Table 3). Because significant differences did not emerge on age, this demographic is not detailed in the ensuing paragraphs. To test differences on the secondary cluster variables gender and education based on the four clusters, chi-square analysis was conducted. To determine the effect size, Cramer's V is calculated. The results of the chi-square test revealed significant differences in gender [χ^2=17.56 (d.f.=3), *p*<.001; Cramer's V=.11, *p*<.001] and education [χ^2=43.06 (d.f.=18), *p*<.001, Cramer's V=.11, *p*<.001] between the four clusters.

	Cluster 1, Less fearful shoppers	**Cluster 2,** Strong fear but ignoring shoppers	**Cluster 3,** Fearless shoppers	**Cluster 4,** Fearful shoppers
Cluster results	n=428	n=317	n=308	n=233
Fear of financial losses	3.37[a]	4.29[b]	2.10[c]	3.79[d]
Fear of reputational damage	2.84[a]	4.30[b]	1.98[c]	3.44[d]
Online trust	2.96[a]	2.78[b]	3.65[c]	2.62[d]
Online purchase intention	4.61[a]	4.46[b]	4.71[a,c]	2.78[d]
Profiling clusters				
Uncertainty avoidance (SD)	2.62 (.76)[a,b]	2.48 (.79)[a]	2.76 (.82)[b]	2.62 (.79)[a,b]
Online shopping experience (SD)	1.84 (.81)[a]	1.97 (.73)[a]	1.62 (.76)[b]	2.07 (.90)[a]
Age (Mean (SD))	36.41 (12.08)[a]	37.22 (11.91)[a]	36.69 (12.16)[a]	36.41 (14.3)[a]
Gender				
Male (%)	236 (55.1)	157 (49.5)	198 (64.3)	115 (49.4)
Female (%)	192 (44.9)	160 (50.5)	110 (35.7)	118 (50.6)
Education				
Still at school (%)	1 (.2)	4 (1.3)	3 (1.0)	2 (.9)
Secondary school (%)	12 (2.8)	20 (6.3)	10 (3.2)	14 (6.0)
O-levels (%)	55 (12.9)	59 (18.6)	30 (9.7)	48 (20.6)
Advanced technical college certificate (%)	31 (7.2)	22 (6.9)	15 (4.9)	14 (6.0)
High school (%)	98 (22.9)	59 (18.6)	78 (25.3)	54 (23.3)
Apprenticeship (%)	77 (18.0)	59 (18.6)	58 (18.8)	47 (20.2)
University degree (%)	146 (34.1)	80 (25.2)	102 (33.1)	48 (20.6)
Not indicated (%)	8 (1.9)	14 (4.4)	12 (3.9)	6 (2.6)

Note: For variables fear of financial losses, fear of reputational damage, online trust, online purchase intention, uncertainty avoidance, online shopping experience, age, mean values with the same superscript are not significantly (p<.05) different from each other (based on ANOVA and Scheffé post-hoc-test); Chi-square tests were applied to variables gender and education; SD=standard deviation.

Table 3.   Results of cluster analysis.

Cluster 1 was the largest segment of the four clusters and labelled *less fearful shoppers* (n=428). In this cluster, customers scored moderately on the two FOIT dimensions; lower than clusters 2 and 4, but higher than cluster 3. It is notable that this is the only segment in which scores of fear of financial losses and fear of reputational damage were substantially different from each other (mean difference of .53), whereas mean scores of FOIT dimensions were closer to each other in the other segments. The online trust score was moderate and second highest of all clusters; the online purchase intention score was the second highest after cluster 3. Regarding the profiling variables, consumers' level of UA was moderate. Members of this cluster considered themselves as not very experienced with online shopping. Fifty-five percent of the consumers in this segment are male; members of this cluster are also better educated than their counterparts in segments 2 and 4.

Cluster 2 was the second largest segment. It was labelled *strong fear but ignoring shoppers* (n=317), on account of the finding that segment members reported high online purchase intention notwithstanding elevated levels of fear. Indeed, consumers in this segment scored the highest on both FOIT dimen-

sions among the four clusters. Relative to cluster 1, online trust and online purchase intention mean values were slightly lower, but similar to cluster 1, this segment's mean UA was moderate—and significantly lower than that for cluster 3 consumers. Moreover, members of this cluster were not exceptionally experienced with online shopping, although they were noticeably higher in this regard than those in cluster 3. Almost half (49.5%) of the group members were male. This segment contained about the same percentage of males and females as the *fearful shoppers* segment but members were less educated than members of segments 1 and 3.

Cluster 3, labelled *fearless shoppers,* was the third largest segment (n=308). Relative to the other clusters, this segment had the lowest scores on both FOIT dimensions and accordingly, the highest scores on both online trust and online purchase intention. Members of this segment scored moderately on UA, although significantly higher than their counterparts in cluster 2. Additionally, consumers of this segment reported the lowest levels of experience with online shopping; further intimating that FOIT concomitantly increases (rather than decreases) with online purchasing experience; FOIT and purchasing experience correlate at a significant level (r=-.18, *p*<.001). This segment contained the most disproportionate number of males (64%) versus the other three clusters. Cluster members also appeared to have higher levels of education.

Customers of cluster 4, labelled *fearful shoppers,* formed the smallest segment (n=233). Members of this cluster scored significantly higher on both FOIT dimensions than those in clusters 1 and 3, albeit lower than their counterparts in cluster 2. Moreover, they reported the lowest scores on both online trust and purchase intention. Regarding the profiling variables, similar to segment 1, members had moderate UA levels. Additionally, compared to cluster three, members of this segment reported considerably higher levels of online shopping experience, although they did not significantly differ on this aspect from segments 1 and 2. About half this segment was female *Fearful shoppers* had the lowest formal education levels amongst all four clusters (i.e., highest percentage of O-level degrees and smallest percentage of university degrees) (see Table 3).

4 Discussion

The objective of this study was to identify different consumer segments based on FOIT, alongside two variables conventionally employed to segment IS consumers, online trust and online purchase intentions. First, we demonstrated the usefulness of FOIT (together with online trust and purchase intention) to identify distinct target group segments. Second, we explored differences between the FOIT segments along relevant secondary variables (i.e., UA, online shopping experience, and key demographic indicators) to demonstrate their practical use. The associated empirical findings have both managerial and theoretical implications.

4.1 Managerial implications

Understanding consumers' FOIT is crucial for ensuring long-term business success in the rapidly developing e-commerce realm. Indeed, our research shows that FOIT is associated with online trust as well as online purchase intentions. This implies that FOIT-prone customers would avoid online shops that are not perceived as trustworthy. Clearly, such avoidance behavior should be a concern to e-businesses because it can hurt the bottom line.

The cluster analysis revealed four different FOIT-prone consumer segments, namely *less fearful shoppers*, *strong fear but ignoring shoppers*, *fearless shoppers* and *fearful shoppers*. Specifically, we found that only 24% of consumers—the *fearless shoppers*—had relatively low scores on FOIT, and high scores on online trust accompanied with the highest scores regarding online purchase intention. The remaining 76% of respondents of the sample had moderate to high mean FOIT levels. Of these, the *fearful shoppers*, representing 18% of the sample, had the highest levels of FOIT, along with the lowest levels of online trust and online purchase intention. Overall, the results suggest that FOIT is a real problem, given that the bulk of our sample of online shoppers reported experiencing it. E-commerce

managers should differentially target the four delineated market segments. For example, customers who belong to the *fearful shoppers* segment could be navigated through customized websites that will pay particular attention to addressing fearful consumers' needs by integrating comprehensive trust designs. Transferring personal and financial data online also depends partly on the trust in a specific online vendor (McCole et al., 2010). Specifically, different drivers of trust exist depending on the website category and the consumer (Bart et al., 2005). One effective way of building consumer trust in the online environment is by using appropriate trust seals (McKnight et al., 2002), to provide reassurance to customers and thus, reduce FOIT. Moreover, security policies can be implemented that can be publicized to customers when buying online, as a means of lowering customers' FOIT (James, 2010). For targeting the *fearful shoppers* (cluster 4), the *strong fear but ignoring shoppers* (cluster 2) as well the *less fearful shoppers* (cluster 1), e-commerce managers should consider customers' relative levels of education when devising interventions to the online interface. This includes the sequencing and explicitness (e.g., trust seals and security promises prominently displayed on merchant's home page), as well as the type of language employed when presenting information on merchant websites, clearly detailing the risks of online identity theft, the types of measures the specific online retailer is taking to protect consumers, and to what extent consumers can protect themselves (e.g., fire walls).

4.2 Research implications and limitations

The outcome of the current study revealed four significantly distinct groups of consumers whose FOIT level is assessed by the FOIT scale. The FOIT dimensions, alongside online trust and online purchase intention, serve as a potential basis for market segmentation, given the finding of significant differences between the distinctive FOIT dimensions, online trust and online purchase intention among several clusters. To our knowledge, this study is the first attempt to segment online consumers based on the negative emotion FOIT. In future research, it would be important to ascertain whether these four segments could be extracted in other online shopping contexts such as in clothing, consumer electronics or finance/banking. It is possible that the evaluation and interrelationships of the four variables differ for consumers when considering different online contexts (e.g., fear of reputation vs. financial loss looming larger, depending on the circumstances and situational risks/vulnerabilities). Moreover, it would be also worthwhile examining whether these clusters could be replicated in other countries. Without further validation of the clustering solution, the findings reported herein can lead to misleading and unwarranted conclusions. In future studies, the results of a cluster analysis should also be validated across two independent samples from the same population to offer some judgment on the reliability and stability of the findings.

The current research provides the empirical grounding for subsequent studies to explore additional variables to further profile these four segments. We used UA, online shopping experience, age, gender, and education as profiling variables. However, UA only differs significantly when comparing clusters 2 and 3 but not among the other clusters. This may be due to the cultural context; mainstream German society ranks relatively high on UA (Hofstede, 2014), which might account for the truncated range on the individual-level measures for this construct (see Table 3). Thus, the usefulness of UA (as well as other aspects associated with individual risk aversion) as profiling variable should be tested in future studies when surveying consumers from different cultures. Furthermore, income should be considered as profiling variable in future research as higher income results in additional privacy concerns (Graeff and Harmon, 2002) and therefore income level may affect consumers' fear of financial losses level as well.

Other context limitations of the present study should be addressed in future studies. The online music business is a highly prominent e-commerce sector—justifying its employment in this research—yet the results may not generalize to other e-commerce sectors. Second, not all panel members took part in the study. Third, the data was collected in Germany. The cluster analysis results lack cross-cultural validation. Fourth, the data is not longitudinal. Thus, it cannot provide a definitive account to explain the migration of consumers across clusters.

References

Anil C., J. D. Carroll, P. E. Green, and J. A. Rotondo (1997). "A Feature-Based Approach to Market Segmentation via Overlapping K-Centroids Clustering." *Journal of Marketing Research* 34 (3), 370–377.

Bagozzi, R. P. and Y. Yi (1988). "On the Evaluation of Structural Equation Models." *Journal of the Academy of Marketing Science* 16 (1), 74–94.

Barnes, S. J., H. H. Bauer, M. M. Neumann, and F. Huber (2007). "Segmenting Cyberspace: A Customer Typology for the Internet. *European Journal of Marketing* 41 (1/2), 71–93.

Bart, Y., V. Shankar, F. Sultan, and G. L. Urban (2005). "Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study." *Journal of Marketing* 69 (4), 133–152.

Bélanger, F. and R. E. Crossler (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4), 1017–1042.

Bhatnager, A. and S. Ghose (2004). "A Latent Class Segmentation Analysis of E-Shoppers." *Journal of Business Research* 57 (7), 758–67.

Coles-Kemp, L., Y.-L. Lai, and M. Ford (2010). *Privacy on the Internet: Attitudes and Behaviours. A survey by VOME.* URL: http://www.vome.org.uk/wp-content/uploads/2010/03/VOME-exploratorium-survey-summary-results.pdf (visited on 04/09/2014).

Dimitriadis, S., A. Kouremenos, and N. Kyrezis (2011). "Trust-Based Segmentation: Preliminary Evidence from Technology-Enabled Bank Channels." *International Journal of Bank Marketing* 29 (1), 5–31.

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

Eisenstein, E. M. (2008). "Identity Theft: An Exploratory Study with Implications for Marketers." *Journal of Business Research* 61 (11), 1160–1172.

Federal Trade Commission (2014). *Consumer Sentinel Network Data Book for January - December 2013" Federal Trade Commission, February 2014.* URL: http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf (visited on 04/07/2014).

Foley, L., K. Barney, J. Foley, J. Lee, J. Fergerson, M. Sarrel, C. Nelson, and M. Frank (2010). *Identity Theft: The Aftermath 2009, Identity Theft Resource Center (ITRC).* URL: https://allclearid.com/themes/allclearid/docs/Aftermath_2009_20100520.pdf (visited on 04/07/2014).

Fornell, C. and D. F. Larcker (1981). "Evaluating Structural Equation Models with Unobserved Variables and Measurement Errors." *Journal of Marketing Research* 18 (2), 39–50.

Forsythe, S., C. Liu, D. Shannon, and L. C. Gardner (2006). "Development of a Scale to Measure the Perceived Benefits and Risks of Online Shopping." *Journal of Interactive Marketing* 20 (2), 55–75.

Fotopoulos, C. and A. Krystallis (2002). "Organic Product Avoidance: Reasons for Rejection and Potential Buyers' Identification in a Countrywide Survey." *British Food Journal* 104 (3/4/5), 233–260.

Furrer, O., B. S. C. Liu, and D. Sudharshan (2000). "The Relationships Between Culture and Service Quality Perceptions Basis for Cross-Cultural Market Segmentation and Resource Allocation." *Journal of Service Research* 2 (4), 355–371.

Ganesh, J., K. E. Reynolds, M. Luckett, and N. Pomirleanu (2010). "Online Shopper Motivations, and E-Store Attributes: An Examination of Online Patronage Behavior and Shopper Typologies." *Journal of Retailing* 86 (1), 106–115.

Gefen, D., D. W. Straub, and M.-C. Boudreau (2000). "Structural Equation Modeling and Regression: Guidelines for Research Practice." *Communications of the Association for Information Systems* 4 (7), 1–70.

Göritz, A. (2004). "The Impact of Material Incentives on Response Quantity, Response Quality, Sample Composition, Survey Outcome and Cost in Online Access Panels." *International Journal of Market Research* 46 (3), 327–346.

Graeff, T. R. and S. Harmon (2002). "Collecting and Using Personal Data: Consumers' Awareness and Concerns." *Journal of Consumer Marketing* 19 (4), 302–318.

Hann, I.-H., K.-L. Hui, S.-Y. T. Lee, and I. P. L. Png (2007). "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24 (2), 13–42.

Harrell, E. and L. Langton (2013). *Victims of Identity Theft, 2012. Justice Department's Bureau of Justice Statistics (BJS)*. URL: http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821 (visited on 09/17/2015).

Harris, E. A., N. Perlroth, N. Popper, and H. Stout (2014). *A Sneaky Path Into Target Customers' Wallets*. New York Times. 2014-01-18. URL: http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html (visited on 05/15/2015).

Heath, L. and K. Gilbert (1996). "Mass Media and Fear of Crime." *American Behavioral Scientist* 39 (4), 379–386.

Hille, P., G. Walsh, and M. Cleveland (2015). "Consumer Fear of Online Identity Theft: Scale Development and Validation." *Journal of Interactive Marketing* 30 (2), 1–19.

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations*. 2nd Edition. Thousand Oaks, CA: Sage.

_____, _____ (2014). *Geert Hofstede Cultural Dimensions, Country Comparison, Germany*. URL: http://geert-hofstede.com/ (visited on 06/23/2015).

ITRC (Identity Theft Resource Center) (2009). *The Need for "Secure Payment Agent" (SPA). ITRC 2009 Consumer Awareness Survey*. URL: http://www.idtheftcenter.org/ITRC-Surveys-Studies/consumer-awareness-survey.html (visited on 03/10/2014).

James, S. (2010). *What Security Fears Cost E-Commerce*. E-Commerce Times. 2010-04-01. URL: http://www.ecommercetimes.com/story/69667.htmlIC3 (visited on 03/06/2014).

Khalifa, M. and V. Liu (2007). "Online Consumer Retention: Contingent Effects of Online Shopping Habit and Online Shopping Experience." *European Journal of Information Systems* 16 (6), 780–792.

Leyden, J. (2005). *ID Theft Fears Prompt Ecommerce Boycott*. The Register. 2005-07-21. URL: http://www.theregister.co.uk/2005/07/21/id_theft_ecommerce_survey (visited on 04/21/2014).

McCole, P., E. Ramsey, and J. Williams (2010). "Trust Considerations on Attitudes Towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns." *Journal of Business Research* 63 (9-10), 1018–1024.

McKnight, D. H., V. Choudhury, and C. Kacmar (2002). "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology." *Information Systems Research* 13 (3), 334–359.

Miri-Lavassani, K., V. Kumar, B. Movahedi, and U. Kumar (2009). "Developing an Identity Fraud Measurement Model: A Factor Analysis Approach." *Journal of Financial Crime* 16 (4), 364–386.

Mitchison, N., M. Wilikens, L. Breitenbach, R. Urry, and S. Portesi (2004). "Identity Theft. A Discussion Paper." URL: http://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf (visited on 02/17/2014).

Montague, D. A. (2011). *Essentials of Online Payment Security and Fraud Prevention*. Hoboken, NJ: John Wiley & Sons.

Mooi, E. and M. Sarstedt (2011). *A Concise Guide to Market Research*, Berlin, Heidelberg: Springer.

Mukherjee, A. and L. Dubé (2012). "Mixing Emotions: The Use of Humor in Fear Advertising." *Journal of Consumer Behavior* 11 (2), 147–161.

Öhman, A. and S. Wiens (2004). "The Concept of an Evolved Fear Module and Cognitive Theories of Anxiety." In: *Feeling and Emotions: The Amsterdam Symposium*. Ed. by A. S. R. Manstead, N. Frijda, and A. Fischer. Cambridge: Cambridge University Press, pp. 58–80.

Orton, E. and C. Schlag (2014). "Creating a Model of Cyber Proficiency: Remodeling Law Enforcement Tactics in Pittsburgh to Address the Evolving Nature of Cybersecurity." *Journal of Technology Law & Policy* 14, 276–279.

Pavlou, P. A. (2011). "State of the Information Privacy Literature: Where are We Now and Where Should We Go?" *MIS Quarterly* 35 (4), 977–988.

Phang, C. W., A. Kankanhalli, K. Ramakrishnan, and K. S. Raman (2010). "Customers' Preference of Online Store Visit Strategies: An Investigation of Demographic Variables." *European Journal of Information Systems* 19 (3), 344–358.

Punj, G. and D. W. Stewart (1983). "Cluster Analysis in Marketing Research: Review and Suggestions for Application." *Journal of Marketing Research* 20 (2), 134–148.

Rachman, S. (1977). "The Conditioning Theory of Fear-Acquisition: A Critical Examination." B*ehaviour Research and Therapy* 15 (5), 375–387.

Ratnasingam, P., P. A. Pavlou, and Y.-h. Tan (2002). "The Importance of Technology Trust for B2B Electronic Commerce." In: *Proceedings of the 15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy*. Bled, Slovenia, pp. 384–398.

Reardon, J., C. Miller, B. Foubert, I. Vida, and L. Rybina (2006). "Antismoking Messages for the International Teenage Segment: The Effectiveness of Message Valence and Intensity across Different Cultures." *Journal of International Marketing* 14 (3), 115–138.

Reisig, M. D., T. C. Pratt, and K. Holtfreter (2009). "Perceived Risk of Internet Theft Victimization. Examining the Effects of Social Vulnerability and Financial Impulsivity." *Criminal Justice and Behavior* 36 (4), 369–384.

Reyns, B. W. (2013). "Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses," *Journal of Research in Crime and Delinquency* 50 (2), 216–238.

Ruan, X. (2014). *Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine*. 1st Edition. New York: Apress.

Salisbury, D. W., R. A. Pearson, A. W. Pearson, and D. W. Miller (2001). "Perceived Security and World Wide Web Purchase Intention." *Industrial Management & Data Systems* 101 (4), 165–176.

Schumann, J. H., F. v. Wangenheim, A. Stringfellow, Z. Yang, S. Praxmarer, F. R. Jiménez, V. Blazevic, R. M. Shannon, S. G. Komor, and M. Komor (2010). "Drivers of Trust in Relational Service Exchange: Understanding the Importance of Cross-Cultural Differences." *Journal of Service Research* 13 (4), 453–468.

Seabra, C., S. Dolnicar, J. L. Abrantes, and E. Kastenholz (2013). "Heterogeneity in Risk and Safety Perceptions of International Tourists." *Tourism Management* 36, 502–510.

Sheehan, K. B. (2002). "Toward a Typology of Internet Users and Online Privacy Concerns." *The Information Society: An International Journal* 18 (1), 21–32.

Sproule, S. and N. Archer (2007). "Defining Identity Theft, Conference Publications." Eighth World Congress on the Management of eBusiness. WCMeB 2007. Toronto, Ontario: IEEE. Computer Society Press.

Tsai, J. Y., S. Egelman, L. Cranor, and A. Acquisti (2011). "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research* 22 (2), 254–268.

Van der Meulen, N. (2006). "The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union." Tilburg University. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.6835&rep=rep1&type=pdf (visited on 05/09/2013).

Wall, D. S. (2008). "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime." *International Review of Law, Computers and Technology* 22 (1-2), 45–63.

Warr, M. (2000). "Fear of Crime in the United States: Avenues for Research and Policy." In: *Measurement and Analysis of Crime and Justice, Criminal Justice 2000.* Ed. by D. Duffee. Washington, D.C.: U.S. Department of Justice. National Institute of Justice, pp. 451–489.

Wedel, M. and W. A. Kamakura (2012). *Market Segmentation: Conceptual and Methodological Foundations*. Vol. 8, Springer Science & Business Media.

Wu, S.-I. (2006). "A Comparison of the Behavior of Different Customer Clusters towards Internet Bookstores." *Information & Management* 43 (8), 986–1001.